

**“All-in-One Is All You Need.”**

ALL-IN-ONE

CompTIA

# Security+<sup>TM</sup>

Exam SY0-601

EXAM GUIDE

SIXTH EDITION

Save 10% on any  
CompTIA exam  
voucher! Coupon  
code inside.

Online content  
includes:

- 250 practice exam  
questions
- Test engine that  
provides full-length  
practice exams and  
customizable quizzes  
by chapter or by  
exam domain

*Complete coverage  
of all exam objectives*

*Ideal as both a study  
tool and an  
on-the-job reference*

*Filled with practice exam  
questions and in-depth  
explanations*

Mc  
Graw  
Hill

WM. ARTHUR CONKLIN, PhD

CompTIA Security+, CISSP®

GREGORY WHITE, PhD

# CompTIA Security +

**Kỳ thi SY0-601  
Phiên bản thứ Sáu**

## Mục lục

Thông tin bản quyền .....	17
Điều khoản Sử dụng .....	18
Về các Tác giả .....	20
Về các Biên tập viên Kỹ thuật .....	23
Lời mở đầu .....	24
Lời cảm ơn .....	27
Giới thiệu .....	29
Tại sao lại tập trung vào Bảo mật? .....	29
Một Nhu cầu Gia tăng đối với các Chuyên gia Bảo mật .....	30
Chuẩn bị cho Kỳ thi CompTIA Security+ .....	33
Quyển sách Này Được Tổ chức Như thế nào .....	34
Những Tính năng Đặc biệt của chuỗi [ấn phẩm] Tất cả trong Một .....	35
Bản đồ Mục tiêu .....	35
Các Biểu tượng .....	35
Cuối Chương - Các Câu hỏi và Đánh giá .....	37
Security+ Danh sách Phần mềm và Phần cứng được Đề xuất .....	37
Phần cứng .....	38
Phần mềm .....	38
Khác .....	38
TotalTester Trực tuyến .....	38
Tiến lên và Đi tới .....	38
Bản đồ Mục tiêu: Kỳ thi SY0-601 .....	39
Giới thiệu về Nhóm dịch ASV .....	43
PHẦN I .....	46
Chương 1 Các Kỹ thuật Kỹ thuật Xã hội (Tấn công phi kỹ thuật) .....	47
Các Phương pháp Kỹ thuật Xã hội (Tấn công Phi kỹ thuật) .....	48
Tấn công giả mạo (Phishing) .....	51
Tấn công giả mạo qua tin nhắn SMS (Smishing) .....	52
Truy cập bất hợp pháp thông qua giọng nói (Vishing) .....	53

Thư rác .....	54
Thư rác qua Tin nhắn Tức thời (SPIM) .....	55
Tấn công giả mạo nhắm mục tiêu (Spear Phishing) .....	55
Dò tìm Đồ phế thải (Dumpster Diving) .....	55
Nhin qua Vai (Shoulder Surfing) .....	56
Chuyển hướng lưu lượng web (Pharming) .....	57
Tấn công Tailgating (Tailgating) .....	57
Thông tin Câu hỏi mở (Eliciting Information) .....	58
Lừa đảo kiểu cá voi (Whaling) .....	59
Prepending.....	59
Gian lận Danh tính (Identity Fraud) .....	60
Lừa đảo Hóa đơn Trực tuyến (Invoice Scams).....	61
Thu thập Thông tin đăng nhập (Credential Harvesting).....	61
Do thám (Reconnaissance) .....	62
Đánh lừa (Hoax) .....	63
Mạo danh (Impersonation).....	64
Tấn công Vũng Nước (Watering hole attacks) .....	66
Chiếm quyền URL (Typosquatting) .....	67
Viện cớ (Pretexting) .....	68
Các Chiến dịch tạo Ảnh hưởng .....	68
Các Nguyên tắc (Lý do Hiệu quả).....	69
Biện pháp phòng thủ.....	72
Tóm tắt Chương .....	75
Chương 2 Các Kiểu Chỉ báo Tấn công .....	82
Phần mềm độc hại (Malware) .....	84
Tấn công Mật khẩu.....	97
Tấn công Vật lý .....	102
Trí tuệ Nhân tạo Đối nghịch (Adversarial Artificial Intelligence) .....	105
Tấn công Chuỗi-Cung ứng .....	107
Tấn công Dựa trên-Đám mây so với Trực tiếp tại Cơ sở .....	107

Tấn công Mật mã .....	108
Tóm tắt Chương .....	111
Chương 3 Các Chỉ báo Tấn công Ứng dụng .....	119
Leo thang Đặc quyền .....	120
Chèn lệnh script độc hại (Cross-Site Scripting) .....	120
Tấn công Chèn lệnh (Injection Attack) .....	122
Giải tham chiếu Con trỏ/Đối tượng (Pointer/Object Dereference) .....	127
Xâm nhập Danh bạ (Directory Traversal) .....	127
Tràn Bộ nhớ đệm (Buffer Overflow) .....	128
Điều kiện Cạnh tranh (Race Condition) .....	130
Xử lý Lỗi Không thích hợp (Improper Error Handling) .....	133
Xử lý Đầu vào Không thích hợp (Improper Input Handling) .....	134
Tấn công Phát lại (Replay Attack) .....	135
Tràn Bộ số nguyên (Integer Overflow) .....	137
Giả mạo Yêu cầu (Request Forgery) .....	137
Tấn công Giao diện Lập trình Ứng dụng (API) .....	139
Cạn kiệt Tài nguyên .....	140
Rò rỉ bộ nhớ .....	141
Tước bỏ SSL (Secure Socket Layer Stripping) .....	141
Thao túng Trình điều khiển (Driver Manipulation) .....	141
Vượt qua Băm (Pass the Hash) .....	143
Tóm tắt Chương .....	144
Chương 4 Các Chỉ báo Tấn công (hệ thống) Mạng .....	151
Không dây .....	152
Tấn công Trên đường (On-path Attack) .....	160
Tấn công Lớp 2 .....	162
Hệ thống Tên Miền (Domain Name System – DNS) .....	164
Hình 4-2 – nslookup của một truy vấn DNS .....	166
Hình 4-4 – Phản hồi bộ đệm cho một truy vấn bằng DNS .....	167
Từ chối Dịch vụ được Phân tán (Distributed Denial-of-Service – DDoS) ..	170

Hình 4-5 - Các cuộc tấn công DDoS.....	171
Hình 4-6 Bắt tay TCP/IP ba-chiều .....	174
Hình 4-7 Một cuộc tấn công gây ngập lụt SYN .....	175
Thực thi Tập lệnh và Mã Phần mềm độc hại .....	178
Tóm tắt Chương .....	181
<b>Chương 5 Các Tác nhân, Véc-tơ và Nguồn Tình báo về Mỗi đe dọa .....</b>	<b>188</b>
Các Tác nhân và Mỗi đe dọa .....	189
Hình 5-1 Sự phân tán của những cấp độ kỹ năng của kẻ tấn công .....	190
Các thuộc tính của các Tác nhân .....	200
Các Véc-tơ .....	203
Nguồn Tình báo về Mỗi đe dọa .....	207
Các Nguồn Nghiên cứu .....	218
Tóm tắt Chương .....	224
<b>Chương 6 Các Lỗ hổng .....</b>	<b>231</b>
Các Lỗ hổng Dựa-trên-Đám-mây so với Tại-Cơ-sở .....	232
Zero Day .....	232
Thiết lập cấu hình Kém .....	233
Những Rủi ro Bên-thứ-ba .....	239
Quản lý Bản vá Kém hoặc Không thích hợp .....	245
Các Nền tảng Kế thừa .....	248
Tác động .....	249
Tóm tắt Chương .....	254
<b>Chương 7 Đánh giá Bảo mật .....</b>	<b>260</b>
Săn tìm Mỗi đe dọa .....	261
Quét Lỗ hổng .....	264
Quản lý Sự kiện và Thông tin Bảo mật/Nhật ký hệ thống (SIEM) .....	271
Điều phối, Tự động hóa và Ứng phó Bảo mật (SOAR) .....	276
Tóm tắt Chương .....	279
<b>Chương 8 Kiểm nghiệm Xâm nhập .....</b>	<b>285</b>
Kiểm nghiệm Xâm nhập .....	286

Do thám Chủ động và Thụ động .....	297
Các kiểu Bài tập .....	302
Tóm tắt Chương .....	306
Phần II .....	312
Chương 9 Kiến trúc Bảo mật Doanh nghiệp .....	313
Quản lý Cấu hình .....	314
Chủ quyền Dữ liệu .....	317
Bảo vệ Dữ liệu .....	318
Những cân nhắc về Vị trí địa lý .....	324
Các biện pháp kiểm soát Ứng phó và Khôi phục .....	324
Secure Socket Layer (SSL)/Transport Layer Security (TLS) .....	325
Băm .....	326
Những cân nhắc về API .....	327
Khả năng Phục hồi của Địa điểm .....	327
Lừa dối và Phá hoại .....	329
Tóm tắt Chương .....	333
Chương 10 Bảo mật Áo hóa và Bảo mật Đám mây .....	339
Các Mô hình Đám mây .....	340
Các nhà cung cấp Dịch vụ Đám mây .....	344
Nhà cung cấp Dịch vụ Được quản lý (MSP)/Nhà cung cấp Dịch vụ Bảo mật Được quản lý (MSSP) .....	345
On-Premises so với Off-Premises .....	345
Điện toán Sương mù .....	346
Điện toán Biên .....	347
Thin Client .....	348
Containers .....	348
Vị dịch vụ/API .....	349
Cơ sở hạ tầng như Mã phần mềm .....	350
Kiến trúc Không máy chủ (Serverless) .....	352
Tích hợp các Dịch vụ .....	353

Các Chính sách Tài nguyên .....	353
Cửa ngõ Chuyển tiếp.....	353
Ảo hóa .....	354
Tóm tắt Chương .....	358
Chương 11 Các Khái niệm về Phát triển, Triển khai và Tự động hóa Ứng dụng An toàn .....	364
Môi trường .....	365
Cấp phép và Ngừng cấp phép .....	367
Phép đo Tính toàn vẹn .....	368
Các Kỹ thuật Lập trình Bảo mật .....	369
Dự án Bảo mật Ứng dụng Web Mở (OWASP) .....	376
Tính đa dạng của Phần mềm .....	376
Tự động hóa/Tập lệnh theo kịch bản .....	379
Tính đàn hồi .....	382
Khả năng mở rộng .....	383
Kiểm soát phiên bản .....	383
Tóm tắt Chương .....	385
Chương 12 Xác thực và Cấp phép .....	391
Các Phương pháp Xác thực .....	391
Sinh trắc học .....	399
Các Yếu tố Xác thực Nhiều lớp (MFA) và các Thuộc tính .....	407
Xác thực, Cấp phép và Tính toán (AAA) .....	413
Các yêu cầu Đám mây so với Tại-chỗ .....	414
Tóm tắt Chương .....	416
Chương 13 Khả năng Phục hồi An ninh mạng .....	423
Dự phòng .....	424
Nhân bản .....	434
Tại chỗ so với Đám mây .....	436
Các kiểu Sao lưu .....	436
Không bền .....	446

Tính Sẵn sàng Cao .....	447
Thứ tự Khôi phục .....	449
Tính đa dạng .....	449
Tóm tắt Chương .....	453
Chương 14 Các Hệ thống Nhúng và Hệ thống Chuyên biệt .....	459
Các Hệ thống Nhúng .....	460
Giám sát Kiểm soát và Thu thập Dữ liệu (SCADA)/Hệ thống Kiểm soát Công nghiệp (ICS) .....	463
Internet Vạn vật .....	467
Các Hệ thống Chuyên biệt .....	470
Âm thanh thoại qua nền IP (VoIP) .....	475
Hệ thống Sưởi, Thông gió, Điều hòa Không khí (HVAC) .....	476
Drones .....	477
Máy in Đa chức năng (MFPs) .....	477
Hệ điều hành Thời gian Thực (RTOSs) .....	478
Hệ thống trên một con chip (SoC) .....	479
Những cân nhắc về Giao tiếp .....	480
Các Ràng buộc .....	483
Tóm tắt Chương .....	488
Chương 15 Các Biện pháp kiểm soát Bảo mật Vật lý .....	494
Rào chắn/Chướng ngại vật .....	496
Hành lang Kiểm soát Truy cập .....	498
Huy hiệu .....	498
Báo động .....	499
Biển báo chỉ dẫn .....	500
Máy ghi hình .....	500
Truyền hình Mạch kín (CCTV) .....	502
Ngụy trang Công nghiệp .....	504
Con người .....	505
Khóa .....	507

Khóa Dữ liệu USB .....	513
Đèn chiếu sáng .....	514
Hàng rào .....	514
Chữa cháy .....	515
Các Cảm biến .....	520
Thiết bị bay không người lái .....	524
Nhật ký Khách viếng thăm .....	524
Lồng Faraday .....	525
Khe hở Không khí .....	526
Mạng con được Sàng lọc .....	526
Phân phối Cáp được Bảo vệ .....	527
Khu vực An ninh .....	527
Phá hủy Dữ liệu An toàn .....	531
Tóm tắt Chương .....	535
<b>Chương 16 Các Khái niệm Mật mã học .....</b>	<b>540</b>
Những khái niệm Mật mã Tổng quát .....	541
Chữ ký Kỹ thuật số .....	543
Độ dài của Khóa .....	545
Kéo căng Khóa .....	546
“Trộn muối” (Salting) .....	547
Băm .....	548
Trao đổi Khóa .....	550
Mật mã Đường cong Elliptic .....	551
Bí mật Chuyển tiếp Hoàn hảo .....	552
Mật mã Lượng tử .....	553
Ký nguyên Hậu-Lượng tử .....	554
Khóa Phù du (Ephemeral) .....	555
Chế độ Vận hành .....	555
Bộ đếm .....	557
Blockchain .....	558

Bộ Mật mã .....	559
Đổi xứng so với Bất đối xứng .....	560
Mật mã Hạng nhẹ .....	562
Steganography .....	563
Mã hóa Đồng hình .....	565
Những trường hợp Sử dụng Phổ biến .....	566
Những hạn chế .....	568
Tóm tắt Chương .....	574
<b>Phần III .....</b>	<b>580</b>
Chương 17 Các Giao thức Bảo mật .....	581
Các Giao thức .....	582
Các Trường hợp Sử dụng .....	592
Tóm tắt Chương .....	598
Chương 18 Bảo mật Máy vật chủ và Ứng dụng .....	603
Bảo vệ Điểm đầu cuối .....	604
Toàn vẹn Khởi động .....	617
Cơ sở dữ liệu .....	619
Bảo mật Ứng dụng .....	621
Tăng cường bảo mật (Hardening) .....	628
Ổ đĩa Tự Mã hóa (SED)/ Mã hóa Ổ đĩa Toàn bộ (FDE) .....	635
Hardware Root of Trust .....	636
Trusted Platform Module (TPM) .....	637
Sandboxing .....	638
Tóm tắt Chương .....	639
Chương 19 Thiết kế Mạng Bảo mật .....	645
Cân bằng tải .....	646
Phân đoạn Mạng .....	649
Mạng Riêng Ảo .....	659
DNS .....	666
Kiểm soát Truy cập Mạng (NAC) .....	667

Quản lý Ngoài-dải-băng-tần (Out-of-band).....	669
Bảo mật Cổng .....	670
Thiết bị Mạng (Network Appliances) .....	675
Tóm tắt Chương .....	701
Chương 20 Bảo mật Không dây.....	708
Các Giao thức Mật mã .....	710
Các Giao thức Xác thực .....	715
Các Phương pháp.....	719
Những Cân nhắc Cài đặt.....	722
Tóm tắt Chương .....	728
Chương 21 Các Giải pháp Bảo mật Di động .....	733
Các Phương pháp và Bộ Nhận Kết nối .....	734
Quản lý Thiết bị Di động (MDM) .....	742
Các Thiết bị Di động .....	752
Tóm tắt Chương .....	766
Chương 22 Triển khai Bảo mật Đám mây .....	771
Các Biện pháp kiểm soát Bảo mật Đám mây .....	772
Các Giải pháp.....	783
Biện pháp kiểm soát Đám-mây-tự-nhiên so với Giải pháp Bên-thứ-ba .....	788
Tóm tắt Chương .....	790
Chương 23 Các Biện pháp kiểm soát Quản lý Tài khoản và Danh tính .....	795
Danh tính.....	796
Các Kiểu Tài khoản .....	801
Các Chính sách Tài khoản .....	806
Tóm tắt Chương .....	821
Chương 24 Triển khai Xác thực và Cấp phép .....	827
Quản lý Xác thực .....	828
Xác thực .....	831
Lược đồ Kiểm soát Truy cập .....	843
Tóm tắt Chương .....	857

Chương 25 Cơ sở hạ tầng Khóa Công khai .....	863
Cơ sở hạ tầng Khóa Công khai (PKI) .....	865
Các kiểu Chứng nhận .....	883
Định dạng Chứng nhận .....	891
Các Khái niệm .....	894
Tóm tắt Chương .....	909
Phần IV .....	915
Chương 26 Các Công cụ/Đánh giá Bảo mật Tổ chức .....	916
Do thám và Khám phá Hệ thống Mạng .....	918
Thao tác Tập tin .....	933
Môi trường Shell và Script .....	936
Bắt và Phát lại Gói tin .....	939
Điều tra pháp y .....	941
dd .....	941
memdump .....	942
WinHex .....	943
FTK Imager .....	943
Autopsy .....	944
Những Khuôn khổ Khai thác .....	944
Bẻ khóa Mật khẩu .....	945
Vệ sinh Dữ liệu .....	946
Tóm tắt Chương .....	947
Chương 27 Các Chính sách, Quy trình và Thủ tục Ứng phó Sự cố .....	952
Các Kế hoạch Ứng phó Sự cố .....	953
Quy trình Ứng phó Sự cố .....	954
Thực hành .....	959
Các Khuôn khổ Tấn công .....	962
Quản lý Bên liên quan .....	966
Kế hoạch Truyền thông .....	967
Kế hoạch Khôi phục Sau thảm họa .....	967

Kế hoạch Liên tục Kinh doanh .....	969
Liên tục Hoạch định Vận hành (COOP) .....	971
Nhóm Ứng phó Sự cố .....	972
Chính sách Lưu giữ .....	973
Tóm tắt Chương .....	976
Chương 28 Điều tra .....	982
Kết quả đầu ra từ việc Quét Lỗi hỏng .....	983
Thông tin tổng quan SIEM .....	983
Tập tin Nhật ký .....	987
Syslog/Rsyslog/Syslog-ng .....	992
Journalctl .....	993
NXLog .....	993
Giám sát Băng thông .....	994
Siêu Dữ liệu .....	994
NetFlow/sFlow .....	1000
IPFIX .....	1001
Tóm tắt Chương .....	1004
Chương 29 Các Kỹ thuật và Biện pháp Giảm nhẹ .....	1009
Tái lập cấu hình Các giải pháp Bảo mật Đầu cuối .....	1010
Những thay đổi Cấu hình .....	1012
Cách ly .....	1018
Ngăn chặn .....	1018
Phân đoạn .....	1019
Điều phối, Tự động hóa và Ứng phó Bảo mật (SOAR) .....	1022
Tóm tắt Chương .....	1025
Chương 30 Điều tra pháp y Kỹ thuật số .....	1030
Tài liệu/Băng chứng .....	1031
Thu thập (Acquisition) .....	1044
Tại-chỗ so với Đám mây .....	1051
Tính toàn vẹn .....	1053

Bảo quản .....	1056
Khám-phá-điện-tử (E-Discovery) .....	1058
Khôi phục Dữ liệu .....	1058
Không khước từ .....	1060
Tình báo Chiến lược/Phản gián .....	1061
Tóm tắt Chương .....	1062
<b>Phần V .....</b>	<b>1069</b>
Chương 31 Các Biện pháp kiểm soát Bảo mật .....	1070
Các Biện pháp kiểm soát Bảo mật .....	1071
Các Thể loại .....	1072
Các Kiểu Kiểm soát .....	1074
Tóm tắt Chương .....	1078
Chương 32 Các Quy định, Tiêu chuẩn và Khuôn khổ .....	1084
Các Quy định, Tiêu chuẩn và Luật lệ .....	1085
Các Khuôn khổ Chính .....	1095
Hướng dẫn So sánh điểm chuẩn và Cấu hình Bảo mật .....	1101
Tóm tắt Chương .....	1106
Chương 33 Các Chính sách Tổ chức .....	1112
Nhân sự .....	1114
Sự đa dạng của các Kỹ thuật Đào tạo .....	1126
Quản lý Rủi ro Bên-Thứ-ba .....	1126
Dữ liệu .....	1132
Các Chính sách Thông tin đăng nhập .....	1134
Các Chính sách Tổ chức .....	1137
Tóm tắt Chương .....	1140
Chương 34 Quản lý Rủi ro .....	1147
Các Kiểu Rủi ro .....	1148
Các Chiến lược Quản lý Rủi ro .....	1151
Phân tích Rủi ro .....	1154
Thảm họa .....	1168

Phân tích Tác động Kinh doanh (BIA) .....	1171
Tóm tắt Chương .....	1177
Chương 35 Quyền riêng tư .....	1184
Những Hậu quả của việc Vi phạm Quyền Riêng tư đối với Tổ chức.....	1185
Thông báo Vi phạm .....	1187
Các Kiểu Dữ liệu .....	1189
Các Công nghệ Tăng-cường-Quyền-Riêng-tư .....	1196
Vai trò và Trách nhiệm .....	1200
Vòng đời của Thông tin .....	1203
Đánh giá Tác động .....	1204
Các Điều khoản Thỏa thuận .....	1205
Thông báo Quyền Riêng tư .....	1206
Tóm tắt Chương .....	1208
Phần VI .....	1214
Phụ lục A Mô hình OSI và các Giao thức Internet .....	1215
Các Khuôn khổ và Giao thức Kết nối mạng .....	1215
Mô hình OSI .....	1216
Các Giao thức Internet .....	1224
Đánh giá .....	1230
Phụ lục B Nói về Nội dung Trực tuyến .....	1232
Yêu cầu Hệ thống .....	1232
Tài khoản trên Trung tâm Đào tạo Hội thảo Tổng của bạn .....	1232
Điều khoản và Điều kiện của Giấy phép Người dùng Đơn .....	1233
TotalTester Online .....	1235
Hỗ trợ Kỹ thuật .....	1236
Chú giải thuật ngữ .....	1237

## Thông tin bản quyền

Bản quyền 2021 McGraw Hill. Tất cả các quyền được bảo lưu. Trừ khi được chấp thuận theo Đạo luật Bản quyền Liên Bang 1976, không có bất cứ phần nào của ấn phẩm này có thể được tái xuất bản hoặc phân phối dưới bất kỳ hình thức nào hoặc bất kỳ phương tiện nào, hoặc được lưu trữ trong một cơ sở dữ liệu hoặc hệ thống có thể truy xuất được, mà không có sự cho phép bằng văn bản của nhà xuất bản, ngoại trừ danh sách liệt kê có thể được nhập, lưu trữ, và thực thi trong một hệ thống máy tính, nhưng chúng không thể được tái sản xuất đối với ấn phẩm này.

ISBN: 978-1-26-046401-6

MHID: 1-26-046401-6

Tài liệu trong phiên bản Sách điện tử này cũng có thể thể hiện trong ấn bản in với tiêu đề: ISBN: 978-1-26-046400-9, MHID: 1-26-046400-8.

Sách điện tử được chuyển đổi bởi codeMantra

Phiên bản 1.0

Mọi thương hiệu là thương hiệu của chủ sở hữu tương ứng của chúng. Thay vì đặt một biểu tượng thương hiệu sau mỗi lần xuất hiện của một tên gọi đã được đăng ký thương hiệu, chúng tôi sử dụng những tên gọi theo cách biên tập, và vì lợi ích của chủ sở hữu thương hiệu, và không có ý định vi phạm nhãn hiệu. Khi những biểu tượng như vậy xuất hiện trong quyển sách này, chúng được in hoa với chữ cái đầu tiên.

Sách điện tử McGraw-Hill Education có sẵn với số lượng giảm giá đặc biệt để sử dụng làm phần thưởng và khuyến mại hoặc để sử dụng trong các chương trình đào tạo của công ty. Để liên hệ với đại diện của chúng tôi, vui lòng ghé thăm trang Contact Us tại địa chỉ trang web: [www.mhprofessional.com](http://www.mhprofessional.com).

Thông tin đã được thu thập bởi McGraw Hill từ nhiều nguồn được cho là đáng tin cậy. Tuy nhiên, vì khả năng xảy ra lỗi con người hoặc máy móc từ những nguồn của chúng tôi, McGraw Hill, hoặc nguồn khác, McGraw Hill không đảm bảo tính chính xác, đầy đủ, hoặc hoàn chỉnh của bất kỳ thông tin nào và không chịu trách nhiệm cho bất kỳ lỗi hoặc sai sót nào từ việc sử dụng những thông tin như vậy.

## **Điều khoản Sử dụng**

Đây là một tác phẩm có bản quyền và McGraw-Hill Education và những người cấp phép của nó bảo lưu mọi quyền trong và đối với tác phẩm. Việc sử dụng tác phẩm này tùy thuộc vào các điều khoản. Trừ khi được cho phép theo Đạo luật Bản quyền 1976 và quyền lưu trữ và truy xuất một bản sao của tác phẩm, bạn không được phép biên dịch ngược, tháo rời, đảo ngược thiết kế, tái tạo, sửa đổi, tạo các tác phẩm phái sinh dựa trên, truyền tải, phân phối, phổ biến, bán, xuất bản hoặc cấp phép phụ cho tác phẩm hoặc bất kỳ phần nào của nó mà không có sự đồng ý trước của McGraw-Hill Education. Bạn có thể sử dụng tác phẩm cho mục đích phi thương mại và cá nhân của bạn, bất kỳ hình thức sử dụng nào khác đối với tác phẩm đều bị nghiêm cấm. Quyền sử dụng tác phẩm của bạn có thể bị chấm dứt nếu bạn không tuân thủ các điều khoản này.

TÁC PHẨM NÀY ĐƯỢC CUNG CẤP "NGUYÊN TRẠNG." McGRAW-HILL EDUCATION VÀ CÁC NHÀ CẤP PHÉP CỦA NÓ KHÔNG ĐẢM BẢO HOẶC BẢO ĐẢM VỀ TÍNH CHÍNH XÁC, ĐẦY ĐỦ HOẶC HOÀN CHỈNH HOẶC KẾT QUẢ CÓ ĐƯỢC KHI SỬ DỤNG TÁC PHẨM NÀY, BAO GỒM BẤT KỲ THÔNG TIN NÀO KHÁC CÓ THỂ ĐƯỢC TIẾP CẬN TỪ TÁC PHẨM THÔNG QUA SIÊU LIÊN KẾT HOẶC NGƯỢC LẠI, VÀ TỪ CHỖI MỘT CÁCH RÕ RÀNG BẤT KỲ SỰ BẢO ĐẢM NÀO, RÕ RÀNG HOẶC NGỤ Ý, BAO GỒM NHƯNG KHÔNG GIỚI HẠN CÁC

## BẢO ĐẢM ĐƯỢC NGỤ Ý VỀ KHẢ NĂNG BÁN ĐƯỢC HOẶC PHÙ HỢP VỚI MỘT MỤC ĐÍCH CỤ THỂ.

McGraw-Hill Education và các nhà cấp phép của McGraw-Hill Education không bảo đảm hoặc đảm bảo rằng các chức năng có trong tác phẩm sẽ đáp ứng yêu cầu của bạn hoặc hoạt động của nó sẽ không bị gián đoạn hoặc không có lỗi. Cả McGraw-Hill Education và người cấp phép của McGraw-Hill Education sẽ không chịu trách nhiệm pháp lý đối với bạn hoặc bất kỳ ai khác về bất kỳ sự không chính xác, sai lầm hoặc thiếu sót nào, bất kể nguyên nhân, trong công việc hoặc bất kỳ thiệt hại nào phát sinh từ đó. McGraw-Hill Education không chịu trách nhiệm về nội dung của bất kỳ thông tin nào được truy cập thông qua tác phẩm. Trong mọi trường hợp, McGraw-Hill Education và/hoặc người cấp phép của McGraw-Hill Education sẽ không chịu trách nhiệm pháp lý đối với bất kỳ thiệt hại gián tiếp, ngẫu nhiên, đặc biệt, trùng phạt, do hậu quả hoặc tương tự do việc sử dụng hoặc không thể sử dụng tác phẩm, ngay cả khi bất kỳ thiệt hại nào trong số chúng đã được thông báo về khả năng xảy ra những thiệt hại đó. Giới hạn trách nhiệm này sẽ áp dụng cho bất kỳ khiếu nại hoặc nguyên nhân nào cho dù khiếu nại hoặc nguyên nhân đó phát sinh trong hợp đồng, sai lầm dân sự hay cách nào khác.

Tác phẩm này được dành riêng cho rất nhiều chuyên gia bảo mật thông tin, những người đang làm việc một cách thầm lặng để đảm bảo sự an toàn của cơ sở hạ tầng tối quan trọng của quốc gia của chúng ta. Chúng tôi muốn ghi nhận hàng nghìn cá nhân tận tụy, những người nỗ lực bảo vệ tài sản quốc gia của chúng ta nhưng hiếm khi nhận được lời khen ngợi và thường chỉ được chú ý đến khi có sự cố xảy ra. Đối với bạn, chúng tôi xin nói lời cảm ơn vì bạn đã hoàn thành tốt công việc!

## Về các Tác giả

**Tiến sĩ Wm. Arthur Conklin**, CompTIA Security+, CISSP, GICSP, GRID, GCIP, GCFA, GCIA, GCDA, CSSLP, CRISC, là một giáo sư và giám đốc Trung tâm Nghiên cứu và Giáo dục Bảo mật Thông tin tại Trường Cao đẳng Công nghệ tại Đại học Houston. Ông có hai bằng cấp — một bằng Tiến sĩ về quản trị kinh doanh (đặc biệt chuyên về bảo mật thông tin) của Đại học Texas tại San Antonio (UTSA) và một bằng kỹ sư điện (chuyên về kỹ thuật hệ thống không gian) của Trường Sau đại học Hải quân ở Monterey, California. Ông là thành viên của ISSA và (CS)<sup>2</sup>AI cũng như là thành viên cấp cao của ASQ, IEEE và ACM. Mỗi quan tâm trong nghiên cứu của ông bao gồm việc sử dụng lý thuyết hệ thống để khám phá bảo mật thông tin, đặc biệt là trong các hệ thống mạng-vật lý. Ông đặc biệt quan tâm đến giáo dục an ninh mạng và tham gia vào Trung tâm NSA/DHS về Tài năng Học thuật về Phòng thủ Mạng (Centers of Academic Excellence in Cyber Defense - CAE CD) và Khuôn khổ Lực lượng lao động An ninh mạng (NICE Framework) của Sáng kiến Quốc gia NIST về Giáo dục An ninh mạng (NICE). Ông là đồng tác giả của sáu quyển sách về bảo mật và nhiều bài báo học thuật liên quan đến bảo mật thông tin. Ông cũng là đồng chủ tịch của ban chỉ đạo cho các nỗ lực của Nhóm Công tác Chung về các Hệ thống Kiểm soát Công nghiệp (Industrial Control Systems Joint Working Group - ICSJWG) do DHS tài trợ liên quan đến việc phát triển lực lượng lao động và các khía cạnh an ninh mạng của các hệ thống kiểm soát công nghiệp. Ông có một nền tảng kiến thức sâu rộng về mã hóa bảo mật và đã từng là đồng chủ tịch của Nhóm Làm việc của Diễn đàn Bảo hiểm Phần mềm DHS/DoD về giáo dục, đào tạo và phát triển lực lượng lao động.

**Tiến sĩ Gregory White** đã tham gia vào lĩnh vực bảo mật máy tính và mạng từ năm 1986. Ông đã dành 19 năm làm nhiệm vụ tại ngũ trong Lực lượng Không quân Hoa Kỳ và 11 năm trong Lực lượng Dự bị Không quân

**CompTIA Security+ - All in One - Exam Guide**

20 | Page

với nhiều vị trí liên quan đến máy tính và bảo mật. Ông lấy bằng Tiến sĩ khoa học máy tính tại Đại học A&M Texas vào năm 1995. Đề tài luận văn tiến sĩ của ông là về lĩnh vực phát hiện xâm nhập mạng máy tính, và hiện nay, ông vẫn đang tiếp tục với chủ đề này. Hiện tại, ông đang là giám đốc của Trung tâm Bảo hiểm và Bảo mật Cơ sở hạ tầng (CIAS) và là một giáo sư về khoa học máy tính tại Trường Đại học Texas tại San Antonio (UTSA). Tiến sĩ White đã viết và trình bày nhiều bài báo và tài liệu hội nghị về bảo mật. Ông cũng là đồng tác giả của sáu quyển sách giáo khoa về bảo mật mạng và máy tính và đã viết một số chương cho hai quyển sách về bảo mật khác. Hiện nay, Tiến sĩ White vẫn tiếp tục hoạt động nghiên cứu về bảo mật. Những sáng kiến nghiên cứu hiện tại của ông bao gồm các nỗ lực trong ứng phó các sự cố cộng đồng, phát hiện xâm nhập và chia sẻ thông tin an toàn.

**Chuck Cothren**, CISSP, là một Nhà Quản lý Hoạt động Phát triển tại Bảo mật Ionic, ứng dụng hơn 20 năm kinh nghiệp bảo mật thông tin trong tư vấn, nghiên cứu và môi trường doanh nghiệp. Ông đã hỗ trợ khách hàng trong nhiều ngành khác nhau, bao gồm chăm sóc sức khỏe, ngân hàng, công nghệ thông tin, bán lẻ, và sản xuất. Ông tư vấn cho khách hàng về những chủ đề chẳng hạn như kiến trúc bảo mật, kiểm nghiệm xâm nhập, đào tạo, quản lý tư vấn, ngăn ngừa mất mát dữ liệu và mã hóa. Ông là đồng tác giả của các quyển sách *Voice and Data Security* (tạm dịch *Bảo mật Giọng nói và Dữ liệu*) và *Principles of Computer Security* (tạm dịch *Các Nguyên tắc Bảo mật Máy tính*).

**Roger L. Davis**, CISSP, CISW, CISM, CISA, là Quản lý Kinh doanh Thành công Khách hàng Cấp cao (Senior Customer Success Account Manager) của Microsoft hỗ trợ cho các công ty cấp doanh nghiệp. Ông đã từng là chủ tịch phân hội Utah của Hiệp hội Bảo mật Hệ thống Thông tin (ISSA) và giữ nhiều vị trí trong hội đồng quản trị phân ban Utah của Hiệp hội Kiểm

soát và Kiểm toán Hệ thống Thông tin (ISACA). Ông là một trung tá Không quân đã nghỉ hưu với 40 năm kinh nghiệm về quân sự và hệ thống thông tin/an ninh. Ông cũng từng là giảng viên của Đại học Brigham Young và Học viện Công nghệ Không quân. Ông là đồng tác giả của các quyển sách *Principles of Computer Security* (tạm dịch *Các Nguyên tắc Bảo mật Máy tính*), và *Voice and Data Security* (tạm dịch *Bảo mật Giọng nói và Dữ liệu*) của McGraw-Hill. Ông có bằng thạc sĩ khoa học máy tính của Đại học George Washington, bằng cử nhân khoa học máy tính từ Đại học Brigham Young và thực hiện các nghiên cứu sau đại học về kỹ thuật điện và khoa học máy tính tại Đại học Colorado.

**Dwayne Williams**, CISSP, CASP, là Phó Giám đốc Công nghệ và Nghiên cứu của Trung tâm Bảo đảm VÀ Bảo mật Cơ sở hạ tầng (Center of Infrastructure Assurance and Security - CIAS) tại Đại học Texas ở San Antonio và là Giám đốc của Cuộc thi Phòng thủ Không gian mạng Quốc gia. Ông có hơn 24 năm kinh nghiệm trong lĩnh vực bảo mật hệ thống thông tin và an ninh mạng. Kinh nghiệm của ông bao gồm sáu năm thực hiện nghĩa vụ quân sự với tư cách là Sĩ quan Hệ thống Thông tin Máy tính - Truyền thông của Không quân Hoa Kỳ, đặc biệt là trong lĩnh vực bảo mật mạng, bảo vệ thông tin doanh nghiệp, các hệ thống phát hiện xâm nhập, ứng phó sự cố, và công nghệ VPN. Trước khi tham gia CIAS, ông là Giám đốc Tư vấn của Tập đoàn SecureLogix, nơi ông đã chỉ đạo và cung cấp các dịch vụ đánh giá bảo mật và tích hợp cho các công ty trong danh sách Fortune 100, các chính phủ, tiện ích công, dầu và khí đốt, tài chính, và các khách hàng công nghệ. Ông tốt nghiệp Trường Đại học Baylor năm 1993 với Bằng Cử nhân Khoa học chuyên ngành khoa học máy tính. Ông là một đồng tác giả của các quyển sách và *Voice and Data Security* (tạm dịch *Bảo mật Giọng nói và Dữ liệu*) và *Principles of Computer Security* (tạm dịch *Các Nguyên tắc Bảo mật Máy tính*).

## Về các Biên tập viên Kỹ thuật

**Chris Crayton**, MCSE, là một tác giả, chuyên gia tư vấn kỹ thuật và một nhà đào tạo. Ông đã từng làm việc với tư cách một giảng viên về công nghệ máy tính và mạng, giám đốc bảo mật thông tin, quản trị viên hệ thống mạng, kỹ sư mạng, và chuyên gia máy tính. Chris là tác giả của một vài quyển sách in ấn và trực tuyến về sửa chữa Máy tính, CompTIA A+, CompTIA Security+, và Microsoft Windows. Ông cũng từng là một biên tập viên kỹ thuật và là người đóng góp nội dung cho nhiều đầu sách kỹ thuật cho một số công ty xuất bản hàng đầu. Ông có nhiều chứng chỉ trong ngành, được công nhận với rất nhiều giải thưởng giảng dạy chuyên nghiệp và cũng từng là giám khảo của cuộc thi SkillsUSA cấp tiểu bang.

## Lời mở đầu

An ninh mạng đã dịch chuyển từ giới hạn trong học viện sang xu thế chủ đạo của nước Mỹ. Từ các cuộc tấn công ransomware đến tiết lộ dữ liệu như Equifax và Văn phòng Quản lý Nhân sự Hoa Kỳ được đưa tin rầm rộ trên các phương tiện truyền thông và được phát sóng tại gia đình bình thường người Mỹ, bảo mật thông tin đã trở thành một chủ đề phổ biến. Trong các phòng họp, chủ đề đã đến từ các cuộc tấn công kỹ thuật chống lại quyền sở hữu trí tuệ cho đến nguy cơ rủi ro từ các sự cố an ninh mạng. Càng ngày, mọi người càng thấy rõ rằng điều gì đó cần phải được thực hiện để bảo vệ không chỉ cho cơ sở hạ tầng quan trọng của quốc gia chúng ta mà còn cho những công việc kinh doanh mà chúng ta xử lý hàng ngày. Những vấn đề này đã làm sáng tỏ sự thiếu hụt nghiêm trọng của các chuyên gia an ninh mạng. Câu hỏi là, "Chúng ta bắt đầu từ đâu?" Một chuyên gia công nghệ thông tin trung bình có thể làm gì để bảo mật hệ thống mà họ được thuê để duy trì?

Câu trả lời cho những câu hỏi này rất phức tạp, nhưng một số khía cạnh nhất định có thể hướng dẫn hành động của chúng ta. Đầu tiên, không một ai biết mỗi đe dọa lớn tiếp theo sẽ là gì. APT, ransomware, tiết lộ dữ liệu — tất cả đều là những mối đe dọa đã được biết đến từ lâu trước khi chúng trở thành mối đe dọa của ngày hôm nay. Tiếp theo sẽ là gì? Không ai biết, vì vậy chúng tôi không thể mua một chiếc hộp ma thuật để khắc phục nó. Vẫn chưa. Nhưng chúng tôi biết rằng chúng tôi sẽ làm điều đó với những con người mà chúng tôi có, ở trình độ đào tạo hiện tại của họ, khi nó đến. Một khoản đầu tư mà chúng tôi biết sẽ là khoản đầu tư tốt là vào con người của chúng tôi, thông qua giáo dục và đào tạo, bởi vì đó sẽ là những gì chúng tôi mang đến cho sự cố, vẫn đề, thách thức tiếp theo, hay nói chung là bảo vệ Tổ quốc của chúng tôi trong lĩnh vực

an ninh mạng. Người ta có thể nói an ninh ngày nay bắt đầu và kết thúc với con người của chúng ta, và những người được đào tạo tốt sẽ mang lại những kết quả tốt hơn.

Chà, là một chuyên gia CNTT đang tìm kiếm thêm nhiều kiến thức về bảo mật, bạn sẽ bắt đầu nghiên cứu của bạn từ đâu? Thế giới CNTT đang quá tải với những chứng chỉ có thể có được bởi những ai đang cố gắng học hỏi nhiều hơn về nghề nghiệp mà họ đã lựa chọn. Ngành bảo mật cũng không khác gì mấy, và kỳ thi CompTIA Security+ cung cấp một mức chứng nhận cơ bản về bảo mật. CompTIA Security+ là một điểm khởi đầu lý tưởng cho những ai quan tâm đến một nghề nghiệp trong lĩnh vực bảo mật. Từ trong những trang sách của ấn phẩm này, bạn sẽ tìm thấy không chỉ là tài liệu có thể giúp bạn chuẩn bị để vượt qua kỳ thi CompTIA Security+ mà còn là những thông tin cơ bản mà bạn sẽ cần đến để hiểu được các vấn đề liên quan đến việc bảo mật hệ thống máy tính và mạng của bạn ngày nay. Không có cách nào khác, hướng dẫn kỳ thi này là nguồn cuối cùng để học hỏi tất cả về việc bảo vệ những hệ thống của tổ chức của bạn, mà nó còn đóng vai trò như là một điểm mà từ đó, khởi động những nghiên cứu và nghề nghiệp trong lĩnh vực bảo mật của bạn.

Một điều chắc chắn đúng về lĩnh vực nghiên cứu này là nó sẽ không bao giờ nhảm chán. Nó liên tục thay đổi vì sự tiến bộ của bản thân công nghệ. Một điều gì đó khác mà bạn sẽ nhận thấy khi tiến bộ trong những nghiên cứu về bảo mật của bạn là bắt kể công nghệ tiến bộ đến đâu và bắt kể bao nhiêu thiết bị bảo mật mới được phát triển, ở cấp độ cơ bản nhất, yếu tố con người vẫn là một mắt xích yếu ớt trong chuỗi bảo mật. Nếu bạn đang tìm kiếm một lĩnh vực thú vị để đào sâu thì bạn chắc chắn là đã lựa chọn một cách khôn ngoan. Bảo mật mang lại một sự thách thức pha trộn giữa các vấn đề con người và công nghệ. Chúng tôi, những tác

giả của hướng dẫn kỳ thi này, chúc bạn may mắn khi dấn thân vào con đường sự nghiệp đầy thú vị và thử thách này.

- *Wm. Arthur Conklin, Tiến sĩ khoa học*
- *Gregory B. White, Tiến sĩ khoa học*

## Lời cảm ơn

Chúng tôi, những tác giả của *CompTIA Security+ All-in-One Exam Guide, Sixth Edition* (*Hướng dẫn Kỳ thi CompTIA Security+ Tất cả trong Một, Phiên bản Thứ Sáu*), muốn gửi lời cảm ơn trân trọng đến rất nhiều người, những người mà nếu không có họ thì nỗ lực này của chúng tôi đã không thành công.

Danh sách cần được bắt đầu với những con người ở McGraw Hill, những người đã làm việc một cách không mệt mỏi với nhiều tác giả của dự án và dẫn dắt chúng tôi vượt qua bối mìn một cách thành công, đó là lịch trình của quyển sách, và những người đã lấy các chương và bản vẽ thô của chúng tôi và biến chúng thành sản phẩm cuối cùng một cách chuyên nghiệp mà chúng tôi có thể tự hào về nó. Chúng tôi xin trân trọng cảm ơn những người tốt trong nhóm Mua lại, Tim Green và Emily Walters. Tim đã khiến cho những hành trình này trở nên khả thi và chúng ta mãi mãi mang ơn vì sự tin tưởng và kiên nhẫn của anh ấy. Từ nhóm Dịch vụ Biên tập, chúng tôi xin chân thành cảm ơn Janet Walden và từ nhóm Sản xuất là Thomas Somers. Chúng tôi cũng rất biết ơn biên tập kỹ thuật - Chris Crayton, biên tập dự án - Rachel Fogelberg, biên tập bản sao - Bart Reed, người hiệu đính - Paul Tyler, và người lập chỉ mục - Ted Laux, vì tất cả sự chú ý của họ đến từng chi tiết đã khiến cho tác phẩm này trở thành một tác phẩm tốt hơn sau khi họ hoàn thành nó.

Chúng tôi cũng cần phải công nhận các nhà tuyển dụng hiện tại của mình, những người mà chúng tôi rất vui mừng, đã cảm thấy thích hợp để trả lương cho chúng tôi để làm việc trong một lĩnh vực nghề nghiệp mà tất cả chúng ta đều thấy thú vị và bổ ích. Không bao giờ có bất kỳ thời điểm buồn tẻ trong lĩnh vực bảo mật vì nó liên tục thay đổi.

Chúng tôi muốn cảm ơn Art Conklin vì đã chăm sóc cho bầy mèo, một lần nữa.

Cuối cùng, mỗi chúng tôi muốn gửi lời cảm ơn riêng đến những người — trên cơ sở cá nhân — đã cung cấp sự hỗ trợ cốt lõi cho chúng tôi. Nếu không có những người đặc biệt này trong cuộc sống của chúng tôi, không một ai trong số chúng tôi có thể kết hợp công việc này lại với nhau.

- Nhóm tác giả

Dành cho vợ tôi, Susan: tình yêu và sự ủng hộ của em rất quan trọng đối với những công việc như thế này. Cảm ơn em.

- Art Conklin

Tôi muốn cảm ơn vợ tôi, Charlan, vì sự ủng hộ tuyệt vời mà cô ấy luôn dành cho tôi.

- Gregory B. White

Josie, Macon, và Jet: Xin cảm ơn vì tình yêu, sự hỗ trợ và những nụ cười của các bạn.

- Chuck Cothren

Geena, tất cả những gì tôi có là vì em. Xin cảm ơn vì đã là sự hỗ trợ lớn nhất cho anh. Và như mọi khi, yêu những đứa trẻ mạnh mẽ và những đứa cháu tuyệt vời của tôi.

- Roger L. Davis

Dành cho vợ tôi và người bạn tốt nhất, Leah, vì tình yêu, năng lượng và sự hỗ trợ của cô ấy, cảm ơn vì em đã luôn ở đó. Dành cho các con tôi — đây là những gì mà Bố đang gõ trên máy tính.

- Dwayne Williams

## Giới thiệu

Bảo mật máy tính đã trở nên cực kỳ quan trọng khi số lượng các sự cố bảo mật ngày càng gia tăng dần. Rất nhiều tập đoàn giờ đây đã chi tiêu một phần đáng kể trong ngân sách của họ cho phần cứng, phần mềm, các dịch vụ và nhân viên bảo mật. Họ đang chi tiêu khoản tiền này không chỉ vì nó làm gia tăng doanh số hoặc nâng cao sản phẩm mà họ cung cấp mà còn bởi vì những hệ quả khả dĩ nếu như họ không thực hiện bất kỳ hành động bảo vệ nào.

## Tại sao lại tập trung vào Bảo mật?

Bảo mật không phải là thứ mà chúng ta muốn phải trả tiền cho nó, sẽ thật tuyệt nếu chúng ta không phải lo lắng về việc bảo vệ dữ liệu của mình khỏi việc bị tiết lộ, sửa đổi hoặc phá hủy từ những cá nhân không được phép, nhưng đó không phải là môi trường mà chúng ta đang sống ngày nay. Thay vào đó, chúng tôi đã nhận thấy rằng chi phí khôi phục sau các sự cố an ninh gia tăng đều đặn cùng với số lượng sự cố. Các cuộc tấn công mạng và tiết lộ thông tin xảy ra thường xuyên đến mức người ta gần như đã bỏ qua chúng trên bản tin. Nhưng với việc đánh cắp hơn 145 triệu hồ sơ dữ liệu tín dụng của người tiêu dùng từ Equifax, với sự từ chức sau đó của CSO và Giám đốc điều hành, và các cuộc điều trần tại Quốc hội về vai trò giám sát lập pháp đối với các hồ sơ tối quan trọng, một nhận thức mới về mục đích liên quan đến việc bảo mật dữ liệu có thể nằm trong tầm tay. Thời đại của các báo cáo trên giấy và "dịch vụ môi giới" của công ty có thể đang tàn lụi, và thời điểm để đổi mới với những thách thức mới của những kẻ tấn công thậm chí còn tinh vi hơn nữa đã đến. Đây sẽ không phải là lần vi phạm dữ liệu cuối cùng, cũng như những kẻ tấn công sẽ không ngừng tấn công hệ thống của chúng ta, vì vậy con đường duy nhất của chúng ta về phía trước là nhờ các chuyên gia có đủ năng lực để bảo vệ hệ thống của chúng ta.

## Một Nhu cầu Gia tăng đối với các Chuyên gia Bảo mật

Nhằm bảo vệ các hệ thống máy tính và hệ thống mạng của chúng ta, chúng ta cần một lượng đáng kể các chuyên gia bảo mật mới đã được đào tạo về nhiều khía cạnh của bảo mật máy tính và mạng. Đây không phải là một nhiệm vụ dễ dàng, khi các hệ thống kết nối tới Internet ngày càng trở nên phức tạp cùng với những phần mềm lên đến hàng triệu dòng mã lập trình. Việc hiểu được nguyên nhân tại sao đây lại là một vấn đề rất khó giải quyết không phải là quá khó nếu như bạn chỉ xem xét xem có bao nhiêu lỗi có thể hiện diện trong một mảnh của phần mềm dài hàng triệu dòng lệnh. Khi bạn bổ sung thêm yếu tố về tốc độ phát triển phần mềm – do nhu cầu, vì thị trường đang liên tục thay đổi – việc hiểu được bao nhiêu lỗi xảy ra là điều dễ dàng.

Không phải tất cả các “bug” trong phần mềm đều sẽ dẫn đến một lỗ hổng bảo mật, tuy nhiên, không cần phải có quá nhiều lỗ hổng để có ảnh hưởng mạnh mẽ đến cộng đồng Internet. Chúng ta không thể chỉ đổ lỗi cho các nhà cung cấp về tình huống này, bởi vì họ đang phải ứng phó với các yêu cầu của chính phủ và của ngành. Rất nhiều nhà cung cấp khá thành thạo trong việc phát triển các bản vá cho các lỗi được tìm thấy trong phần mềm của họ và các bản vá liên tục được phát hành để bảo vệ hệ thống khỏi các lỗi có thể gây ra các vấn đề bảo mật. Điều này nêu ra một vấn đề hoàn toàn mới cho người quản lý và quản trị viên — quản lý bản vá. Việc này trở nên quan trọng như thế nào có thể được minh họa một cách dễ dàng bằng cách có bao nhiêu sự kiện bảo mật gần đây nhất đã xảy ra do lỗi bảo mật từng được phát hiện từ vài tháng trước sự cố bảo mật và bản vá đã có sẵn nhưng cộng đồng đã không cài đặt nó một cách đúng đắn, do đó khiến cho sự cố trở nên khả dĩ. Có rất nhiều lý do cho những thất bại này, nhưng cuối cùng, giải pháp là vẫn đề về các chuyên gia được đào tạo ở nhiều cấp trong một tổ chức làm việc cùng nhau để giải quyết những vấn đề này.

Nhưng vấn đề về những con người được đào tạo không chỉ dừng lại ở các chuyên gia bảo mật. Mỗi người dùng, từ phòng họp cho đến phòng thư tín đều đóng một vai trò trong thế trận an ninh mạng của một công ty. Việc huấn luyện nhân viên không chuyên về bảo mật trong doanh nghiệp sử dụng mức độ cẩn thận thích hợp khi tương tác với các hệ thống cũng sẽ không làm cho vấn đề biến mất, nhưng về cơ bản nó sẽ củng cố vị thế của doanh nghiệp. Việc hiểu được khóa đào tạo cần thiết và biến nó thành hiện thực là một nhiệm vụ khác nữa trong danh sách những việc cần làm của chuyên gia bảo mật.

Do nhu cầu ngày càng tăng đối với số lượng các chuyên gia bảo mật được đào tạo ở mức độ hiểu biết tối thiểu, các chứng chỉ như CompTIA Security+ đã được phát triển. Những người sử dụng lao động tương lai muốn biết rằng cá nhân mà họ đang cân nhắc tuyển dụng biết được họ phải làm gì xét về mặt bảo mật. Những nhân viên tương lai, ngược lại, muốn có một cách thức để minh chứng cho mức độ hiểu biết của họ, vốn có thể tăng cường cơ hội được thuê của ứng viên. Toàn thể cộng đồng chỉ đơn giản là muốn có thêm nhiều chuyên gia bảo mật được đào tạo hơn nữa.

Mục đích của việc tham gia kỳ thi CompTIA Security+ là để chứng minh rằng bạn đã nắm vững các tiêu chuẩn trên toàn thế giới dành cho những người hành nghề bảo mật cấp cơ sở. Kỳ thi sẽ mang đến cho bạn một cơ hội hoàn hảo để xác minh kiến thức và hiểu biết của bạn về lĩnh vực bảo mật máy tính, và đây là một cơ chế thích hợp cho nhiều cá nhân khác nhau, bao gồm quản trị viên mạng và hệ thống, chuyên gia phân tích, lập trình viên, nhà thiết kế web, nhà phát triển ứng dụng và chuyên gia cơ sở dữ liệu, để trình bày bằng chứng về thành tích chuyên nghiệp trong lĩnh vực bảo mật. Theo CompTIA, kỳ thi hướng đến những cá nhân có:

- Tối thiểu hai năm kinh nghiệm trong quản trị CNTT tập trung vào bảo mật,
- Kinh nghiệm bảo mật thông tin kỹ thuật hàng ngày,
- Kiến thức rộng về các mối quan tâm và triển khai bảo mật, bao gồm những chủ đề được tìm thấy trong các lĩnh vực CompTIA Security + cụ thể.

Các mục tiêu của kỳ thi đã được phát triển với sự đóng góp và hỗ trợ từ các cơ quan trong ngành và cơ quan chính phủ. Kỳ thi CompTIA Security+ được thiết kế để bao hàm một loạt các chủ đề về bảo mật - các chủ đề mà một người hành nghề bảo mật sẽ phải biết. Bài kiểm tra bao gồm thông tin từ năm lĩnh vực kiến thức sau:

Lĩnh vực	Tỷ lệ phần trăm trong Kỳ thi
1.0 Các Mối đe dọa, các Cuộc tấn công, và những Lỗi hổng	24%
2.0 Kiến trúc và Thiết kế	21%
3.0 Triển khai	25%
4.0 Vận hành và Ứng phó Sự cố	16%
5.0 Quản trị, Rủi ro, và Tuân thủ	14%

Kỳ thi được cấu thành từ một loạt các câu hỏi, mỗi câu hỏi được thiết kế để có một đáp án hoặc phản hồi tốt nhất. Những lựa chọn sẵn có khác được thiết kế để cung cấp các tùy chọn mà một cá nhân có thể chọn nếu thí sinh đã có một kiến thức hoặc hiểu biết không hoàn chỉnh về chủ đề bảo mật được trình bày trong câu hỏi. Kỳ thi sẽ có cả những câu hỏi nhiều lựa chọn lẫn những câu hỏi dựa trên-hiệu suất. Những câu hỏi dựa trên

hiệu suất đưa ra cho thí sinh một nhiệm vụ hoặc một vấn đề trong một môi trường CNTT được mô phỏng. Thí sinh được cung cấp một cơ hội để chứng minh khả năng của họ trong việc thực hiện các kỹ năng. Những câu hỏi trong đề thi được căn cứ vào tài liệu "Những Mục tiêu Kỳ thi Chứng nhận CompTIA Security+: SY0-601" có thể có được từ trang web của CompTIA tại địa chỉ URL sau đây: <https://certification.comptia.org/certifications/security>.

CompTIA khuyến nghị rằng những cá nhân muốn tham gia kỳ thi CompTIA Security+ phải có chứng chỉ CompTIA Network+ và hai năm kinh nghiệm quản trị CNTT với một sự tập trung vào lĩnh vực bảo mật. Ban đầu chỉ được tổ chức bằng tiếng Anh, kỳ thi giờ đây hiện được cung cấp tại các trung tâm khảo thí trên toàn thế giới bằng tiếng Anh, Nhật, Bồ Đào Nha và tiếng Trung Giản thể. Tham khảo thêm trang web của CompTIA tại địa chỉ [www.comptia.org](http://www.comptia.org) để định vị trung tâm khảo thí gần bạn nhất.

Kỳ thi bao gồm tối đa 90 câu hỏi cần phải được hoàn thành trong vòng 90 phút. Điểm tối thiểu để vượt qua kỳ thi là 750/900. Kết quả sẽ có ngay lập tức sau khi bạn hoàn thành bài thi. Một cá nhân không vượt qua được kỳ thi trong lần đầu tiên sẽ được yêu cầu trả thêm chi phí để thực hiện lại bài thi, nhưng không cần phải có thời gian chờ bắt buộc trước khi thi lại lần thứ hai. Nếu một cá nhân vẫn tiếp tục không đạt, một khoảng thời gian chờ tối thiểu 30 ngày sẽ được yêu cầu cho mỗi lần thi lại tiếp theo. Để biết thêm thông tin về việc thi lại, vui lòng tham khảo chính sách thi lại của CompTIA, vốn có thể được tìm thấy trên trang web của CompTIA.

### **Chuẩn bị cho Kỳ thi CompTIA Security+**

*Hướng dẫn Kỳ thi CompTIA Security+ Tất cả Trong Một, Phiên bản Thứ Sáu*, được thiết kế để giúp bạn chuẩn bị cho kỳ thi chứng nhận CompTIA Security+ SY0-601.

## Quyển sách này Được Tổ chức Như thế nào

Quyển sách này được chia thành các phần và các chương để phù hợp với các mục tiêu của bản thân kỳ thi. Một vài trong số các chương mang tính kỹ thuật hơn các chương khác – phản ảnh bản chất của môi trường bảo mật, nơi mà bạn sẽ bị bắt buộc phải xử lý không chỉ những chi tiết kỹ thuật mà còn cả các vấn đề khác chẳng hạn như các chính sách và thủ tục bảo mật cũng như là giáo dục và đào tạo. Mặc dù có rất nhiều cá nhân liên quan đến bảo mật mạng và máy tính có những bằng cấp nâng cao về toán học, khoa học máy tính, hệ thống thông tin, hoặc kỹ sư máy tính hoặc kỹ sư điện nhưng bạn không nhất thiết phải có nền tảng kỹ thuật để giải quyết những vấn đề bảo mật trong tổ chức của bạn một cách có hiệu quả. Ví dụ, bạn không cần phải tự phát triển thuật toán mã hóa của riêng bạn, bạn đơn giản chỉ cần có khả năng hiểu được cách mã hóa được sử dụng như thế nào, cùng với những điểm mạnh và điểm yếu của nó. Khi bạn tiến bộ trong nghiên cứu của bạn, bạn sẽ học được rằng có rất nhiều vấn đề về bảo mật gây ra bởi các yếu tố con người. Công nghệ tốt nhất trên thế giới cuối cùng vẫn phải được đưa vào một môi trường nơi con người có cơ hội để làm hỏng mọi thứ - và rất thường xuyên.

Như bạn có thể thấy từ mục lục, cấu trúc tổng thể của quyển sách được thiết kế để phản chiếu những mục tiêu của kỳ thi CompTIA Security+. Phần lớn các chương được thiết kế để khớp với thứ tự của các mục tiêu như đã được đăng bởi CompTIA. Cấu trúc này đã được sử dụng để khiến cho việc tìm kiếm những nội dung cụ thể dựa trên mục tiêu trở nên dễ dàng hơn. Khi nghiên cứu về những chủ đề nhất định, bạn có thể được yêu cầu để đi đến một vài nơi trong quyển sách này để có thể bao hàm toàn bộ một chủ đề có nhiều mục tiêu.

Ngoài ra, có hai phụ lục trong quyển sách này. [Phụ lục A](#) cung cấp một giải thích bổ sung sâu hơn về Mô hình OSI và các giao thức Internet, và nếu những thông tin này là mới mẻ đối với bạn, và [Phụ lục B](#) giải thích thêm về cách tốt nhất để sử dụng những tài liệu trực tuyến được đưa ra trong quyển sách này.

Được định vị ngay trước phần Chỉ mục, bạn sẽ tìm thấy một Chú giải thuật ngữ hữu ích về những thuật ngữ bảo mật, bao gồm rất nhiều từ viết tắt có liên quan và ý nghĩa của chúng. Chúng tôi hy vọng rằng bạn sử dụng Chú giải thuật ngữ một cách thường xuyên và nhận thấy rằng nó là một công cụ hỗ trợ nghiên cứu hữu ích khi bạn làm việc theo cách của mình thông qua các chủ đề khác nhau trong hướng dẫn kỳ thi này.

## **Những Tính năng Đặc biệt của chuỗi [ấn phẩm] Tất cả trong Một**

Để khiến cho hướng dẫn kỳ thi này hữu ích hơn và thoải mái hơn khi đọc, chuỗi [ấn phẩm] *Tất cả trong Một* đã được thiết kế để bao gồm một vài tính năng.

### **Bản đồ Mục tiêu**

Bản đồ mục tiêu tiếp theo sau phần giới thiệu này đã được xây dựng để cho phép bạn tham khảo chéo các mục tiêu kỳ thi chính thức với các mục tiêu khi chúng được trình bày và đề cập trong ấn phẩm này. Những tham chiếu đã được cung cấp cho từng mục tiêu một cách chính xác như CompTIA đã trình bày nó, cùng với một tham chiếu chương.

### **Các Biểu tượng**

Để cảnh báo bạn về một lời khuyên quan trọng, một lỗi tắt, hoặc một cạm bẫy, và bạn sẽ thỉnh thoảng trông thấy [biểu tượng] LƯU Ý, Mách nước, Cảnh báo và MÁCH NƯỚC CHO KỲ THI rải rác xuyên suốt các đoạn văn bản.



## LƯU Ý

Những LƯU Ý cung cấp những thông tin đặc biệt hữu ích, những giải thích cơ bản, và những thông tin, và đôi khi chúng xác định các thuật ngữ.



## MÁCH NƯỚC

Những MÁCH NƯỚC đưa ra những gợi ý và sắc thái để giúp bạn học hỏi để khéo léo trong công việc của bạn. Hãy nhận những mách nước từ chúng tôi và đọc chúng một cách cẩn thận.



## CẢNH BÁO

Khi bạn nhận ra một biểu tượng CẢNH BÁO, hãy đặc biệt lưu tâm đến chúng. Các Cảnh báo xuất hiện khi bạn đưa ra một lựa chọn tối quan trọng hoặc khi bạn đang chuẩn bị thực hiện một việc gì đó có thể rẽ nhánh mà bạn có thể không dự đoán được ngay lập tức. Hãy đọc chúng để bạn không phải hối tiếc sau đó.



## MÁCH NƯỚC CHO KỲ THI

Các MÁCH NƯỚC CHO KỲ THI đưa ra cho bạn những lời khuyên đặc biệt hoặc có thể cung cấp những thông tin đặc biệt liên quan đến việc chuẩn bị cho bản thân kỳ thi.

### Cuối Chương - Các Câu hỏi và Đánh giá

Một phần quan trọng của quyển sách này nằm ở cuối mỗi chương, nơi bạn sẽ tìm thấy một đánh giá tóm tắt về những điểm quan trọng cùng với một loạt các câu hỏi, và tiếp theo là những đáp án cho các câu hỏi đó. Mỗi câu hỏi đều có định dạng nhiều đáp án. Câu trả lời được đưa ra cũng sẽ bao gồm một giải thích ngắn gọn về lý do tại sao câu trả lời đúng là câu trả lời đúng trên thực tế.

Những câu hỏi được đưa ra như là một công cụ hỗ trợ nghiên cứu cho bạn, cho độc giả và những thí sinh CompTIA Security+ trong tương lai. Chúng tôi rõ ràng không thể đảm bảo rằng nếu bạn trả lời được tất cả những câu hỏi của chúng tôi thì bạn chắc chắn sẽ vượt qua được kỳ thi chứng nhận. Thay vào đó, chúng tôi có thể đảm bảo rằng những câu hỏi sẽ mang lại cho bạn một ý tưởng về mức độ sẵn sàng của bạn cho kỳ thi.

### Security+ Danh sách Phần mềm và Phần cứng được Đề xuất

CompTIA cung cấp một danh sách mẫu này về những phần cứng và phần mềm trong mô tả Mục tiêu Kỳ thi của mình để giúp cho các thí sinh khi họ chuẩn bị cho kỳ thi Security+. Vì các tài liệu bao gồm những phần tử đòi hỏi năng lực thực hành nên sẽ rất hữu ích khi xây dựng một kỹ năng thí nghiệm và thực hành thực tiễn như là một phần của quá trình học tập. Danh sách được gạch đầu dòng dưới từng chủ đề là các danh sách mẫu và không phải là một danh sách toàn diện.

## Phần cứng

- Máy tính xách tay truy cập Internet,
- Thẻ truy cập mạng (network access card) không dây tách biệt,
- Điểm truy cập không dây (WAP),
- Tường lửa,
- Giám sát mối đe dọa được hợp nhất (UTM),
- Máy chủ/Máy chủ đám mây,
- Thiết bị Internet Vạn vật (IoT).

## Phần mềm

- Phần mềm ảo hóa,
- Hệ điều hành/bản phân phôi kiểm nghiệm xâm nhập (ví dụ, Kali Linux, Parrot OS),
- Quản lý sự kiện và thông tin bảo mật (SIEM),
- Wireshark,
- Metasploit,
- Tcpdump.

## Khác

- Truy cập tới một nhà cung cấp dịch vụ đám mây.

## TotalTester Trực tuyến

*Hướng dẫn Kỳ thi CompTIA Security+ Tất cả trong Một, Phiên bản Thứ Sáu* cũng cung cấp cho bạn một công cụ kiểm tra còn chứa nhiều câu hỏi thực tiễn hơn và những đáp án của chúng sẽ giúp bạn chuẩn bị tốt hơn cho kỳ thi. Hãy đọc thêm về phần mềm kiểm tra trực tuyến đồng hành và cách đăng ký và truy cập bài thi của bạn trong [Phụ lục B](#).

## Tiến lên và Đi tới

Đến thời điểm này, chúng tôi hy vọng bạn hiện đã hào hứng với chủ đề về bảo mật, ngay cả khi bạn đã không thích chủ đề này ngay từ ban đầu.

Chúng tôi chúc bạn may mắn trong những nỗ lực của mình và chào đón bạn đến với lĩnh vực đầy phẩn khích về bảo mật mạng và máy tính.

## Bản đồ Mục tiêu: Kỳ thi SY0-601

Các Lĩnh vực và Mục tiêu Kỳ thi Chính thức	Chương bao hàm trong Tất cả trong Một
<b>1.0 Các Mối đe dọa, các Cuộc tấn công và các Lỗ hổng</b>	
1.1 So sánh và đối chiếu các kiểu kỹ thuật kỹ thuật xã hội khác nhau	1
1.2 Đưa ra một kịch bản, phân tích các chỉ báo tiềm năng để xác định kiểu tấn công	2
1.3 Đưa ra một kịch bản, phân tích các chỉ báo tiềm năng tương ứng với các cuộc tấn công ứng dụng	3
1.4 Đưa ra một kịch bản, phân tích các chỉ báo tiềm năng tương ứng với các cuộc tấn công mạng	4
1.5 Giải thích về các tác nhân, véc-tơ và nguồn tình báo khác nhau	5
1.6 Giải thích về những mối quan tâm về bảo mật tương ứng với các kiểu lỗ hổng khác nhau	6
1.7 Tóm tắt về những kỹ thuật được sử dụng trong đánh giá bảo mật	7
1.8 Giải thích về các kỹ thuật khác nhau được sử dụng trong kiểm nghiệm xâm nhập	8

<b>2.0 Kiến trúc và Thiết kế</b>	
2.1 Giải thích về tầm quan trọng của các khái niệm về bảo mật trong một môi trường doanh nghiệp	9
2.2 Tóm tắt các khái niệm về ảo hóa và điện toán đám mây	10
2.3 Tóm tắt về các khái niệm phát triển, triển khai và tự động hóa ứng dụng an toàn	11
2.4 Tóm tắt về các khái niệm thiết kế xác thực và cấp phép	12
2.5 Đưa ra một kịch bản, triển khai khả năng phục hồi an ninh mạng	13
2.6 Giải thích về hàm ý bảo mật của các hệ thống nhúng và hệ thống chuyên biệt	14
2.7 Giải thích về tầm quan trọng của các biện pháp kiểm soát bảo mật vật lý	15
2.8 Tóm tắt về các khái niệm mã hóa cơ bản	16
<b>3.0 Triển khai</b>	
3.1 Đưa ra một kịch bản, triển khai các giao thức bảo mật	17
3.2 Đưa ra một kịch bản, triển khai các giải pháp bảo mật ứng dụng hoặc bảo mật máy vật chủ	18

3.3 Đưa ra một kịch bản, triển khai bảo mật thiết kế mạng	19
3.4 Đưa ra một kịch bản, cài đặt và thiết lập cấu hình các thiết lập bảo mật không dây	20
3.5 Đưa ra một kịch bản, triển khai các giải pháp bảo mật di động	21
3.6 Đưa ra một kịch bản, áp dụng các giải pháp an ninh mạng cho đám mây	22
3.7 Đưa ra một kịch bản, triển khai các biện pháp kiểm soát quản lý nhân dạng và tài khoản	23
3.8 Đưa ra một kịch bản, triển khai các giải pháp xác thực và cấp phép	24
3.9 Đưa ra một kịch bản, triển khai cơ sở hạ tầng khóa công khai	25
<b>4.0 Vận hành và Ứng phó Sự cố</b>	
4.1 Đưa ra một kịch bản, sử dụng các công cụ thích hợp để đánh giá mức độ bảo mật của tổ chức	26
4.2 Tóm tắt về tầm quan trọng của các chính sách, quy trình và thủ tục ứng phó sự cố	27
4.3 Đưa ra một sự cố, sử dụng các nguồn dữ liệu thích hợp để hỗ trợ cho một cuộc điều tra	28
4.4 Đưa ra một sự cố, áp dụng các kỹ thuật hoặc biện pháp kiểm soát giảm nhẹ để bảo vệ môi trường	29

4.5 Giải thích về các khía cạnh then chốt của điều tra pháp y kỹ thuật số	30
<b>5.0 Quản trị, Rủi ro và Tuân thủ</b>	
5.1 So sánh và đối chiếu các kiểu kiểm soát khác nhau	31
5.2 Giải thích về tầm quan trọng của các quy định, tiêu chuẩn hoặc khuôn khổ có thể áp dụng được có tác động đến tình huống bảo mật của tổ chức	32
5.3 Giải thích về tầm quan trọng của các chính sách đối với bảo mật của tổ chức	33
5.4 Tóm tắt về các quy trình và khái niệm quản lý rủi ro	34
5.5 Giải thích về các khái niệm quyền riêng tư và dữ liệu nhạy cảm trong mối tương quan với bảo mật	35

## **Giới thiệu sơ lược về Nhóm dịch ASV**

Nhóm dịch Bảo mật và Quản trị Mạng hiện tại đang bao gồm một số thành viên hiện đang công tác trong lĩnh vực CNTT như sau:

### **Đỗ Thượng Điện (Hà Nội)**

- ✓ Công việc hiện tại: Quản trị Hệ thống,
- ✓ Đơn vị: Công ty CP CNTT New Vision,
- ✓ Điểm mạnh:
  - Quản lý hệ thống máy chủ Linux, Windows,
  - Triển khai và quản lý hệ thống SQLServer, MariaDB, Postgres, Haproxy, Nginx và Elasticsearch,
  - Giám sát các hệ thống Zabbix, Prometheus, ELK.

### **Nguyễn Văn Thắng (Hà Nội)**

- ✓ Công việc hiện tại: Kỹ sư hệ thống,
- ✓ Đơn vị: Công ty 3C JSC,
- ✓ Điểm mạnh:
  - Triển khai các Dự án Tích hợp hệ thống,
  - Triển khai các hệ thống máy chủ Linux, lưu trữ, sao lưu vàảo hóa VMWare.

### **Mai Thành Việt (Hà Nội)**

- ✓ Công việc hiện tại: Cán bộ kỹ thuật Phòng Dự án,
- ✓ Đơn vị: Công ty TNHH Điện tử Tin học EI,
- ✓ Điểm mạnh:
  - Cẩn thận và chu đáo trong công việc.
  - Các dự án lưu trữ lớn trên nền tảng IBM.

### **Phan Văn Sáng (Hà Nội)**

- ✓ Công việc hiện tại: Tổng Giám đốc,
- ✓ Đơn vị: Công ty ITSUPRO,

✓ Điểm mạnh:

- Tư vấn triển khai hệ thống mạng,
- Dịch vụ IT Outsourcing cho doanh nghiệp,
- Hỗ trợ sự cố người dùng đầu cuối.

### **Nguyễn Sơn Tùng (Tp. Hồ Chí Minh)**

- ✓ Công việc hiện tại: Quản lý Phòng Tư vấn giải pháp,
- ✓ Đơn vị: Digital Work Network,
- ✓ Điểm mạnh:
  - Thiết kế và tư vấn các giải pháp Cisco Meraki và SD-WAN.

### **Nguyễn Thành Đông (Tp. Hồ Chí Minh)**

- ✓ Công việc hiện tại: Team Leader,
- ✓ Đơn vị: Công ty TNHH Chứng khoán Yuanta Việt Nam,
- ✓ Điểm mạnh:
  - Chuyên môn chính về phần mềm (có thể lập trình, thiết kế DB);
  - Khả năng nắm bắt nhanh về nghiệp vụ hệ thống (như : core chứng khoán (BOSC, AFE, TTL, FW), core finance);
  - Chịu khó học hỏi, có kiến thức cơ bản về hệ thống (Network, Firewall, AD, SAN, VMWare, v.v...).

### **Phạm Hoàng Minh (Tp. Hồ Chí Minh)**

- ✓ Công việc hiện tại: IT Manager,
- ✓ Đơn vị: Công ty SOFACOMPANY VIETNAM,
- ✓ Điểm mạnh:
  - Triển khai, vận hành, quản lý hạ tầng CNTT
  - Quản lý các nhà cung cấp dịch vụ CNTT
  - Biên soạn và xuất bản các chính sách CNTT
  - Quản lý nguồn ngân sách CNTT,

### **Trần Sơn Hải (Tp. Hồ Chí Minh)**

- ✓ Công việc hiện tại: IT Manager,
- ✓ Đơn vị: Công ty Discovery Loft,
- ✓ Điểm mạnh:
  - Quản lý Dự án CNTT,
  - IT Help Desk.

### **Nguyễn Thế Hùng (Tp. Hồ Chí Minh)**

- ✓ Công việc hiện tại: Giám đốc CNTT,
- ✓ Đơn vị: Công ty Luật Frasers,
- ✓ Điểm mạnh:
  - Quản lý và Thiết kế doanh nghiệp;
  - Định hướng và Đào tạo;
  - Quản lý Dự án với OKRs.

## PHẦN I

### Các Mối đe dọa – các Cuộc tấn công và các Lỗi hổng

- Chương 1 Các Kỹ thuật Kỹ thuật Xã hội
- Chương 2 Các Kiểu Chỉ báo Tấn công
- Chương 3 Các Chỉ báo Tấn công Ứng dụng
- Chương 4 Các Chỉ báo Tấn công Mạng
- Chương 5 Các Tác nhân, Véc-tơ và Nguồn Tình báo về Mối đe dọa
- Chương 6 Các Lỗi hổng
- Chương 7 Đánh giá Bảo mật
- Chương 8 Kiểm nghiệm Xâm nhập

## Chương 1      Các Kỹ thuật Kỹ thuật Xã hội (Tấn công phi kỹ thuật)

### Các Kỹ thuật Kỹ thuật Xã hội (Tấn công phi kỹ thuật)

Trong chương này, bạn sẽ:

- Xem xét các kiểu tấn công tương ứng với kỹ thuật xã hội,
- So sánh và đối chiếu các kỹ thuật kỹ thuật xã hội khác nhau.

Kỹ thuật xã hội là một phương pháp sử dụng con người như là một phần của quá trình tấn công. Kỹ thuật xã hội chỉ là một bước trong quá trình tấn công tổng thể, nhưng đó là một cách rất hiệu quả để bắt đầu một cuộc tấn công vào một hệ thống. Có rất nhiều hình thức tấn công kỹ thuật đối với các thành phần máy tính của một hệ thống, nhưng trong mỗi trường hợp, luôn có một điểm khởi đầu mà tại đó cuộc tấn công xảy ra với hệ thống. Trong chương này, chúng ta sẽ kiểm tra các kiểu kỹ thuật kỹ thuật xã hội khác nhau có thể được sử dụng để bắt đầu một chu trình tấn công.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 1.1 của kỳ thi CompTIA Security+: So sánh và đối chiếu các kiểu kỹ thuật kỹ thuật xã hội.

## Các Phương pháp Kỹ thuật Xã hội (Tấn công Phi kỹ thuật)

Kỹ thuật xã hội là một cuộc tấn công vào một người dùng, và thường liên quan đến một số hình thức tương tác xã hội. Điểm yếu sẽ bị khai thác trong cuộc tấn công không nhất thiết là một điểm yếu về kiến thức kỹ thuật hoặc thậm chí là nhận thức về bảo mật. Trọng tâm của kỹ thuật xã hội liên quan đến việc thao túng bản chất rất xã hội của các mối quan hệ qua lại lẫn nhau giữa các cá nhân. Về bản chất, nó (kỹ thuật xã hội) ưa thích một số đặc trưng mà chúng ta có khuynh hướng mong muốn. Ví dụ, sự sẵn lòng giúp đỡ [người khác] là một đặc điểm mà người ta muốn nhìn thấy trong một môi trường đội nhóm. Chúng ta mong muốn những nhân viên giúp đỡ lẫn nhau, và chúng ta có khuynh hướng khen thưởng những người hữu ích và trừng phạt những ai không có ích.

Nếu văn hóa làm việc của chúng ta được xây dựng xoay quanh sự cộng tác và làm việc nhóm thì làm thế nào mà việc này có thể được khai thác? Không đơn giản, nhưng nó có thể được hoàn thành thông qua một loạt các thủ đoạn tinh vi. Một trong số đó được xây dựng xoay quanh ý tưởng về việc phát triển một ý thức về sự quen thuộc – khiến cho bạn trông có vẻ như đang thuộc về nhóm. Ví dụ, bằng cách tự đưa bản thân vào một cuộc hội thoại hoặc gấp gỡ, được trang bị những từ ngữ phù hợp và thông tin chính xác, bạn có thể khiến cho nó trông có vẻ như đang thuộc về bạn. Thông qua việc đặt tên cẩn thận và liên kết câu chuyện của bạn với các sự kiện và kỳ vọng hiện tại, bạn có thể lọt vào danh sách không gây ra sự chú ý. Một ví dụ khác là bằng cách đến cửa cùng lúc với một người có thẻ căn cước, và bê một thứ gì đó trong cả hai tay, bạn có thể nhờ họ mở và giữ cửa cho bạn. Một kỹ thuật thậm chí thành công hơn nữa là có một cuộc trò chuyện trên đường đi đến cửa về một điều gì đó khiến bạn có vẻ phù hợp. Mọi người đều muốn giúp đỡ và chiến thuật này khuyến khích người đó giúp đỡ bạn.

Một phương pháp thứ hai liên quan đến việc tạo ra một tình huống thù địch. Mọi người đều có khuynh hướng muốn tránh sự thù địch, vì vậy, nếu bạn đang tham gia vào một cuộc tranh cãi nảy lửa với ai đó khi bạn vào nhóm mà bạn muốn tham gia - đảm bảo rằng bạn không đang chỉ thua trong cuộc tranh luận, mà còn có vẻ hoàn toàn không công bằng — bạn ngay lập tức có thể xây dựng một kết nối với bất kỳ ai từng chịu sự ngược đãi tương tự. Chơi dựa trên sự cảm thông [của mọi người], mong muốn sự từ bi của họ, và sử dụng tình huống để bỏ qua cơ hội kết nối.

Một kỹ sư xã hội giỏi hiểu cách sử dụng ngôn ngữ cơ thể để gây ảnh hưởng đến người khác - cách mỉm cười đúng lúc, cách phản chiếu những chuyển động, cách gây ảnh hưởng đến người khác không phải bằng lời nói mà thông qua tín hiệu ngôn ngữ của cơ thể. Bất kỳ người phụ nữ nào đã sử dụng ngôn ngữ cơ thể để yêu cầu một người đàn ông làm điều gì đó mà không trực tiếp yêu cầu anh ta làm điều đó hiểu trò chơi này. Đàn ông cũng hiểu, và họ chơi vì họ cũng đang cố gắng đạt được thứ gì đó. Khi ai đó có thông tin quan trọng mà bạn cần cho một dự án, một đề xuất hoặc bất kỳ thứ quan trọng nào khác, giao dịch một vật gì đó để bồi thường là một nghi thức bắt thành văn. Và nếu bạn làm điều này với một người có ý định xấu, thì hãy nhớ câu nói, "Hãy coi chừng người Hy Lạp mang quà tặng" (*có lẽ hàm ý chỉ câu chuyện người Hy Lạp tặng Ngựa gỗ cho thành Troia/Trojan*).



**LƯU Ý** Phần lớn kỹ thuật xã hội sẽ ảnh hưởng đến hành vi mang tính khuôn mẫu đã biết. Việc nêu chi tiết tài liệu này không nhằm mục đích biện minh cho những hành vi, vì trong thực tế chúng rõ ràng là sai. Nhưng điều quan trọng là phải theo dõi chúng, vì đây là những công cụ được sử dụng bởi những kỹ thuật xã hội — những đứa trẻ đang khóc, sự tán tỉnh,

ẩn mình ở chỗ dễ thấy (người trông cửa, tưới cây hoặc người giao bánh pizza). Chúng ta đều bị bịt mắt bởi những thành kiến và bởi điều kiện, và những kỹ thuật xã hội biết và khai thác được những điểm yếu này. Và nếu bị chỉ trích về hành vi của họ, họ thậm chí sẽ tiếp tục với điều đó và phản kháng quá nhiều hoặc đồng ý quá nhiều – bất kỳ điều gì để chiến thắng một người khác. Đừng trở thành những người đó – người sử dụng khuôn mẫu hoặc trở thành con mồi cho họ.

Biện pháp phòng thủ tốt nhất để chống lại kỹ thuật xã hội là một chương trình đào tạo và nâng cao nhận thức toàn diện bao gồm cả kỹ thuật xã hội, nhưng điều này không có nghĩa là nhân viên nên được đào tạo để trở nên cứng đầu và vô ích. Thay vào đó, việc đào tạo nên nhấn mạnh vào giá trị của việc trở nên hữu ích và làm việc như một nhóm nhưng chỉ làm thế trong một môi trường nơi sự tin tưởng đã được kiểm chứng và là một nghi thức không có sự kỳ thị xã hội. Không một ai có thể qua mặt được các nhân viên Quản lý An ninh Vận tải (Transportation Security Administration – TSA) với các kỹ thuật xã hội khi làm thủ tục tại sân bay, vì họ luôn thực thi và tuân thủ các thủ tục đã được đặt ra một cách bình thản, nhưng họ thường làm thế với sự tử tế, lịch sự và hữu ích trong khi vẫn đảm bảo rằng các thủ tục sàng lọc luôn được hoàn thành.



**MÁCH NƯỚC CHO KỲ THI** Ví dụ, hãy làm quen với mọi cuộc tấn công kỹ thuật xã hội khác nhau và tính hiệu quả tương ứng với từng cuộc tấn công.

### Các Công cụ

Các công cụ trong một hộp công cụ kỹ thuật xã hội đều dựa trên kiến thức về tâm lý và không nhất thiết đòi hỏi một kiến thức tinh vi về phần mềm hoặc phần cứng. Kỹ thuật xã hội sẽ sử dụng các chiến lược nhằm

khai thác những định kiến và niềm tin của chính bản thân mọi người theo cách từ chối ngay lập tức sự phán đoán tốt và việc sử dụng các thủ tục tiêu chuẩn. Việc sử dụng các công cụ kỹ thuật xã hội là bản chất thứ hai đối với một kỹ sư xã hội, và cùng với kỹ năng, họ có thể chuyển các công cụ này vào và ra trong bất kỳ tình huống cụ thể nào, giống như một thợ sửa ống nước sử dụng các công cụ cầm tay khác và một quản trị viên hệ thống sử dụng các câu lệnh của Hệ điều hành để hoàn thành các tác vụ phức tạp. Khi quan sát bất kỳ chuyên gia nào trong số này làm việc, chúng ta có thể thấy làm lại về cách họ vận dụng các công cụ của họ, và điều tương tự cũng đúng với các kỹ sư xã hội – ngoại trừ việc các công cụ của họ tinh vi hơn, và các đích nhắm mục tiêu thường là con người và sự tin tưởng. “Các Kỹ thuật” phổ biến thường được sử dụng trong rất nhiều cuộc tấn công kỹ thuật xã hội sẽ được mô tả tiếp theo đây.

### **Tấn công giả mạo (Phishing)**

*Phishing* (được phát âm là “câu cá/fishing”) là một dạng kỹ thuật xã hội mà theo đó, một kẻ tấn công cố gắng chiếm đoạt những thông tin nhạy cảm từ phía người dùng bằng cách giả mạo một thực thể đáng tin cậy trong một email hoặc tin nhắn tức thời được gửi cho một nhóm lớn thường bao gồm những người dùng ngẫu nhiên. Kẻ tấn công sẽ cố gắng lấy được những thông tin chẳng hạn như tên người dùng, mật khẩu, số thẻ tín dụng, và các chi tiết về tài khoản ngân hàng của người dùng. Thông điệp được gửi đi thường khuyến khích người dùng truy cập vào một trang web trông có vẻ như thuộc về một thực thể đáng tin cậy như PayPal hoặc eBay, và cả hai đều thường được sử dụng trong những nỗ lực phishing. Tuy nhiên, trang web mà người dùng thực tế truy cập tới không được sở hữu bởi tổ chức danh tiếng, và yêu cầu người dùng cung cấp những thông tin có thể được sử dụng cho các cuộc tấn công sau này. Thường thì thông điệp đã gửi cho người dùng tuyên bố rằng tài khoản của người dùng đã

bị xâm phạm và yêu cầu, vì mục đích bảo mật, người dùng nhập thông tin tài khoản của họ để xác minh chi tiết.

Trong một ví dụ rất phổ biến khác về phishing, kẻ tấn công gửi một loạt các email, được cho là từ ngân hàng, nói với người nhận rằng một vi phạm an ninh đã diễn ra và hướng dẫn họ nhấp chuột vào một đường liên kết để xác minh rằng tài khoản của họ đã không bị giả mạo. Nếu một cá nhân thực sự nhấp chuột vào đường liên kết, họ được đưa đến một trang web thể hiện rằng nó (trang web) được sở hữu bởi ngân hàng nhưng trong thực tế lại được kiểm soát bởi kẻ tấn công. Khi họ cung cấp thông tin tài khoản và mật khẩu vì mục đích “xác minh”, cá nhân đó thực sự đã cung cấp chúng cho kẻ tấn công.



**MÁCH NƯỚC CHO KỲ THI** Phishing giờ đây là hình thức tấn công kỹ thuật xã hội phổ biến nhất có liên quan đến bảo mật máy tính. Đích nhắm mục tiêu có thể là một hệ thống máy tính và quyền truy cập đến những thông tin trên đó (đó là trường hợp khi phishing cố gắng yêu cầu một danh tính và mật khẩu của người dùng), hoặc cũng có thể là thông tin cá nhân, thường là thông tin tài chính, về một cá nhân (trong trường hợp phishing cố gắng yêu cầu về thông tin ngân hàng của một cá nhân).

### Tấn công giả mạo qua tin nhắn SMS (Smishing)

*Smishing* là một kiểu tấn công sử dụng Dịch vụ Tin nhắn Ngắn gọn (Short Message Service – SMS) trên điện thoại di động của nạn nhân. Đây là một phiên bản của phishing qua SMS. Nó bắt đầu với một tin nhắn SMS định hướng người dùng đến một địa chỉ URL có thể đóng vai trò như một véc-tơ tấn công đa dạng, bao gồm cả các hình thức malware. Kiểu tấn công này chủ yếu hoạt động do việc sử dụng tính khẩn cấp và sự đe dọa trong tin nhắn, vốn có thể sử dụng một cảnh báo chặng hạn như “Bạn đã đăng

ký thuê bao dịch vụ XYZ, vốn sẽ bắt đầu tính phí định kỳ mỗi 2\$ một tháng. Hãy nhấp vào đây để hủy đăng ký thuê bao trước khi việc tính phí diễn ra". Khi người dùng nhấp vào URL, giai đoạn tiếp theo của cuộc tấn công có thể được bắt đầu.

### **Truy cập bất hợp pháp thông qua giọng nói (Vishing)**

*Vishing* là một hình thức phishing khác sử dụng công nghệ giao tiếp bằng giọng nói để thu thập được những thông tin mà kẻ tấn công đang tìm kiếm. Vishing lợi dụng sự tin tưởng mà một số người đã đặt vào mạng điện thoại. Người dùng đã không nhận thức được rằng những kẻ tấn công có thể giả mạo (mô phỏng) những cuộc gọi từ những thực thể hợp pháp bằng cách sử dụng công nghệ Âm thanh qua IP (VoIP). Chiến thuật này được sử dụng để thiết lập một hình thức của sự tin tưởng mà sau đó bị khai thác bởi những kẻ tấn công qua điện thoại. Nói chung, kẻ tấn công đang hy vọng thu thập được số thẻ tín dụng hoặc những thông tin khác có thể được sử dụng trong việc đánh cắp danh tính. Người dùng có thể nhận được một email yêu cầu họ gọi đến một số điện thoại mà có khả năng được trả lời bằng một hệ thống thông điệp giọng nói đã bị xâm phạm. Người dùng cũng có thể nhận được một thông điệp đã được ghi âm thể hiện rằng thông điệp đến từ một thực thể hợp pháp. Trong cả hai trường hợp, người dùng sẽ được khuyến khích hồi đáp một cách nhanh chóng và cung cấp những thông tin nhạy cảm để từ đó việc truy cập vào tài khoản của họ không bị khóa. Nếu một người dùng thậm chí nhận được một tin nhắn yêu cầu đến từ một thực thể có uy tín và yêu cầu những thông tin nhạy cảm, người dùng không nên cung cấp những thông tin này mà thay vào đó, nên sử dụng Internet hoặc kiểm tra một sao kê tài khoản hợp pháp để tìm kiếm một số điện thoại có thể được sử dụng để liên hệ với thực thể đó. Sau đó, người dùng có thể xác minh rằng thông điệp đã nhận được là hợp pháp và báo cáo về nỗ lực tấn công bằng giọng nói.



**LƯU Ý** Một đoạn phim tuyệt vời cho thấy cách sử dụng một vài công cụ kỹ thuật xã hội có thể tìm thấy tại địa chỉ <https://www.youtube.com/watch?v=1c7scxvKQOo> ("Đây là cách mà những tin tức tấn công bạn bằng cách sử dụng kỹ thuật xã hội đơn giản"). Đoạn phim này chứng minh việc sử dụng tấn công bằng giọng nói để đánh cắp thông tin đăng nhập điện thoại di động của một ai đó.



**MÁCH NƯỚC CHO KỲ THI** Phishing, smishing, vishing – tất cả đều là những cuộc tấn công chống lại trạng thái nhận thức của người dùng. Sử dụng các nguyên tắc đổi mới tính hiệu quả, được thảo luận sau trong chương, người ta có thể tạo ra một thông điệp khiến cho khả năng trở thành nạn nhân của những cuộc tấn công này cao hơn. Cuộc tấn công là sự kết hợp giữa các yếu tố kỹ thuật và áp lực tâm lý, và cùng với nhau, chúng khiến cho người dùng mắc bẫy và nhấp vào đường liên kết.

### Thư rác

*Spam* (Thư rác), như tất cả mọi người đều biết, là một loạt email không được yêu cầu. Mặc dù thường không được mọi người xem là một vấn đề kỹ thuật xã hội, hoặc thậm chí, một vấn đề về bảo mật đối với chủ đề đó, thư rác vẫn có thể là một mối quan tâm về bảo mật. Nó (thư rác) có thể là hợp pháp theo nghĩa nó được gửi từ một công ty đang quảng cáo một sản phẩm hoặc dịch vụ, nhưng nó cũng có thể độc hại và có thể bao gồm một tập tin đính kèm có chứa phần mềm độc hại được thiết kế để gây hại cho hệ thống của bạn, hoặc một đường liên kết đến một trang web độc hại mà có thể cố gắng thu thập những thông tin cá nhân từ bạn. Do thư rác là không được mong muốn, mọi người nên luôn luôn cân nhắc về

nguồn gốc [của thư rác] trước khi nhấp vào bất kỳ đường liên kết nào hoặc trước khi phản hồi trực tiếp. Bởi vì thư rác có thể dẫn đến kết quả lý người dùng nhấp chuột vào đường liên kết, nó nên được coi là một hình thức thay đổi hành vi của con người hoặc là kỹ thuật xã hội.

### **Thư rác qua Tin nhắn Tức thời (SPIM)**

Mặc dù không được biết đến nhiều nhưng một biến thể khác của thư rác là *SPIM (Spam over Instant Messaging)*, về cơ bản là thư rác được phân phối qua một ứng dụng tin nhắn tức thời. Mục đích của SPIM độc hại cũng giống như mục đích của thư rác – khiến cho người dùng nhấp chuột vào nội dung hoặc đường liên kết độc hại mà không nghi ngờ gì, từ đó, khởi đầu một cuộc tấn công.

### **Tấn công giả mạo nhắm mục tiêu (Spear Phishing)**

*Spear phishing* là một thuật ngữ được tạo ra để đề cập đến một cuộc tấn công lừa đảo nhắm mục tiêu đến một cá nhân hoặc một nhóm cá nhân cụ thể có cùng một điểm chung nào đó. Vì cuộc tấn công nhắm mục tiêu đến một nhóm cụ thể, chẳng hạn như giám đốc điều hành cấp cao, tỷ lệ của các cuộc tấn công thành công (nghĩa là, số lượng phản hồi nhận được) so với tổng số email hoặc thông điệp đã được gửi đi thường gia tăng vì một cuộc tấn công đã được nhắm mục tiêu sẽ trông có vẻ hợp lý hơn là một thông điệp được gửi cho người dùng một cách ngẫu nhiên.

### **Dò tìm Đồ phế thải (Dumpster Diving)**

Quá trình lục lọi thùng rác của một mục tiêu với hy vọng tìm thấy những thông tin có giá trị để có thể được sử dụng trong một nỗ lực thâm nhập được cộng đồng bảo mật gọi là *dò tìm thùng rác/dò tìm đồ phế thải*. Một khu vực phổ biến để tìm kiếm thông tin, nếu kẻ tấn công ở gần mục tiêu, chính là trong thùng rác của mục tiêu. Kẻ tấn công có thể tìm thấy những mẫu thông tin nhỏ có thể hữu ích cho một cuộc tấn công. Tuy nhiên, chiến thuật này không phải là độc đáo đối với cộng đồng máy tính, nó đã

được sử dụng trong nhiều năm bởi những người khác, chẳng hạn như kẻ trộm danh tính, điều tra viên tư nhân và nhân viên thực thi pháp luật, để lấy được thông tin về một cá nhân hoặc tổ chức. Nếu kẻ tấn công rất may mắn và các thủ tục bảo mật của mục tiêu rất kém, chúng có thể thực sự tìm thấy mã định người dùng cùng với mật khẩu.

Một kẻ tấn công có thể thu thập nhiều loại thông tin có thể rất hữu ích trong một cuộc tấn công kỹ thuật xã hội. Trong hầu hết các địa điểm, thùng rác không còn được coi là tài sản cá nhân sau khi nó đã được vứt bỏ (và thậm chí, ngay cả ở những nơi việc dò tìm là bất hợp pháp, việc bắt buộc tuân thủ rất ít xảy ra). Một tổ chức thực sự nên có các chính sách về loại bỏ các tài liệu. Những thông tin nhạy cảm nên được băm nhỏ và tổ chức nên cân nhắc việc bảo vệ thùng rác để các cá nhân không thể lục lọi nó. Mọi người cũng nên xem xét việc cắt nhỏ thông tin cá nhân hoặc thông tin nhạy cảm khi họ muốn loại bỏ vào thùng rác của riêng họ. Một máy cắt nhỏ tài liệu chất lượng hợp lý không quá đắt tiền và rất đáng giá khi so sánh với tổn thất tiềm năng có thể xảy ra do kết quả của hành vi trộm cắp danh tính.

### **Nhìn qua Vai (Shoulder Surfing)**

*Nhìn qua Vai* không nhất thiết phải liên quan đến việc liên hệ trực tiếp với mục tiêu mà thay vào đó, kẻ tấn công quan sát trực tiếp việc một cá nhân nhập những thông tin nhạy cảm vào một biểu mẫu, bàn phím số hoặc bàn phím. Kẻ tấn công có thể chỉ đơn giản là nhìn qua vai của một người dùng đang làm việc, ví dụ, hoặc có thể cài đặt một camera hoặc sử dụng hai mắt để quan sát người dùng nhập những thông tin nhạy cảm. Kẻ tấn công có thể cố gắng thu thập được những thông tin như số định danh cá nhân (PIN) ở một máy rút tiền tự động (ATM), một mã truy nhập kiểm soát truy cập tại một cửa an ninh, hoặc một số thẻ tín dụng hoặc thẻ điện thoại. Giờ đây, rất nhiều địa điểm sử dụng một bộ lọc hoặc màn

hình riêng tư để bao quanh một bàn phím nhỏ để từ đó, sẽ khó quan sát được một cá nhân khi họ nhập những thông tin của họ. Các hệ thống tinh vi hơn có thể xáo trộn vị trí thực tế của các chữ số để hàng trên cùng tại một thời điểm có thể bao gồm các số 1,2 và 3 và trong lần tiếp theo sẽ bao gồm 4,8 và 0. Mặc dù điều này khiến cho người dùng sẽ bị chậm hơn một chút khi nhập thông tin nhưng nó ngăn chặn được những nỗ lực của một kẻ tấn công để quan sát những con số nào đang được bấm và sau đó ăn cùng một hình mẫu phím vì vị trí của các con số liên tục thay đổi.

### **Chuyển hướng lưu lượng web (Pharming)**

*Pharming* bao gồm việc chuyển hướng người dùng sai đến các trang web giả mạo được tạo ra để trông như một trang web chính thức. Bằng cách sử dụng phishing, những kẻ tấn công nhắm đến các cá nhân, từng người một, bằng cách gửi email đi. Để trở thành một nạn nhân, người nhận phải thực hiện một hành động (ví dụ, phản hồi bằng cách cung cấp thông tin cá nhân). Trong kiểu tấn công chuyển hướng lưu lượng web, người dùng sẽ được chuyển hướng đến một trang web giả mạo vốn là kết quả của hành động như nhiễm độc DNS (một cuộc tấn công thay đổi các URL trong một bảng tên miền của máy chủ) hoặc sửa đổi tập tin host cục bộ (được sử dụng để chuyển đổi các URL thành địa chỉ IP tương ứng). Khi đã ở trang giả mạo, người dùng có thể cung cấp thông tin cá nhân, và tin rằng họ đang kết nối tới một trang web hợp pháp.

### **Tấn công Tailgating (Tailgating)**

*Tailgating* (hoặc piggybacking) là một chiến thuật đơn giản về việc theo dõi sát sao phía sau của một cá nhân chỉ vừa mới sử dụng thẻ truy cập hoặc mã PIN của họ để có quyền truy cập vật lý vào một căn phòng hoặc tòa nhà. Mọi người thường vội vã và thường sẽ không tuân thủ các thực tiễn và thủ tục bảo mật tốt. Những kẻ tấn công biết được điều này và có thể cố gắng khai thác đặc trưng này trong hành vi của mọi người. Từ đó,

một kẻ tấn công có thể có được quyền tiếp cận vào cơ sở vật chất mà không cần phải biết mã truy cập hoặc phải có một thẻ truy cập. Điều này tương tự như việc nhìn qua vai ở chỗ dựa vào việc kẻ tấn công lợi dụng một người dùng đã được cấp phép, người đã không tuân theo các thủ tục bảo mật. Rất thường xuyên, kẻ tấn công thậm chí có thể bắt đầu một cuộc thảo luận với mục tiêu trước khi đi vào cửa để từ đó, người dùng có thể thoải mái hơn trong việc cho phép một cá nhân đi vào mà không nghi ngờ họ. Thao nghĩa này, piggybacking có liên quan đến các cuộc tấn công kỹ thuật xã hội.

Cả hai kỹ thuật piggybacking và nhìn qua vai đều dựa vào những thực tiễn bảo mật kém của một người dùng đã được cấp phép để thành công. Do đó, cả hai kỹ thuật đều có thể được chống lại một cách dễ dàng bằng cách đào tạo nhân viên sử dụng những thủ tục đơn giản để đảm bảo rằng không có ai đi theo họ quá gần hoặc ở một vị trí có thể quan sát được những hành động của họ. Một biện pháp ứng phó tinh vi hơn đối với piggybacking liên quan đến việc sử dụng một *bẫy người* (*mantrap*), sử dụng hai cửa để có quyền truy cập vào cơ sở. Cửa thứ hai không mở ra trừ khi cửa đầu tiên được đóng lại, và các cửa được đặt gần nhau để hình thành nên một vòng vây để chỉ cho phép một cá nhân đi qua tại một thời điểm.

### **Thông tin Câu hỏi mở (Eliciting Information)**

Các cuộc gọi đến và đi từ đơn vị hỗ trợ dịch vụ hoặc hỗ trợ kỹ thuật có thể được sử dụng đối với *thông tin câu hỏi mở* (*eliciting information*). Một kỹ sư xã hội có kinh nghiệm có thể sử dụng một loạt các kỹ thuật tâm lý để thuyết phục mọi người, những người mà công việc chính của họ là giúp đỡ những người khác, để hoàn tất các tác vụ dẫn đến sự xâm phạm an ninh. Đóng vai một nhân viên, một kẻ tấn công có thể khôi phục mật khẩu, thông tin về một số hệ thống hoặc những thông tin hữu ích

khác. Cuộc gọi cũng có thể đi theo chiều hướng khác, nơi mà kỹ sư xã hội đang đóng vai trò là người trợ giúp hoặc người hỗ trợ công nghệ. Sau đó, bằng cách gọi cho nhân viên, kẻ tấn công có thể nhận được thông tin về trạng thái hệ thống và các yếu tố thú vị khác mà chúng có thể sử dụng sau này.

### **Lừa đảo kiểu cá voi (Whaling)**

Những mục tiêu có giá trị cao thường được gọi là những chú cá voi. Một cuộc tấn công kiểu *lừa đảo cá voi* là một cuộc tấn công mà mục tiêu là một cá nhân có giá trị cao, chẳng hạn như CEO hoặc CFO. Các cuộc tấn công kiểu cá voi không được thực hiện bằng cách tấn công nhiều mục tiêu và hy vọng một sự phản hồi, mà thay vào đó, được xây dựng tùy chỉnh để gia tăng tỷ lệ thành công. Spear phishing là một phương pháp phổ biến được sử dụng để chống lại các chú cá voi, vì giao tiếp được thiết kế để trông có vẻ như một hoạt động kinh doanh thông thường đối với mục tiêu, được tạo ra để trông có vẻ không nguy hiểm. Các chú cá voi có thể bị lừa theo cùng một cách như với những người khác, sự khác biệt ở đây là nhóm mục tiêu được hạn chế, để một kẻ tấn công không thể chỉ dựa vào sự phản hồi ngẫu nhiên từ một nhóm mục tiêu rộng lớn.

### **Prepending**

*Thêm trước (Prepending)* được định nghĩa là hành động bổ sung thêm một thứ gì đó khác vào đầu một hạng mục. Khi được sử dụng trong bối cảnh kỹ thuật xã hội, thêm trước là hành động cung cấp thông tin mà người khác sẽ hành động theo đó, thường xuyên trước khi họ yêu cầu nó, nhằm cố gắng hợp pháp hóa yêu cầu thực tế, yêu cầu này vốn sẽ đến sau đó. Bằng cách sử dụng các cấu trúc tâm lý về quyền hạn, kẻ tấn công có thể sử dụng prepending bằng cách nói rằng chúng được gửi bởi sếp của mục tiêu hoặc một nhân vật có thẩm quyền khác, như một phương tiện để biện minh cho lý do tại sao mục tiêu nên thực hiện một hành động cụ

thể — thường là một hành động mà trong những trường hợp không có việc prepending, sẽ là không bình thường.

### **Gian lận Danh tính (Identity Fraud)**

*Gian lận danh tính* là sử dụng những thông tin đăng nhập giả mạo để đạt được mục đích cuối cùng. Điều này có thể trở thành rủi ro cao như việc giả vờ là một đại diện chính thức của một cơ quan chính phủ hoặc một cơ quan quản lý, hoặc rủi ro thấp hơn như việc thể hiện như là một người tưới cây ngoài vườn. Người ta có thể giả làm một nhân viên giao hàng, xuất hiện với một cái hộp – hoặc thậm chí tốt hơn nữa, một máy chủ - và cố gắng giao hàng trực tiếp đến phòng máy chủ. Việc này hoạt động tốt nhất khi nạn nhân đang mong đợi người đó, như trong trường hợp một máy chủ bị hư hỏng vẫn đang trong hạn bảo hành sửa chữa. Gian lận danh tính cũng có thể được thực hiện trực tuyến, bằng cách sử dụng những thông tin đã biết về cá nhân mà bạn đang mạo danh (xem phần “Mạo danh” ở phần sau của chương này), và đánh lừa nạn nhân mà bạn đang tấn công. Biện pháp phòng thủ để chống lại gian lận danh tính cũng giống như với hầu hết các cuộc tấn công kỹ thuật xã hội khác: sử dụng những chính sách và thủ tục mạnh mẽ và không có ngoại lệ. Ví dụ, tất cả các gói hàng phải được đặt tại bàn bảo vệ, mọi khách thăm, những người cần truy cập phải được tháp tùng, không có ngoại lệ, v.v... Ngoài ra, không nên có ngoại lệ đối với các chính sách tiết lộ, chẳng hạn như thiết lập lại mật khẩu hoặc cấp quyền truy cập cho một bên nào đó. Thực hiện mọi điều theo các quy tắc công việc – chỉ cần nhìn vào an ninh TSA, nơi mà không có bất kỳ cách nào để lén qua vạch kẻ của họ. Độ chính xác và hiệu quả của việc sàng lọc của họ có thể là một nghi vấn nhưng việc giải quyết vấn đề thì không. Đây là chìa khóa cho việc ngăn chặn hầu hết các cuộc tấn công kỹ thuật xã hội.

## Lừa đảo Hóa đơn Trực tuyến (Invoice Scams)

*Lừa đảo hóa đơn* sử dụng một hóa đơn giả mạo trong một nỗ lực để yêu cầu một công ty thanh toán cho một thứ gì đó mà họ đã không đặt hàng. Lập luận rất đơn giản: gửi một hóa đơn giả mạo và sau đó được thanh toán. Trên thực tế, vì hầu hết các công ty đều có các biện pháp kiểm soát kẽ toán tương đối mạnh mẽ nên việc lừa đảo sẽ liên quan đến việc nhờ được một ai đó nắm ngoài nhóm kế toán để bắt đầu quá trình, cho thấy tính hợp pháp hợp lý. Tất cả những điều này trông có vẻ sẽ không hoạt động nhưng tội phạm mạng đã thu về hàng tỷ đô la theo nghĩa đen bằng cách sử dụng phương pháp này. Những hạng mục thường được sử dụng trong các trò lừa đảo là các sản phẩm văn phòng như mực in hoặc các văn phòng phẩm phổ biến, các sản phẩm vệ sinh, các thẻ thành viên của tổ chức, và một loạt các dịch vụ doanh nghiệp. Đôi khi, để tăng thêm tính khẩn cấp, một thông báo tài chính được đưa vào, đe dọa rằng sẽ báo cáo một tổ chức cho một cơ quan thu nợ, từ đó khiến cho một người trả nêu do dự trước khi ném hóa đơn đi.

## Thu thập Thông tin đăng nhập (Credential Harvesting)

*Thu thập thông tin đăng nhập* liên quan đến việc thu thập những thông tin đăng nhập, chẳng hạn như mã định danh người dùng, mật khẩu, v.v..., cho phép một kẻ tấn công có một loạt quyền truy cập vào hệ thống. Một hình thức phổ biến của thu thập thông tin đăng nhập bắt đầu với một email phishing thuyết phục một người dùng nhấp chuột vào một đường liên kết và đáp lại là một trang nhân bản của trang web ngân hàng của họ. Người dùng thường sẽ không kiểm tra các thiết lập bảo mật của kết nối trình duyệt của họ, và khi họ nhập những thông tin mã định danh người dùng và mật khẩu vào, thông tin đăng nhập của họ đã bị thu thập và được lưu trữ cho các tội phạm sử dụng sau này.

Mục tiêu của việc thu thập thông tin đăng nhập chỉ là để có được những thông tin đăng nhập. Khi những kẻ tội phạm đã lừa được bạn cung cấp thông tin đăng nhập của bạn, chúng sẽ chuyển hướng bạn đến đúng trang web hoặc đưa ra một báo lỗi và một kết nối mới đến đúng trang web để bạn thử lại. Chúng muốn che giấu thực tế rằng chúng đã đánh cắp thông tin đăng nhập của bạn. Phương pháp tấn công này đã rất thành công, và giờ đây các công ty tài chính đã tuân theo một thông lệ tiêu chuẩn khi theo dõi mã định danh và mật khẩu của một người dùng thông thường với một yếu tố thứ hai, thẩm tra năm ngoài dài băng tần (out-of-band) để ngăn chặn việc sử dụng thông tin đăng nhập đã bị thu thập tiếp theo sau đó. Mặc dù việc này bổ sung thêm một lớp phức tạp và bất tiện đối với người dùng nhưng đây là điều cần thiết để ngăn chặn việc tái sử dụng những thông tin đăng nhập đã bị thu thập.



**LƯU Ý** Rất nhiều cuộc tấn công được thiết kế để thu thập được những thông tin đăng nhập của người dùng. Bất kỳ thông tin đăng nhập nào bạn có thể dùng chung là một rủi ro, và để chống lại rủi ro này, các tổ chức phải áp dụng xác thực hai yếu tố. Yếu tố thứ hai là một phương pháp khác để xác định người dùng và thường là duy nhất và chỉ có hiệu lực trong một khoảng thời gian giới hạn. Một ví dụ là khi bạn đăng nhập vào trang web ngân hàng của bạn, bạn nhận được một tin nhắn văn bản cùng với một mã số để cấp phép cho mục nhập của bạn. Việc sử dụng mã số này gây ra sự phức tạp đáng kể cho những kẻ tấn công khi chúng đã có được thông tin đăng nhập của bạn.

### **Do thám (Reconnaissance)**

*Do thám* là một thuật ngữ quân sự được sử dụng để mô tả những hành động khảo sát một chiến trường để thu thập thông tin trước khi xảy ra

chiến sự. Trong lĩnh vực an ninh mạng, khái niệm cũng tương tự: một kẻ thù sẽ kiểm tra các hệ thống mà chúng dự định tấn công, sử dụng một loạt các phương pháp. Một vài trong số các phương pháp này nằm ngoài phạm vi hiểu biết của nạn nhân: những tìm kiếm trên Google, những tìm kiếm hồ sơ công khai, v.v... Nhưng những khía cạnh khác liên quan trực tiếp đến việc thao túng mọi người để thu thập thông tin. Khảo sát một sơ đồ tổ chức của một công ty, gọi điện và yêu cầu thông tin liên hệ của mọi người và xây dựng một danh bạ cá nhân, đặt ra những câu hỏi về phần cứng và phần mềm thông qua các khảo sát, và đọc các thông cáo báo chí có thể được sử dụng để có được thông tin mô tả về hệ thống sẽ bị tấn công. Mặc dù hầu hết các hoạt động do thám được chấp nhận là không thể tránh khỏi, nhưng một vài trong số chúng được giúp sức thông qua các thông cáo báo chí cho thế giới biết rằng ai là đối tác bảo mật của bạn, sản phẩm bảo mật nào bạn đang sử dụng, v.v... Từng mục thông tin này sau đó sẽ được sử dụng như một phần của quá trình tấn công. Những điểm yếu đã biết so với các sản phẩm cụ thể có thể được sử dụng và dễ dàng tìm kiếm hơn nếu những kẻ tấn công biết được những sản phẩm nào công ty đang sử dụng. Việc thực hiện việc do thám liên tục trước khi tấn công mang lại cho kẻ tấn công những yếu tố thông tin then chốt sau này khi những mục thông tin này được cần đến.

### **Đánh lừa (Hoax)**

Thoáng qua, thoạt nhìn thì trò lừa bịp trông có vẻ như liên quan đến bảo mật sẽ được cân nhắc là một mối phiền toái và không phải là một vấn đề bảo mật thực sự. Điều này có thể đúng với một số trò bịp, đặc biệt là những trò bịp thuộc kiểu truyền thuyết đô thị, nhưng trong thực tế là một tình huống mà một *trò bịp* có thể trở nên rất nguy hiểm nếu như nó khiến cho người dùng thực hiện một số loại hành động làm suy yếu bảo mật. Ví dụ, một trò lừa bịp thực sự mô tả một mẫu phần mềm độc hại mới và có tính phá hoại cao. Nó đã hướng dẫn người dùng kiểm tra sự

tồn tại của một tập tin nhất định và xóa nó đi nếu như tập tin đó được tìm thấy.Trong thực tế, tập tin đã được đề cập đến là một tập tin rất quan trọng được sử dụng bởi hệ điều hành, và việc xóa nó đã gây ra vấn đề vào lần khởi động hệ thống tiếp theo. Thiệt hại gây ra bởi việc người dùng sửa đổi các thiết lập có thể trở nên nghiêm trọng. Như với các hình thức kỹ thuật xã hội khác, việc đào tạo và nâng cao nhận thức là tuyển phòng thủ đầu tiên và tốt nhất đối với cả người dùng lẫn quản trị viên. Người dùng nên được đào tạo để nghi ngờ những email và câu chuyện bất thường và nên biết liên hệ với ai trong tổ chức để xác minh tính xác thực của chúng nếu họ nhận được. Một trò bịa cũng thường khuyên người dùng gửi nó cho bạn bè của họ để từ đó họ cũng biết được về vấn đề (trong trò bịa) – và bằng cách thực hiện việc này, người dùng đã giúp phát tán trò bịa. Người dùng cần phải nghi ngờ bất kỳ email nào khuyên họ rằng “hãy truyền bá cho thế giới”.

### **Mạo danh (Impersonation)**

*Mạo danh* là một kỹ thuật kỹ thuật xã hội phổ biến và có thể được sử dụng theo nhiều cách. Nó có thể diễn ra đối với cá nhân, qua điện thoại, hoặc trực tuyến. Trong trường hợp một cuộc tấn công mạo danh, kẻ tấn công đảm nhiệm một vai trò đã được công nhận bởi cá nhân đang bị tấn công, và bằng việc đảm nhiệm vai trò này, kẻ tấn công sử dụng những thành kiến tiềm ẩn của nạn nhân chống lại khả năng phán đoán tốt hơn của họ để tuân thủ các thủ tục. Mạo danh có thể diễn ra theo nhiều cách khác nhau – từ các bên-thứ-ba, đến nhân viên vận hành bộ phận hỗ trợ dịch vụ, đến các nhà thầu, hoặc thậm chí các nguồn trực tuyến.

### **Ủy quyền Bên-thứ-ba**

Sử dụng những thông tin đã có được trước đây về một dự án, thời hạn, các ông chủ, v.v..., kẻ tấn công (1) đi đến với thứ gì đó mà nạn nhân có vẻ như đang mong đợi hoặc sẽ thấy là bình thường, (2) sử dụng chiêu

bài dự án đang gặp rắc rối hoặc một số tình huống khác sẽ được coi là hữu ích hoặc như một ai đó không gây phiền phức, và (3) phô trương thanh thê như một “Ông Lớn”, một người đang không có mặt ở văn phòng và không thể liên lạc được tại thời điểm đó, và do đó, tránh được sự kiểm tra chéo. Ngoài ra, kẻ tấn công hiếm khi yêu cầu bất kỳ điều gì trông có vẻ bất hợp lý hoặc không có khả năng được chia sẻ dựa trên các tình huống. Những hành động này có thể tạo ra sự ủy quyền của bên-thứ-ba, trong khi thực tế là không có.

### **Các Nhà thầu/Các bên bên ngoài**

Một điều phổ biến trong rất nhiều tổ chức là đều có các nhà thầu bên ngoài để làm vệ sinh tòa nhà, tưới cây, và thực hiện những việc lặt vặt theo thường lệ khác. Trong rất nhiều những tình huống này, nếu không có các biện pháp bảo vệ thích hợp, một kẻ tấn công có thể chỉ đơn giản là mặc một bộ đồng phục của một nhà thầu phù hợp, xuất hiện để thực hiện công việc tại một thời điểm hơi khác so với thời gian thực hiện bình thường, và, nếu bị nghi ngờ, họ sẽ đánh vào sự đồng cảm của người lao động bằng cách nói rằng họ đang trám vào chỗ của X hoặc thay thế cho Y. Kẻ tấn công sau đó đi lang thang trong các hội trường mà không bị chú ý vì chúng hòa lẫn vào, trong khi chụp ảnh bẩn làm việc và giấy tờ và tìm kiếm thông tin.

### **Tấn công trực tuyến**

Sự mạo danh có thể được sử dụng trong các cuộc tấn công trực tuyến. Trong những trường hợp này, công nghệ đóng vai trò trung gian trong chuỗi giao tiếp. Một số hình thức cũ hơn, chẳng hạn như các cửa sổ pop-up, có khuynh hướng kém hiệu quả hơn trong ngày nay bởi vì người dùng đã cảnh giác với chúng. Tuy nhiên, vẫn có rất nhiều những nỗ lực tấn công lừa đảo qua email và các trò gian lận trên các phương tiện xã hội.

## Biện pháp phòng thủ

Trong tất cả các trường hợp mạo danh, biện pháp phòng thủ tốt nhất thực ra rất đơn giản – có sẵn một quy trình đòi hỏi nhân viên yêu cầu được xem mã định danh (ID) của một cá nhân trước khi tương tác với họ nếu nhân viên không thực sự biết những chi tiết cá nhân về họ. Việc đó bao gồm cả những người đáng nghi ngờ như tài xế giao hàng hoặc công nhân hợp đồng. Đừng để mọi người đi qua cửa, “piggybacking” mà không kiểm tra mã định danh của họ. Nếu như đây là một quy trình tiêu chuẩn thì không có ai vi phạm, và nếu ai đó giả mạo hành vi phạm tội thì điều đó lại càng đáng nghi ngờ. Đào tạo và nâng cao nhận thức cũng có tác dụng, như đã được chứng minh bởi các xu hướng chẳng hạn như tính hiệu quả giảm dần của các cửa sổ pop-up. Nhưng mấu chốt của việc bảo vệ này là tiến hành việc đào tạo trên cơ sở định kỳ và điều chỉnh nó theo những gì đang được trải qua, thay vì đọc thuộc lòng những thực tiễn tốt nhất.



## MÁCH NƯỚC CHO KỲ THI

Một chương trình đào tạo và nâng cao nhận thức vẫn là biện pháp phòng thủ tốt nhất để chống lại các cuộc tấn công kỹ thuật xã hội.

## Tấn công Vũng Nước (Watering hole attacks)

Véc-tơ tấn công được công nhận phổ biến nhất là những gì nhắm đến một mục tiêu. Do bản chất định hướng của các cuộc tấn công, những biện pháp phòng thủ được vạch ra để phát hiện và chống lại chúng. Tuy nhiên, điều gì xảy ra nếu người dùng “yêu cầu” tấn công bằng cách truy cập một trang web. Cũng giống như một thợ săn rình rập cạnh một vũng nước để bắt những con vật đến uống nước, những kẻ tấn công có thể gieo rắc những phần mềm độc hại vào những trang web mà người dùng thường hay truy cập. Được xác định trước tiên bởi hãng bảo mật RSA, một tấn công Comptia Security+ - All in One - Exam Guide

công vũng nước liên quan đến việc lây nhiễm một trang web mục tiêu bằng malware. Trong một số những trường hợp đã được phát hiện, sự lây nhiễm đã được giới hạn trong một khu vực địa lý cụ thể. Đây không phải là những cuộc tấn công đơn giản, nhưng chúng có thể rất có hiệu quả trong việc lây nhiễm malware cho những nhóm người dùng đầu cuối cụ thể. Các cuộc tấn công vũng nước rất phức tạp để đạt được và thường như được tài trợ bởi các quốc gia và những kẻ tấn công có nguồn tài nguyên dồi dào khác. Xét về tỷ lệ, véc-tơ tấn công điển hình sẽ là zero-day để tránh bị phát hiện thêm.

### **Chiếm quyền URL (Typosquatting)**

*Chiếm quyền URL* là một hình thức tấn công liên quan đến việc tận dụng các lỗi đánh máy phổ biến. Nếu như người dùng nhập sai một URL thì kết quả nên là một lỗi 404, hoặc "tài nguyên không được tìm thấy". Nhưng nếu một kẻ tấn công đã đăng ký một địa chỉ URL lỗi thì người dùng sẽ được đưa đến trang web của kẻ tấn công. Hình thái tấn công này còn được gọi là *chiếm quyền URL*, *URL giả mạo* hoặc *đánh cắp thương hiệu* nếu như mục tiêu là để đánh lừa dựa trên thương hiệu.

Có một số nguyên nhân mà một kẻ tấn công sẽ theo đuổi cách thức tấn công này. Rõ ràng nhất là một cuộc tấn công lừa đảo phishing. Trang web giả mạo thu thập thông tin đăng nhập, chuyển những thông tin này cho trang web thực tế, sau đó ngừng cuộc đàm thoại để tránh bị phát hiện khi đã thu thập được những thông tin đăng nhập. Nó cũng có thể được sử dụng để gieo rắc tấn công malware trên máy của nạn nhân. Nó có thể chuyển các gói tin thông qua một mạng liên kết, kiểm doanh thu thông qua các cú nhấp chuột dựa trên lỗi chính tả. Có một loạt các hình thức tấn công khác có thể được thực hiện với việc sử dụng một địa chỉ URL làm điểm khởi đầu.

## **Viện cớ (Pretexting)**

*Viện cớ* là một hình thức kỹ thuật xã hội, trong đó, kẻ tấn công sử dụng một câu chuyện (cái cớ) để gây tác động đến việc từ bỏ một số mục thông tin của nạn nhân. Một ví dụ là gọi lên, đóng giả như một sinh viên cùng trường đại học hoặc một quản trị viên đồng nghiệp với một giám đốc điều hành cấp cao. Cái cớ không nhất thiết phải đúng, nó chỉ cần đáng tin cậy và phù hợp để thuyết phục nạn nhân giúp đỡ. Việc cớ sử dụng sự lừa dối và động cơ giả để thao túng nạn nhân. Mục tiêu chính của kẻ tấn công là đạt được sự tin tưởng của mục tiêu và khai thác nó. Một cuộc tấn công viện cớ có thể xảy ra trực tiếp, qua email, qua điện thoại hoặc hầu như với bất kỳ hình thức liên lạc nào khác.

## **Các Chiến dịch tạoẢnh hưởng**

*Các chiến dịch tạo ảnh hưởng* liên quan đến việc sử dụng thông tin đã được thu thập và xuất bản có chọn lọc tài liệu cho những cá nhân quan trọng nhằm nỗ lực thay đổi nhận thức và thay đổi suy nghĩ của mọi người về một chủ đề. Người ta có thể tham gia vào một chiến dịch gây ảnh hưởng chống lại một người duy nhất, nhưng hiệu quả bị hạn chế. Chiến dịch ảnh hưởng thậm chí còn mạnh mẽ hơn khi được sử dụng kết hợp với các phương tiện truyền thông xã hội để lan truyền ảnh hưởng thông qua sự lan truyền người ảnh hưởng. Những người có ảnh hưởng là những người có một lượng lớn người theo dõi - những người đọc những gì họ đăng - và trong nhiều trường hợp, họ hành động theo đúng hoặc tán thành [*n*hững g*i* mà *n*hững ng*o*ười có ảnh h*u*ơng đã đưa ra – *ng*ười *d*ịch]. Điều này dẫn đến một cơ chế khuếch đại, nơi mà các mẩu thông tin sai lệch đơn lẻ có thể được lan truyền một cách nhanh chóng và tạo dựng nên một lượng theo dõi trên Internet. Tác động đủ mạnh đến mức các quốc gia đã sử dụng những kỹ thuật này như một hình thức xung đột, còn được gọi là *chiến tranh hỗn hợp*, nơi thông tin được sử dụng để lay chuyển mọi người hướng đến một vị trí được những người đã truyền bá

nó ưa thích. Điều làm cho việc này trở nên hiệu quả là tác động tâm lý của các nhóm, trải qua hiệu ứng bầy đàn, nơi khi mà một người dẫn đầu và rất nhiều người làm theo, thường không cần xem xét kỹ lưỡng tiền đề mà họ đang tuân theo. Trong các cuộc chiến tranh trước đây, phương pháp này được gọi là *tuyên truyền*, và ngày nay, với sự truyền thông nhanh chóng trên toàn thế giới thông qua các nền tảng phương tiện truyền thông xã hội, những phương pháp này thậm chí còn hiệu quả hơn trong việc dịch chuyển niềm tin đa số của các nhóm cộng đồng dân cư.

### Các Nguyên tắc (Lý do Hiệu quả)

Kỹ thuật xã hội rất thành công vì hai nguyên nhân phổ quát. Đầu tiên là mong muốn cơ bản của hầu hết mọi người muốn trở nên hữu ích. Khi một ai đó hỏi một câu hỏi mà chúng ta đã biết câu trả lời, phản ứng bình thường của chúng ta không phải là nghi ngờ mà thay vào đó, chúng ta thường sẽ trả lời câu hỏi. Vấn đề với việc này nằm là rằng những thông tin trông có vẻ như vô hại có thể được sử dụng trực tiếp trong các cuộc tấn công hoặc gián tiếp để xây dựng một bức tranh rộng hơn mà kẻ tấn công có thể sử dụng để tạo ra một cảm giác xác thực trong một cuộc tấn công – một cá nhân càng có nhiều thông tin về tổ chức thì càng dễ dàng để thuyết phục những người khác rằng họ là một phần của tổ chức và thậm chí có quyền tiếp cận những thông tin nhạy cảm hơn.

Nguyên nhân thứ hai của sự thành công của các kỹ thuật xã hội là rằng các cá nhân thường tìm cách tránh các vấn đề và sự xung đột. Nếu như kẻ tấn công tìm cách đe dọa mục tiêu, hăm dọa rằng sẽ gọi cho quản lý của mục tiêu để nói về sự thiếu giúp đỡ, mục tiêu có thể sẽ đầu hàng và cung cấp thông tin để tránh xung đột. Những phần sau đây sẽ xem xét các khái niệm về thẩm quyền, đe dọa, sự đồng lòng, sự khan hiếm, sự quen thuộc, sự tin tưởng, và tính khẩn cấp được áp dụng cho việc sử

dụng chúng trong việc thúc đẩy một cuộc tấn công kỹ thuật xã hội thành công.

---



**LƯU Ý** Tính hiệu quả của các cuộc tấn công kỹ thuật xã hội là một phần kỹ thuật và một phần tâm lý. Để với một cuộc tấn công đánh lừa được hầu hết người dùng, các móc (hook) tâm lý được sử dụng để khiến cho các cuộc tấn công trở nên hiệu quả hơn trong việc khiến người dùng thực hiện một hành động mong muốn. Việc hiểu được thành phần tâm lý của các cuộc tấn công này là điều rất quan trọng.

### **Thẩm quyền**

Sử dụng *thẩm quyền* trong những tình huống xã hội có thể dẫn đến một môi trường nơi mà một bên cảm thấy rủi ro trong việc thách thức một bên khác về một vấn đề. Nếu một kẻ tấn công có thể đe dọa một mục tiêu rằng họ (kẻ tấn công) có thẩm quyền trong một tình huống cụ thể, họ có thể dụ dỗ mục tiêu hành động theo một cách cụ thể hoặc ngược lại, mục tiêu sẽ phải đổi mới với những hậu quả bất lợi. Nói tóm lại, nếu bạn hành động giống như một ông chủ khi yêu cầu một điều gì đó, mọi người sẽ ít có khả năng từ chối điều đó.

Biện pháp phòng thủ tốt nhất để chống lại rất nhiều cuộc tấn công kỹ thuật xã hội là một bộ các chính sách mạnh mẽ và không có ngoại lệ. Giống như với các vạch kẻ an ninh tại sân bay, khi đi đến điểm sàng lọc, mọi người phải được sàng lọc, thậm chí cả với phi hành đoàn, do đó, không có một phương pháp nào để vượt qua bước tối quan trọng này.

### **Sự đe dọa**

*Sự đe dọa* có thể rất tinh vi, thông qua sức mạnh nhận thức, hoặc trực tiếp hơn, thông qua việc sử dụng các biện pháp truyền thông giao tiếp

để xây dựng nên một kỳ vọng về sự ưu việt. Sử dụng chức danh của một ai đó, hoặc thông tin đăng nhập khác thường, giống như trở thành một “người đánh giá chính cho tiêu chuẩn”, tạo ra một bầu không khí uy quyền xung quanh tính cách của một ai đó.

### **Sự đồng thuận**

*Sự đồng thuận* là một quyết định quy mô toàn bộ-nhóm. Nó thường không đến từ một nhà vô địch, mà thay vào đó thông qua các vòng thương lượng nhóm. Những vòng này có thể được thao túng để đạt được những kết quả mong muốn. Kỹ sư xã hội chỉ đơn giản là thúc đẩy những người khác để đạt được những kết quả mong muốn của họ.

### **Sự khan hiếm**

Nếu một thứ gì đó đang khan hiếm và có giá trị cao thì việc đi đến với những thứ cần thiết có thể được tưởng thưởng – và chấp thuận. “Chỉ có vật dụng X với mức giá này” là một ví dụ về kỹ thuật này. Thậm chí ngay cả khi nếu một thứ gì đó không khan hiếm, được hàm ý chỉ sự khan hiếm, hoặc hàm ý những thay đổi trong tương lai không có sẵn, cũng có thể tạo ra một nhận thức về sự khan hiếm. Bằng cách tạo ra ấn tượng về *sự khan hiếm* (hoặc không cung cấp đủ) của một sản phẩm được mong đợi, một kẻ tấn công có thể thúc đẩy mục tiêu đưa ra một quyết định một cách nhanh chóng mà không nghi ngờ gì.

### **Sự quen thuộc**

Mọi người làm những điều cho những ai mà họ thích hoặc cảm thấy có mối liên hệ với họ. Việc xây dựng cảm giác *quen thuộc* và hấp dẫn này có thể dẫn đến sự tin tưởng vào nhầm chỗ. Kỹ sư xã hội có thể tập trung vào cuộc đàm thoại về những mục quen thuộc chứ không phải khác biệt. Một lần nữa, việc dẫn dắt bằng cách thuyết phục rằng một người đã từng đến đó và làm một điều gì đó, ngay cả khi họ thực sự chưa làm, sẽ dẫn đến cảm giác “quen thuộc” mong muốn ở mục tiêu.

## Sự tin cậy

*Sự tin cậy* được xác định là có được một sự hiểu biết về cách mà một điều gì đó sẽ hoạt động như thế nào dưới những điều kiện cụ thể. Các kỹ sư xã hội có thể định hình nhận thức của một mục tiêu đến nơi mà họ sẽ áp dụng những phán đoán đối với phương trình tin cậy và đi đến những kết luận sai lầm. Toàn bộ mục tiêu của kỹ thuật xã hội không chỉ là bắt buộc mọi người làm những điều mà họ không muốn mà thay vào đó, tạo cho họ một lộ tuyến dẫn họ đến cảm giác là họ đang thực hiện những điều đúng đắn trong thời điểm đó.

## Tính khẩn cấp

Thời gian có thể được thao túng để thúc đẩy một cảm giác về *sự khẩn cấp* và đưa ra những lỗi tắt có thể dẫn đến những cơ hội can thiệp vào các quy trình. Những đề xuất bị giới hạn về mặt thời gian nên luôn bị coi là đáng nghi ngờ. Nhận thức chính là chìa khóa. Việc đưa ra cho mục tiêu một nguyên nhân để tin rằng họ có thể có được những lợi thế của một tình huống kịp thời, bất kể nó có thực tế hay không, đạt được kết quả của việc họ hành động theo một cách thức được mong đợi.



## MÁCH NƯỚC CHO KỲ THI

Điều then chốt trong mọi cuộc tấn công kỹ thuật xã hội là rằng bạn đang thao túng một cá nhân và những hành động của họ bằng cách thao túng nhận thức của họ về một tình huống. Một kỹ sư xã hội làm day dứt niềm tin, định kiến và khuôn mẫu của mọi người – để gây tổn hại cho nạn nhân. Đây chính là phá hoại khía cạnh con người của một hệ thống.

## Biện pháp phòng thủ

Mặc dù rất nhiều trong số các cuộc tấn công kỹ thuật xã hội có thể khiến cho bạn khó chịu và nghĩ rằng chúng không bao giờ hoạt động, nhưng

trên thực tế, chúng đã xảy ra, và hàng tỷ đô la đã mất đi hàng năm vì những phương pháp này. Dù cho nó là lừa đảo trực tiếp hoặc là những giai đoạn đầu tiên của một cuộc tấn công lớn hơn nhiều, những yếu tố đã được giới thiệu trong chương này được sử dụng tại mọi thời điểm bởi tin tặc và những kẻ tấn công. May mắn thay, những biện pháp phòng thủ hữu hiệu chống lại các cuộc tấn công kỹ thuật xã hội này dễ dàng thiết lập hơn những biện pháp phòng thủ đối với các cuộc tấn công mang tính kỹ thuật hơn. Việc ngăn chặn kỹ thuật xã hội bắt đầu bằng các chính sách và quy trình loại bỏ các lô tuyển dụng được sử dụng bởi các cuộc tấn công này. Quyền truy cập của khách viếng thăm, các quy tắc trước khi hỗ trợ khách hàng, xác minh các yêu cầu là hợp pháp trước khi chia sẻ các yếu tố nhạy cảm nhất định — đây đều là những hạng mục có thể thực hiện được. Một khi bạn đã có các chính sách và thủ tục được phân lớp để tránh những vấn đề này hoặc những kết quả của chúng, thì yếu tố quan trọng chính là đào tạo nhân viên. Việc duy trì sự cảnh giác đối với các hành động của nhân viên là một thách thức và việc thường xuyên nhắc nhở, đào tạo lại và thông báo về các vi phạm có thể tiến một bước dài trong việc giúp bạn đạt được sự bảo vệ mong muốn. Cuối cùng, có nhiều lớp bảo vệ, bao gồm những sự phê duyệt và các biện pháp bảo vệ liên quan để một sai lầm của nhân viên sẽ không trao đi chìa khóa cho vương quốc. Ngoài ra, một lượng kiến thức lành mạnh, thông qua việc chia sẻ các trường hợp lớn bắt đầu bởi các kỹ thuật xã hội dưới hình thức các chiến dịch nâng cao nhận thức cộng đồng sẽ giữ cho nhân viên phòng vệ một cách tích cực trước kỹ thuật xã hội.



**LƯU Ý** Rất nhiều trường hợp “hacking” nổi tiếng đã bắt đầu với kỹ thuật xã hội:

- Xâm phạm dữ liệu mục tiêu, 2013: phishing email,
- Sony, 2014: phishing,
- Rò rỉ email của Ủy ban Quốc gia Đảng Dân chủ, 2016: spear phishing,
- Tấn công lưới điện Ukrainam 2018: phishing.

## Tóm tắt Chương

Chương này đã kiểm tra một loạt các công cụ và kỹ thuật khác nhau được sử dụng trong kỹ thuật xã hội. Việc sử dụng hành vi lừa dối để khiến người dùng trả lời tin nhắn qua các kênh truyền thông giao tiếp khác nhau bao gồm phishing, smishing, vishing, spear phishing, spam, SPIM, and whaling. Chương này cũng đề cập đến các phương pháp vật lý như tailgating, dumpster diving và shoulder surfing. Các kỹ thuật khác như watering holes, credentials harvesting, typosquatting và influence campaigns cũng được đề cập đến. Chương này kết thúc với việc kiểm tra một số đặc điểm tâm lý khiến người dùng dễ bị tấn công kỹ thuật xã hội cũng như các kỹ thuật để bảo vệ chống lại kỹ thuật xã hội.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Khi đang đợi khách ở sảnh của tòa nhà của bạn, bạn chú ý đến một người đàn ông mặc một chiếc áo sơ mi màu đỏ đang đứng gần một cánh cửa đã khóa với một chiếc hộp lớn trong tay. Anh ta đang đợi một ai đó để đi cùng và mở ra cánh cửa đã khóa và đi theo cô ấy vào bên trong. Kiểu tấn công kỹ thuật xã hội nào mà bạn vừa được chứng kiến?  
**A. Impersonation**  
**B. Phising**  
**C. Boxing**  
**D. Tailgating.**
2. Một đồng nghiệp yêu cầu bạn cho lời khuyên về việc tại sao anh ta không thể đăng nhập vào tài khoản Gmail của anh ta. Khi xem xét trình duyệt của anh ta, bạn nhận thấy anh ta đã nhập [www.gmal.com](http://www.gmal.com) vào thanh địa chỉ của trình duyệt. Màn hình trông rất giống màn hình đăng nhập Gmail. Đồng nghiệp của bạn đã là nạn nhân của kiểu tấn công nào?  
**A. Jamming**  
**B. Rainbow table**  
**C. Whale phishing**  
**D. Typosquatting.**
3. Một người dùng trong tổ chức của bạn liên hệ với bạn để xem liệu có bất kỳ cập nhật nào về "sự xâm phạm tài khoản" đã diễn ra trong tuần trước. Khi bạn yêu cầu anh ta giải thích về yêu cầu của anh ta, và người dùng nói với bạn rằng anh ta nhận được một

cuộc gọi vào đầu tuần từ bộ phận của bạn và đã yêu cầu xác minh mã định danh người dùng và mật khẩu của anh ta. Người dùng nói rằng anh ta đã đưa mã định danh người dùng và mật khẩu của mình cho người gọi. Người dùng này đã là nạn nhân của kiểu tấn công cụ thể nào?

- A. Spear phishing**
  - B. Vishing**
  - C. Phishing**
  - D. Replication**
4. Khi đến văn phòng của mình, bạn đã nghe được một cuộc hội thoại giữa hai nhân viên an ninh. Một người đang nói cho người kia rằng cô ấy đã bắt gặp một số người đào bới các thùng rác phía sau tòa nhà trong sáng sớm hôm nay. Nhân viên an ninh nói rằng những người đó giải thích rằng họ tìm kiếm những lon nhôm [*tìm phế liệu – người dịch*] – nhưng không có bất kỳ cái lon nào, chỉ có một túi đầy những giấy tờ. Kiểu tấn công nào mà nhân viên an ninh này đã được chứng kiến?
- A. Spear phishing**
  - B. Pharming**
  - C. Dumpster diving**
  - D. Rolling refuse.**
5. Những điều nào dưới đây đặc biệt được sử dụng để lan truyền ảnh hưởng, thay thế nhận thức, và gây ảnh hưởng đến mọi người, hướng đến một vị trí được yêu thích bởi người đang lan truyền nó?
- A. Gian lận danh tính, lừa đảo hóa đơn, thu thập thông tin đăng nhập (Identity fraud, invoice scams, credential harvesting)**
  - B. Lừa bịp, thông tin rõ ràng, khẩn cấp (Hoaxes, eliciting information, urgency)**

- C.** Chiến dịch gây ảnh hưởng, phương tiện xã hội, chiến tranh hỗn hợp (Influence campaigns, social media, hybrid warfare)
- D.** Thẩm quyền, đe dọa, đồng thuận (Authority, intimidation, consensus).
- 6.** Những điều nào dưới đây là một kiểu tấn công kỹ thuật xã hội mà theo đó, một kẻ tấn công cõi gắng có được những thông tin nhạy cảm từ một người dùng bằng cách giả mạo như một thực thể đáng tin cậy trong một email?
- A.** Phishing
- B.** Pharming
- C.** Spam
- D.** Vishing.
- 7.** (Những) Điều nào dưới đây là các công cụ tâm lý được sử dụng bởi kỹ sư xã hội để tạo ra niềm tin sai lầm nơi một mục tiêu?
- A.** Impersonation
- B.** Urgency hoặc scarcity
- C.** Authority
- D.** Tất cả những điều trên.
- 8.** Khi các chính sách bảo mật của một tổ chức đã được xác lập, phương pháp duy nhất có hiệu quả để đối phó với các cuộc tấn công kỹ thuật xã hội tiềm năng là gì?
- A.** Một chương trình nâng cao nhận thức bảo mật có hiệu lực
- B.** Một cơ chế kiểm soát truy cập vật lý tách biệt cho từng bộ phận trong tổ chức
- C.** Kiểm nghiệm thường xuyên cả các thủ tục bảo mật vật lý lẫn sử dụng điện thoại thực tế của tổ chức
- D.** Triển khai các thẻ kiểm soát truy cập và đeo các huy hiệu xác thực bảo mật.

- 9.** Bạn nhận thấy một nhân viên bảo vệ mới trong văn phòng, đi làm sớm hơn bình thường, đổ các thùng rác và di chuyển chậm rãi qua những người khác đang làm việc. Bạn hỏi anh ta rằng nhân viên thường ngày đâu và bằng một thứ tiếng Anh đứt quãng, anh ta nói rằng "Nghỉ ốm", chỉ ra một cơn ho. Điều gì đang diễn ra?
- A.** Watering hole attach
  - B.** Impersonation
  - C.** Prepending
  - D.** Identity fraud.
- 10.** Ông chủ của bạn cảm ơn bạn về những bức hình bạn đã gửi từ đợt dã ngoại gần đây của công ty. Bạn hỏi ông ấy rằng ông ấy đang nói về điều gì, và ông ấy nói rằng ông đã nhận được một email từ bạn với những tấm hình từ buổi dã ngoại. Biết rằng bạn đã không gửi cho ông ấy email đó, kiểu tấn công nào mà bạn ngờ là đang diễn ra?
- A.** Phising
  - B.** Spear phishing
  - C.** Reconnaissance
  - D.** Impersonation.

## Đáp án

1. **D** Tailgating (hoặc piggybacking) là một chiến thuật đơn giản khi đi gần sát một người chỉ vừa sử dụng thẻ, chìa khóa hoặc mã PIN truy cập của mình để có được quyền truy cập vật lý vào một phòng hoặc một tòa nhà. Chiếc hộp lớn rõ ràng là đang ngăn cản khả năng mở cửa của người đàn ông mặc áo sơ mi màu đỏ, do đó họ nhờ ai đó mở cửa và đi theo người đó vào bên trong.
2. **D** Typosquatting tận dụng các lỗi đánh máy phổ biến, chẳng hạn như gmal thay vì gmail. Kẻ tấn công đăng ký một tên miền rất giống với tên miền thực tế và cố gắng thu thập thông tin đăng nhập hoặc những thông tin nhạy cảm khác từ những người dùng ngây thơ và không nghi ngờ gì.
3. **B** Vishing là một cuộc tấn công kỹ thuật xã hội sử dụng công nghệ giao tiếp bằng giọng nói để thu thập những thông tin mà kẻ tấn công đang tìm kiếm. Rất thường xuyên, kẻ tấn công sẽ gọi cho một nạn nhân và giả vờ là một ai đó khác trong một nỗ lực truy xuất thông tin từ nạn nhân.
4. **C** Dumpster diving là quá trình tìm kiếm trong thùng rác của mục tiêu với hy vọng tìm thấy những thông tin có giá trị như các danh sách người dùng, danh bạ, sơ đồ tổ chức, bản đồ hệ thống mạng, mật khẩu, v.v...
5. **C** Influence campaigns được sử dụng để thay thế nhận thức và thay đổi tư duy của mọi người về một chủ đề. Chúng thậm chí còn mạnh mẽ hơn khi được sử dụng kết hợp với các phương tiện truyền thông xã hội để lan truyền sự ảnh hưởng thông qua sự truyền bá của người gây ảnh hưởng. Các quốc gia thường sử dụng chiến tranh hối hợp để gây ảnh hưởng lên mọi người để hướng đến một vị thế được yêu thích bởi những ai lan truyền nó.

6. **A** Đây là định nghĩa về một cuộc tấn công phishing, như đã được đưa ra trong chương. Phần tử then chốt của câu hỏi là email và bản chất không được mong đợi của việc gửi nó (spam).
7. **D** Các kỹ sư xã hội sử dụng một loạt các mánh khốe tâm lý để lừa bịp người dùng tin vào chúng, bao gồm giả mạo thẩm quyền, mạo danh, tạo ra một cảm giác về sự khan hiếm hoặc khẩn cấp, và khẳng định về sự quen thuộc.
8. **A** Bởi vì bất kỳ nhân viên nào cũng có thể là đích nhắm mục tiêu của một cuộc tấn công kỹ thuật xã hội, do đó, điều tốt nhất bạn có thể làm để bảo vệ tổ chức của bạn trước những cuộc tấn công này là triển khai một chương trình nâng cao nhận thức về bảo mật tích cực để đảm bảo rằng tất cả nhân viên đều hiểu rõ về mối đe dọa và những gì họ có thể làm để giải quyết nó.
9. **B** Đây có nhiều khả năng là một cuộc tấn công mạo danh, sử dụng vỏ bọc của người gác cổng. Bởi vì những tình huống bất thường, sẽ là khôn ngoan khi báo cáo cho một nhà quản lý để tiếp tục điều tra.
10. **B** Đây là spear phishing, vốn là một cuộc tấn công phishing được nhắm mục tiêu để chống lại một cá nhân cụ thể.

## Chương 2     Các Kiểu Chỉ báo Tấn công

### Các Kiểu Chỉ báo Tấn công

Trong chương này, bạn sẽ

- So sánh và đối chiếu các kiểu tấn công khác nhau,
- Học cách phân tích các chỉ báo tiềm năng để xác định kiểu của cuộc tấn công

Các cuộc tấn công có thể được thực hiện đối với hầu như bất kỳ lớp hoặc cấp độ phần mềm nào, từ các giao thức mạng cho đến các ứng dụng. Khi một kẻ tấn công tìm thấy một lỗ hổng trong một hệ thống, chúng khai thác điểm yếu để tấn công hệ thống. Ảnh hưởng của một cuộc tấn công tùy thuộc vào dự định của kẻ tấn công và có thể dẫn tới một loạt các ảnh hưởng khác, từ thứ yếu đến cực kỳ nghiêm trọng. Một cuộc tấn công vào một hệ thống có thể không hữu hình đối với hệ thống đó bởi vì cuộc tấn công thực tế diễn ra trên một hệ thống khác, và dữ liệu mà kẻ tấn công sẽ kiểm soát trên hệ thống thứ hai có được bằng cách tấn công hệ thống thứ nhất. Các cuộc tấn công có thể chống lại người dùng, như trong kỹ thuật xã hội, hoặc chống lại các ứng dụng, mạng, hoặc các thành phần mã hóa đang được sử dụng trong một hệ thống. Chương này so sánh và đối chiếu các kiểu tấn công này.

Dấu cho tin tặc và vi-rút máy tính nhận được hầu hết sự quan tâm trong các bản tin, chúng không chỉ là các phương pháp được sử dụng để tấn công các hệ thống máy tính và mạng. Chương này xác định rất nhiều cách thức khác nhau để đe dọa đến ít nhất là một trong ba yêu cầu bảo mật: tính bảo mật, tính toàn vẹn và tính sẵn sàng (tam giác CIA về bảo mật).

Từ một quan điểm cấp cao, các cuộc tấn công vào những hệ thống và mạng máy tính có thể được nhóm thành 2 nhóm chính: tấn công vào phần mềm cụ thể (chẳng hạn như một ứng dụng hoặc hệ điều hành) và tấn công vào giao thức hoặc dịch vụ cụ thể. Các cuộc tấn công vào một ứng dụng hoặc hệ điều hành cụ thể nói chung là khả thi vì sự sai sót trong mã (và có khả năng trong việc kiểm nghiệm mã phần mềm đó) hoặc do một khiếm khuyết hoặc lỗi trong mã (một lần nữa cho thấy thiếu sự kiểm tra kỹ lưỡng). Các cuộc tấn công vào các giao thức hoặc dịch vụ cụ thể là những nỗ lực nhằm lợi dụng một tính năng cụ thể của giao thức hoặc dịch vụ hoặc sử dụng nó theo một cách mà nó không được dự kiến. Chương này thảo luận về các hình thức tấn công khác nhau mà các chuyên gia bảo mật cần phải nhận biết được.

### **Mục tiêu Chứng nhận**

Chương này đề cập đến mục tiêu kỳ thi CompTIA Security+ 1.2: Đưa ra một kịch bản, phân tích các chỉ báo tiềm năng để xác định kiểu tấn công.

## Phần mềm độc hại (Malware)

*Malware* đề cập đến một phần mềm được thiết kế cho mục đích xấu xa. Những phần mềm như vậy có thể được thiết kế để phá hoại một hệ thống, chẳng hạn như xóa tất cả các tập tin, hoặc nó có thể được thiết kế để tạo ra một cổng hậu trong hệ thống để cấp quyền truy cập cho những cá nhân trái phép. Thường thì việc cài đặt malware được thực hiện sao cho những cá nhân được phép không quan sát được quá trình này. Một số kiểu khác nhau của phần mềm độc hại có thể được sử dụng, chẳng hạn như vi-rút, ngựa trojan, bom logic, phần mềm gián điệp, và sâu [máy tính], và chúng khác nhau trong cách thức chúng được cài đặt và mục đích của chúng.

## Ransomware

*Ransomware* là một dạng phần mềm độc hại thực hiện một số hành động và đòi tiền chuộc từ người dùng. Ransomware thường mã hóa các tập tin trên một hệ thống và sau đó khiếu cho chúng vĩnh viễn không thể sử dụng được, hoạt động giống như kiểu từ chối dịch vụ, hoặc tạm thời cho đến khi tiền chuộc được trả, do đó mới có tên gọi là ransomware (phần mềm tống tiền). Ransomware thường là một sâu máy tính, hoàn toàn tự động, và khi được nhắm mục tiêu như là phương tiện để từ chối dịch vụ thì cơ chế sửa chữa duy nhất là xây dựng lại hệ thống. Việc này có thể tiêu tốn thời gian và/hoặc không thực tế trong một số trường hợp, khiến cho cơ chế tấn công này tương đương với việc phá hủy tài sản vật lý.

Một mối đe dọa ransomware hiện tại, xuất hiện lần đầu tiên vào năm 2013, là CryptoLocker. CryptoLocker là một ngựa trojan mã hóa những tập tin nhất định bằng cách sử dụng khóa mã hóa công khai RSA. Khi người dùng cố gắng lấy lại những tập tin đó, họ được cung cấp một thông điệp hướng dẫn họ cách làm thế nào để trả tiền cho khóa giải mã. Bởi vì

hệ thống sử dụng mã hóa RSA-2048 bit, việc giải mã bằng cách dò tìm cưỡng bức (brute force) nằm ngoài phạm vi của các tùy chọn khôi phục. Hệ thống có tính tự động hóa cao và người dùng chỉ có rất ít thời gian để lấy được khóa riêng tư. Thất bại trong việc lấy được khóa giải mã sẽ dẫn đến mất dữ liệu. Trong năm 2017, một sâu tống tiền có tên gọi là NotPetya đã lây lan trên quy mô toàn cầu, chỉ tấn công một số công ty, nhưng một khi nó tấn công ở đâu thì nó sẽ phá hủy mọi thứ. Nguyên nhân là mặc dù nó trông có vẻ và hoạt động giống như ransomware nhưng nó không có khóa giải mã. Vào khoảng đầu năm 2017, một khuynh hướng ransomware có tên gọi là WannaCry đã tấn công rất nhiều công ty, bao gồm cả Dịch vụ Y tế Quốc gia của Vương quốc Anh (NHS). Ransomware này đã tạo ra sự hỗn loạn bằng cách khai thác lỗ hổng ExternalBlue trong các hệ thống Microsoft Windows đã bị phát hiện bởi một nhóm có tên gọi là Shadow Broker. WannaCry đã bị ngăn chặn lại bởi một hacker mũ trắng, Marcus Hutchins, người đã tìm ra một lỗ hổng trong sâu WannaCry và có thể vô hiệu hóa nó trên toàn cầu.



## MÁCH NƯỚC CHO KỲ THI

Ransomware là một dạng malware khóa người dùng khỏi các tập tin của họ hoặc thậm chí toàn bộ thiết bị cho đến khi một khoản thanh toán tiền chuộc trực tuyến được trả để khôi phục lại quyền truy cập.

## Ngựa Trojan (Trojans)

Một trojan horse, hoặc đơn giản là *trojan*, là một mảnh phần mềm xuất hiện để làm một điều gì đó (và có thể, trong thực tế, thực sự làm điều đó) nhưng ẩn giấu một vài tính năng khác. Sự tương đồng với câu chuyện nổi tiếng của thời cổ đại (*câu chuyện Ngựa gỗ thành Troy – người dịch*) là rất chính xác. Trong câu chuyện nguyên thủy, vật thể xuất hiện như là

một con ngựa gỗ lớn, và thực tế đúng là như vậy. Nhưng đồng thời, nó còn ẩn dấu một điều gì đó nham hiểm và nguy hiểm hơn nhiều đối với những người dân cư ngụ trong thành phố Troy. Chừng nào con ngựa vẫn còn được đặt bên ngoài tường thành, nó có thể sẽ không gây ra thiệt hại cho cư dân. Tuy nhiên, nó đã được tiếp nhận bởi những người dân thành Troy, và chính từ bên trong, mục đích ẩn giấu đã được kích hoạt. Trojan máy tính cũng hoạt động theo cùng một cách. Không giống như vi-rút, vốn sinh sản bằng cách tự gắn vào các tập tin hoặc chương trình khác, trojan là một chương trình độc lập phải được sao chép và cài đặt bởi người dùng - nó phải được "đưa vào bên trong" hệ thống bởi người dùng được cấp phép. Thách thức đối với kẻ tấn công nằm ở chỗ lôi kéo người dùng sao chép và chạy chương trình. Điều này nói chung có nghĩa là chương trình phải được ngụy trang thành thứ gì đó mà người dùng muốn chạy – chẳng hạn như một tiện ích đặc biệt hoặc một trò chơi. Một khi nó đã được sao chép và nằm bên trong hệ thống, trojan sẽ thực hiện mục đích được ẩn dấu của nó mà người dùng thường vẫn không nhận biết về bản chất thực sự của nó.

Một ví dụ điển hình về trojan là Back Orifice (BO), ban đầu được tạo ra vào năm 1999 và hiện được cung cấp trong một số phiên bản. BO có thể được gắn vào một số loại chương trình khác nhau. Khi nó đã được đính kèm và khi một tập tin bị nhiễm được chạy, BO sẽ tạo ra một cách thức để các cá nhân trái phép tiếp quản hệ thống từ xa, như thể họ đang ngồi trước bảng điều khiển. BO được thiết kế để hoạt động với các hệ thống dựa trên Windows. Rất nhiều trojan giao tiếp với bên ngoài thông qua một cổng mà trojan mở ra và đây là một trong những cách trojan có thể được phát hiện.



**MÁCH NƯỚC CHO KỲ THI** Hãy đảm bảo rằng bạn hiểu được sự khác biệt giữa vi-rút, sâu, trojan và các kiểu mối đe dọa khác cho kỳ thi.

### Sâu (Worm)

Việc phân biệt giữa sâu và vi-rút đã từng rất dễ dàng. Gần đây, với sự ra đời của các loại mã độc tinh vi mới, sự phân biệt đã bị mờ đi. *Sâu* là những đoạn mã phần mềm cố gắng xâm nhập vào mạng và hệ thống máy tính. Một khi sự xâm nhập xảy ra, sâu sẽ tạo ra một bản sao mới của chính nó trên hệ thống bị xâm nhập. Do đó, sự sinh sản của một con sâu không phụ thuộc vào việc gắp vi-rút vào một đoạn mã khác hoặc vào một tập tin, vốn là định nghĩa về vi-rút.

Vi-rút thường được coi là một vấn đề dựa trên hệ thống và sâu là một vấn đề dựa trên mạng. Nếu mã độc được gửi qua mạng, sau đó nó có thể được gọi là sâu. Tuy nhiên, điểm khác biệt quan trọng là liệu mã đó có phải tự gắn chính nó vào một thứ khác (vi-rút) hay nó có thể tự "tồn tại" (một sâu) hay không.

Một số ví dụ về sâu có nổi tiếng bao gồm sâu Sobig năm 2003, sâu SQL Slammer năm 2003, cuộc tấn công Code Red và Nimda năm 2001 và sâu Zotob năm 2005 đã hạ gục CNN Live. Nimda đặc biệt ấn tượng ở chỗ nó sử dụng 5 phương pháp khác nhau để phát tán: qua email, qua mạng chia sẻ mở, từ việc duyệt các trang web bị nhiễm, sử dụng lỗ hổng truyền tải thư mục của Microsoft IIS 4.0/5.0 và ấn tượng nhất là thông qua việc sử dụng backdoor được để lại bởi Code Red II và sâu sadmind. Gần đây, sâu đã trở thành một công cụ được lựa chọn cho các cuộc tấn công ransomware, vì chúng có thể lây lan từ hệ thống này sang hệ thống khác.

mà không cần sự can thiệp của nhân viên vận hành. Sâu NotPetya năm 2017 đã gây ra thiệt hại ước tính 10 tỷ USD.

---



**MÁCH NƯỚC CHO KỲ THI** Sâu hoạt động giống như vi-rút nhưng còn có thêm khả năng di chuyển mà không cần hành động can thiệp của con người. Chúng không cần sự giúp đỡ để lây lan.

### **Chương trình Không mong muốn Tiềm ẩn**

*Chương trình không mong muốn tiềm ẩn (PUP)* là một tên gọi được sử dụng bởi các công ty bảo mật và các nhà cung cấp phần mềm chống vi-rút để xác định các chương trình mà có thể có những ảnh hưởng xấu đến bảo mật hoặc quyền riêng tư của một máy tính. Thường thì các chương trình này liên quan đến các thành phần phần mềm quảng cáo hoặc các phần mềm gián điệp và được sử dụng cho mục đích tạo ra doanh thu.

---



**LƯU Ý** Các chương trình không mong muốn tiềm ẩn là một dạng phần mềm độc hại (malware). Tên gọi được ngành lựa chọn vì người tạo ra các PUP yêu cầu bạn đọc và thõng nhất với các điều khoản của họ như một phần của một thỏa thuận tải về. Bạn có thể dễ dàng bỏ qua những chi tiết này khi đang cài đặt chương trình và sau đó, bạn có những ứng dụng không mong muốn. PUP có thể biểu lộ một số đặc điểm không được mong đợi, chẳng hạn như:

- Làm chậm máy tính của bạn,
- Hiển thị hàng đống các quảng cáo gây khó chịu,
- Bổ sung thêm các thanh công cụ gây chiếm không gian trên trình duyệt,

- Thu thập thông tin cá nhân.

Một nguồn PUP phổ biến là các trang tải về của bên-thứ-ba để tải các ứng dụng – thậm chí ngay cả các ứng dụng hợp pháp cũng có thể được đóng gói bởi các nhà phân phối bên-thứ-ba. Việc sử dụng một giải pháp chống phần mềm độc hại (anti-malware) phải bắt được và cho phép dừng các PUP trước khi cài đặt.

### **Vi-rút Fileless**

Hầu hết các giải pháp chống vi-rút/chống phần mềm độc hại đều tìm kiếm phần mềm độc hại thông qua việc giám sát việc ghi lên hệ thống tập tin và sau đó lọc các lần ghi đối với các chữ ký đã biết. Khi một mẫu phần mềm độc hại hoạt động chỉ trong bộ nhớ và không bao giờ đụng chạm đến hệ thống tập tin thì sẽ khó phát hiện hơn nhiều. Kiểu tấn công này được gọi là *vi-rút fileless*, hoặc tấn công dựa trên-bộ nhớ.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng không như các vi-rút truyền thống, vốn tự đính kèm chúng vào một tập tin, một vi-rút fileless cư trú trong bộ nhớ và sẽ tiếp tục hoạt động cho đến khi thiết bị được tắt đi.

### **Điều khiển và Kiểm soát**

Các máy chủ điều-khiển-và-kiểm-soát được sử dụng bởi những kẻ tấn công để kiểm soát phần mềm độc hại đã được khởi chạy để chống lại các mục tiêu. Sự lây nhiễm phần mềm độc hại hiếm khi xảy ra ở một tập tin đơn lẻ trên một máy đơn lẻ khi một cuộc tấn công diễn ra trong một doanh nghiệp. Rất nhiều thành phần phần mềm độc hại, trên nhiều hệ thống, với các ID khác nhau, tất cả đều hoạt động để cung cấp một phương tiện cho tin tặc để xâm nhập lại hệ thống, thường được thấy trong các doanh nghiệp. Những thành phần phần mềm độc hại này cũng hoạt động để lọc lại dữ liệu đã bị đánh cắp.

## Các Bot

Một *bot* là một mẩu đang hoạt động của phần mềm thực hiện một số tác vụ, dưới sự kiểm soát của một chương trình khác. Một loạt các bot được kiểm soát trên hệ thống mạng trong một nhóm, và tổ hợp toàn bộ được gọi là một *botnet* (kết hợp hai thuật ngữ *bot* và *network*). Một số botnet là hợp pháp và thực hiện những hành động được mong muốn theo cách phân tán. Các botnet bất hợp pháp hoạt động theo cùng cách thức, với các bot phân tán và được kiểm soát từ một bộ các máy chủ kiểm soát và điều khiển trung tâm. Các bot có thể thực hiện hàng loạt công việc – từ việc làm gia tăng thư rác cho đến thực hiện hành vi gian lận, cài đặt phần mềm gián điệp, v.v...

Các botnet tiếp tục làm gia tăng các mối đe dọa phần mềm độc hại. một số botnet mới nhất được thiết kế để đào bitcoin, bằng cách sử dụng năng lực xử lý được phân tán để có được lợi nhuận. Một trong những botnet nổi tiếng hơn cả là Zeus, một botnet thực hiện việc ghi lén tổ hợp phím và được sử dụng chủ yếu cho mục đích đánh cắp thông tin ngân hàng. Zeus đã từng được liên kết với việc phát tán ransomware CryptoLocker. Một botnet nổi tiếng khác là Conficker, đã lây nhiễm cho hàng triệu máy tính trên toàn cầu. Botnet Conficker là một trong những phần mềm độc hại đã từng được nghiên cứu nhiều nhất, với một nhóm công tác chung chính phủ-ngành được triệu tập để chống lại nó.

## Crypto-malware

Suy nghĩ đầu tiên khi một ai đó nhìn thấy từ *crypto-malware* là nghĩ về ransomware. Tuy nhiên, điều này là một sai lầm. *Crypto-malware* là tên gọi của ngành bảo mật đưa ra đổi với phần mềm độc hại sử dụng những tài nguyên của hệ thống để khai thác tiền mã hóa. Đây thực sự chỉ là kiểu tấn công đánh-cắp-dịch-vụ, khi một kẻ tấn công sử dụng các chu kỳ

của CPU trên máy tính của người khác để thực hiện việc khai thác tiền điện tử.

### Bom Logic

Các bom logic, không giống như vi-rút và trojan, là một kiểu phần mềm độc hại được cài đặt một cách có chủ đích, thường là bởi một người dùng đã được cấp phép. Một *bom logic* là một đoạn mã phần mềm nằm Quản lý Sự cố trong một khoảng thời gian cho đến khi một số sự kiện hoặc ngày tháng nào đó gọi ra tải trọng độc hại của nó. Một ví dụ về một bom logic có thể là một chương trình được thiết lập để tải và chạy một cách tự động, và đồng thời kiểm tra định kỳ cơ sở dữ liệu nhân sự hoặc bảng lương của tổ chức đối với một nhân viên cụ thể. Nếu như nhân viên không được tìm thấy, tải trọng độc hại sẽ thực thi, xóa đi các tập tin quan trọng của công ty.

Nếu như sự kiện là một ngày hoặc thời điểm cụ thể, chương trình thường sẽ được gọi là một *bom thời gian/bom hẹn giờ*. Trong một ví dụ nổi tiếng, một nhân viên bất mãn đã để lại một quả bom hẹn giờ ngay trước khi bị sa thải. Hai tuần sau, hàng ngàn hồ sơ khách hàng đã bị xóa. Cuối cùng, cảnh sát đã có thể lần ra mối liên hệ giữa mã độc với người nhân viên cũ bất mãn, người đã bị truy tố vì hành động của anh ta. Anh ta đã hy vọng rằng hai tuần trôi qua kể từ khi bị sa thải sẽ khiến các nhà điều tra cho rằng anh ta không thể là người đã gây ra việc mất các xóa hồ sơ.

Bom logic rất khó bị phát hiện vì chúng thường được cài đặt bởi người dùng có thẩm quyền và đặc biệt, đã được cài đặt bởi các quản trị viên, những người cũng thường chịu trách nhiệm về bảo mật. Điều này cho thấy sự cần thiết của việc tách bạch các nhiệm vụ và đánh giá định kỳ tất cả các chương trình và dịch vụ đang chạy trên một hệ thống. Nó cũng minh họa sự cần thiết phải duy trì một chương trình sao lưu chủ động để nếu tổ chức của bạn mất các tập tin quan trọng cho loại mã phần mềm

độc hại này, nó sẽ chỉ mất các giao dịch đã xảy ra kể từ lần sao lưu gần đây nhất, dẫn đến việc không bị mất dữ liệu vĩnh viễn.

### **Phần mềm gián điệp**

*Phần mềm gián điệp* là một phần mềm “bí mật theo dõi” người dùng, ghi lại và báo các về các hoạt động của họ. Thường được cài đặt mà không cần đến kiến thức của người dùng, phần mềm gián điệp có thể thực hiện một loạt các hoạt động. Nó có thể ghi lại tổ hợp phím (thường hay được gọi là *keylogging*) khi người dùng đăng nhập vào một trang web cụ thể. Nó có thể giám sát cách thức một người dùng sử dụng một phần mềm cụ thể, chẳng hạn như theo dõi những nỗ lực gian lận trong các trò chơi. Thoạt nhìn ban đầu, rất nhiều cách sử dụng phần mềm gián điệp trông có vẻ như vô hại, nhưng việc giám sát trái phép một hệ thống có thể bị lạm dụng một cách dễ dàng. Trong các trường hợp khác, phần mềm gián điệp được thiết kế một cách đặc biệt để đánh cắp thông tin. Rất nhiều tiểu ban đã thông qua quy định cấm việc cài đặt phần mềm không được phê duyệt nhưng phần mềm gián điệp có thể vượt qua vấn đề này bằng những thỏa thuận cấp phép người-dùng-đầu-cuối phức tạp và gây nhầm lẫn.

### **Keylogger**

Như tên gọi của nó cho thấy, *một keylogger* là một phần mềm ghi lại mọi tổ hợp phím mà người dùng nhập vào. Keylogger theo khía cạnh riêng của nó không nhất thiết là xấu, vì bạn cũng có thể coi Microsoft Word là một keylogger. Điều khiến cho keylogger trở thành một phần mềm độc hại khi hoạt động của nó là (1) người dùng không xác định được và (2) không nằm dưới sự kiểm soát của người dùng. Keylogger đã được bán trên thị trường cho nhiều mục đích sử dụng - từ giám sát hoạt động của con bạn hoặc hoạt động của vợ/chồng, đến duy trì hồ sơ về những gì đã được thực hiện trên máy. Keylogger độc hại có một số đặc điểm cụ thể

như sau: chúng thường được ẩn khuất khỏi tầm nhìn của người dùng, thậm chí ngay cả khi xem xét trong Task Manager, và chúng được sử dụng để chống lại lợi ích của người dùng cuối. Các tin tức sử dụng keylogger để thu thập mật khẩu và các mảnh thông tin nhạy cảm khác, cho phép chúng sử dụng những bí mật này để hoạt động với tư cách là người dùng mà không cần sự đồng ý của người dùng. Chức năng keylogger thậm chí còn được tìm thấy trong các chương trình hợp pháp, nơi các lần nhấn phím được ghi lại cho các mục đích "hợp pháp" và sau đó được lưu trữ theo cách cho phép người dùng trái phép lấy cắp dữ liệu.

### **Trojan Truy cập Từ xa (Remote-Access Trojan)**

Một *Trojan truy cập từ xa (RAT)* là một bộ công cụ được thiết kế để cung cấp cung cấp khả năng giám sát bí mật và/hoặc khả năng truy cập trái phép vào hệ thống được nhắm mục tiêu. RAT thường bắt chước hành vi của keylogger và packet sniffer bằng cách sử dụng bộ sưu tập các lần gõ phím được tự động hóa, tên người dùng, mật khẩu, ảnh chụp màn hình, lịch sử trình duyệt web, email, nhật ký trò chuyện, v.v... nhưng chúng thực hiện điều đó với một thiết kế thông minh. RAT cũng có thể sử dụng phần mềm độc hại để lây nhiễm hệ thống bằng mã phần mềm có thể được sử dụng để tạo điều kiện thuận lợi cho việc khai thác mục tiêu. Thay vì chỉ thu thập thông tin, RAT trình bày nó cho kẻ tấn công dưới hình thức để tạo điều kiện cho khả năng truy cập trái phép vào máy mục tiêu. Điều này thường liên quan đến việc sử dụng các giao thức truyền thông đã được thiết lập cấu hình đặc biệt được thiết lập khi máy tính mục tiêu bị lây nhiễm lần đầu. Cổng hậu này vào máy mục tiêu có thể cho phép kẻ tấn công truy cập mà không bị kiểm soát, bao gồm khả năng giám sát hành vi của người dùng, thay đổi các cài đặt thiết lập máy tính, duyệt và sao chép các tập tin, truy cập vào hệ thống được kết nối, v.v... RAT thường được sử dụng bởi các tác nhân đe dọa có kỹ năng cao hơn, mặc

dù có những RAT đủ dễ dàng để ngay cả những người mới bắt đầu cũng có thể sử dụng được.

Một RAT nên được coi là một dạng khác của phần mềm độc hại, nhưng thay vì chỉ là một chương trình, nó còn có một người điều hành đứng đằng sau nó, hướng dẫn nó gây ra những thiệt hại dai dẳng hơn. RAT có thể được gửi qua email lừa đảo, tấn công kiểu vũng nước (watering holes) hoặc bất kỳ kiểu nào trong số vô số các vectơ lây nhiễm phần mềm độc hại khác. Các RAT thường liên quan đến việc tạo ra các cấu trúc tập tin ẩn trên hệ thống và dễ bị phát hiện bởi các chương trình chống phần mềm độc hại hiện đại. Có một số họ RAT chính, nhưng một danh sách đầy đủ sẽ dài và ngày càng gia tăng. Khi đổi mặt với một đối thủ lành nghề hơn, không có gì lạ khi tìm thấy các gói RAT đã được sửa đổi để sử dụng cụ thể, chẳng hạn như chương trình được sử dụng trong vụ tấn công lưới điện của Ukraine năm 2015.

## **Rootkit**

*Rootkit* là một dạng phần mềm độc hại được thiết kế một cách đặc biệt để sửa đổi hoạt động của hệ điều hành theo một số cách để tạo điều kiện cho chức năng không tiêu chuẩn. Lịch sử của rootkit quay trở lại thời kỳ đầu của hệ điều hành UNIX, nơi rootkit là tập hợp các công cụ quản trị đã được sửa đổi. Ban đầu được thiết kế để cho phép một chương trình kiểm soát tốt hơn các chức năng của một hệ điều hành khi nó bị lỗi hoặc không phản hồi, kỹ thuật này đã phát triển và được sử dụng theo nhiều cách khác nhau. Một trường hợp nổi tiếng đã xảy ra tại Sony BMG Corporation, khi công nghệ rootkit đã được sử dụng để cung cấp công nghệ bảo vệ bản sao trên một số đĩa CD của công ty. Có hai vấn đề chính khiến Sony trở thành một sự cố hoàn toàn: Đầu tiên, phần mềm đã sửa đổi hệ thống mà không có sự chấp thuận của người dùng. Thứ hai, phần mềm đã mở một lỗ hổng bảo mật trên các hệ thống chạy Windows, tạo ra

một lỗ hổng có thể bị khai thác ở cấp độ rootkit. Điều này khiến trường hợp của Sony bị gắn nhãn là *phần mềm độc hại*, đây là cách sử dụng rootkit phổ biến nhất.

Một rootkit có thể làm được nhiều thứ — trên thực tế, nó có thể làm hầu như mọi thứ mà hệ điều hành thực hiện. Rootkit sửa đổi hạt nhân của hệ điều hành và các chức năng hỗ trợ, thay đổi bản chất hoạt động của hệ thống. Rootkit được thiết kế để tránh, bằng cách phá hoại hoặc trốn tránh các chức năng bảo mật của hệ điều hành nhằm tránh việc bị phát hiện. Rootkit hoạt động như một dạng phần mềm độc hại có thể thay đổi mức độ ưu tiên của luồng để tăng hiệu suất của ứng dụng, thực hiện việc ghi nhật ký bàn phím, hoạt động như một sniffer, ẩn các tập tin khác khỏi các ứng dụng khác hoặc tạo ra các cổng hậu trong hệ thống xác thực. Việc sử dụng chức năng rootkit để ẩn các tiến trình và tập tin khác cho phép kẻ tấn công sử dụng một phần của máy tính mà người dùng hoặc các ứng dụng khác không thực sự biết điều gì đang xảy ra. Điều này ẩn giấu mã khai thác khỏi các chương trình chống vi-rút và chống phần mềm gián điệp, hoạt động giống như một tấm áo tang hình.

Rootkit có thể được tải trước khi hệ điều hành tải lên, hoạt động như một lớp ảo hóa, như trong SubVirt và Blue Pill. Rootkit có thể tồn tại trong phần firmware và chúng đã được chứng minh trong cả card video và card mở rộng. Rootkit có thể tồn tại dưới dạng các mô-đun thư viện có thể tải được, thay đổi một cách hiệu quả các phần của hệ điều hành nằm bên ngoài hạt nhân. Thông tin thêm về các rootkit cụ thể trong tự nhiên có thể được tìm thấy tại trang web [www.antirootkit.com](http://www.antirootkit.com).



## MÁCH NƯỚC CHO KỲ THI

Có 5 kiểu rootkit đang tồn tại: mức firmware, ảo, hạt nhân, thư viện và ứng dụng.

Khi một rootkit được phát hiện, nó cần phải được loại bỏ và làm sạch. Do bản chất xâm nhập của rootkit, và thực tế rằng rất nhiều khía cạnh của rootkit không thể được phát hiện một cách dễ dàng, hầu hết các quản trị viên hệ thống thậm chí còn không loại bỏ hoặc làm sạch rootkit. Việc sử dụng hình ảnh hệ thống sạch đã được chụp lại trước đó và xây dựng lại hình ảnh của máy dễ dàng hơn nhiều so với việc cố gắng xác định mức độ sâu và rộng của thiệt hại và cố gắng sửa chữa các tập tin riêng lẻ.

### Cổng hậu (Backdoor)

Ban đầu, Backdoor (và đôi khi vẫn là) không phải điều gì khác hơn là các phương pháp đã được các nhà phát triển phần mềm sử dụng để đảm bảo rằng họ có thể truy cập vào một ứng dụng, ngay cả khi có điều gì đó xảy ra trong tương lai để ngăn cản các phương pháp truy cập thông thường. Một ví dụ sẽ là một mật khẩu đã được mã hóa cứng có thể được sử dụng để truy cập vào chương trình trong trường hợp quản trị viên quên mất mật khẩu hệ thống của chính mình. Vẫn đề rõ ràng với loại cổng hậu này (đôi khi còn được gọi là *cửa sập/trapdoor*) là, bởi vì nó được mã hóa cứng nên nó không thể được gỡ bỏ. Nếu kẻ tấn công biết được cổng hậu, tất cả các hệ thống chạy phần mềm đó sẽ dễ bị tấn công.

Thuật ngữ *cổng hậu* cũng, và phổ biến hơn, được sử dụng để chỉ các chương trình mà kẻ tấn công cài đặt sau khi truy cập trái phép vào hệ thống để đảm bảo rằng chúng vẫn có thể tiếp tục có quyền truy cập không hạn chế vào hệ thống, thậm chí ngay cả khi phương thức truy cập ban đầu của chúng bị phát hiện và bị ngăn chặn. Cổng hậu cũng có thể được cài đặt bởi các cá nhân được ủy quyền một cách vô tình nếu họ chạy phần mềm có chứa trojan (như đã được giới thiệu trước đó). Các cổng hậu thông thường bao gồm NetBus và Back Orifice. Cả hai cổng hậu này, nếu chạy trên hệ thống của bạn, có thể cho phép kẻ tấn công truy cập từ xa vào hệ thống của bạn — quyền truy cập cho phép chúng thực hiện bất kỳ

chức năng nào trên hệ thống của bạn. Một biến thể của cỗng hậu là rootkit, đã được thảo luận trong phần trước, được thiết lập không phải để giành được quyền truy cập root mà là để đảm bảo quyền truy cập root vẫn được tiếp tục.



**MÁCH NƯỚC CHO KỲ THI** Mục tiêu kỳ thi Security+ bao gồm việc phân tích các chỉ báo tiềm năng để xác định kiểu của cuộc tấn công, bao gồm keylogger, phần mềm gián điệp, bot, RAT, bom logic, cỗng hậu, v.v... Để chuẩn bị cho kỳ thi, bạn nên hiểu được sự khác biệt giữa rất nhiều cuộc tấn công phần mềm độc hại đã được thảo luận trong chương này.

### Tấn công Mật khẩu

Hình thức xác thực phổ biến nhất là sự kết hợp mã định danh người dùng và mật khẩu. Mặc dù nó vốn dĩ không phải là một cơ chế xác thực kém nhưng sự kết hợp này vẫn có thể bị tấn công theo một số cách. Rất thường xuyên, những cuộc tấn công này đều mang lại những kết quả thuận lợi cho kẻ tấn công, không phải như là một kết quả của một điểm yếu trong lược đồ, mà thường do người dùng không tuân theo những thủ tục mật khẩu mạnh mẽ.

### Phun (Spraying)

*Phun (spraying)* mật khẩu là một cuộc tấn công sử dụng một số lượng giới hạn những mật khẩu phổ biến đã được sử dụng và áp dụng chúng cho một lượng lớn các tài khoản. Các cuộc tấn công brute-force truyền thống cố gắng cố gắng có được quyền truy cập trái phép vào một tài khoản đơn lẻ bằng cách đoán mật khẩu. Spraying lại thực hiện điều ngược lại, sử dụng một lượng mật khẩu giới hạn và cố gắng sử dụng chúng cho toàn bộ mọi mật khẩu. Đây là một cuộc tấn công hữu dụng khi bạn không quan tâm đến tài khoản mà bạn đang có và khá thành công khi đưa ra

với một tập hợp lớn các tài khoản. Việc chống lại điều này là rất quan trọng đối với tổ chức, bởi vì nếu một tài khoản bị xâm phạm thì đó là vị thế cần thiết để có được quyền thâm nhập.

## Từ điển

Một phương pháp khác để xác định mật khẩu là sử dụng một chương trình bẻ-khóa-mật-khẩu sử dụng một danh sách các từ trong từ điển để cố gắng đoán mật khẩu, do đó, được đặt tên là tấn công mật khẩu theo kiểu *từ điển*. Những từ ngữ có thể được sử dụng bởi chính bản thân chúng hoặc hai hoặc ba từ ngắn hơn có thể được kết hợp để hình thành nên một mật khẩu khả dĩ đơn lẻ. Một số lượng các chương trình bẻ-khóa-mật-khẩu thương mại và miễn-công-khai sử dụng một phương pháp biến đổi để bẻ khóa mật khẩu, bao gồm việc sử dụng các biến thể với mã định danh người dùng.

Những chương trình này thường cho phép kẻ tấn công tạo ra các quy tắc khác nhau để cho chương trình biết về cách thức kết hợp các từ ngữ như thế nào để hình thành nên những mật khẩu khả dĩ. Người dùng thường thay thế những con số nhất định cho các ký tự cụ thể. Nếu người dùng muốn sử dụng từ *secret* để làm mật khẩu, ví dụ, ký tự *e* có thể được thay thế bằng số *3*, tạo ra mật khẩu *s3cr3t*. Mật khẩu này sẽ không thể được tìm thấy trong từ điển, do đó một cuộc tấn công từ điển đơn thuần sẽ không thể bẻ khóa nó, nhưng mật khẩu này vẫn dễ nhớ đối với người dùng. Tuy nhiên, nếu như một quy tắc đã được tạo ra để cố gắng thử mọi từ trong từ điển và sau đó thử cùng những từ ngữ nhưng thay thế số *3* cho ký tự *e* thì mật khẩu có thể sẽ bị bẻ khóa.

Các quy tắc cũng có thể được định nghĩa để từ đó chương trình bẻ-khóa-mật-khẩu sẽ thay thế những ký tự đặc biệt cho những ký tự khác hoặc kết hợp các từ ngữ. Khả năng kẻ tấn công bẻ khóa được mật khẩu liên quan trực tiếp đến phương pháp mà người dùng sử dụng để tạo ra mật

khẩu trong lần đầu tiên, cũng như là từ điển và các quy tắc được sử dụng.

Một cuộc tấn công kiểu từ điển liên quan đến việc sử dụng một bảng tra cứu để thử và tìm ra một đáp án. Với suy nghĩ đó, việc sử dụng mật khẩu lặp lại nhiều lần, cùng với sự vi phạm dữ liệu, cung cấp một bộ mật khẩu để thử. Đây là lý do tại sao mật khẩu duy nhất cho các trang web nhạy-cảm-về-bảo-mật lại rất quan trọng, vì việc vi phạm dữ liệu tại một công ty có thể khiến bạn mất tất cả tài khoản của mình, vì công việc của kẻ tấn công trở nên chỉ đơn giản là tra cứu chúng.

### **Brute Force**

Nếu như người dùng đã lựa chọn một mật khẩu không được tìm thấy trong một từ điển, thậm chí ngay cả khi các ký tự số và ký tự đặc biệt đã được thay thế cho các ký tự bình thường, cách duy nhất để mật khẩu có thể bị bẻ khóa đối với một kẻ tấn công là cố gắng thử một cuộc tấn công kiểu *brute force*, trong đó chương trình bẻ-khóa-mật-khẩu cố gắng thử tất cả mọi kết hợp mật khẩu khả dĩ.

Độ dài của mật khẩu và kích cỡ của bộ các ký tự khả dĩ trong mật khẩu sẽ ảnh hưởng rất lớn đến thời lượng của một cuộc tấn công kiểu brute force. Một vài năm trước, phương pháp tấn công này rất tốn thời gian, vì nó mất thời gian đáng kể để tạo ra mọi kết hợp mật khẩu. Với sự gia tăng của tốc độ tính toán, tuy nhiên, việc tạo ra các kết hợp mật khẩu nhanh hơn nhiều, khiến cho việc khởi chạy một cuộc tấn công brute force trở nên khả thi hơn để chống lại những hệ thống và mạng máy tính nhất định.

Một cuộc tấn công kiểu brute force đối với một mật khẩu có thể diễn ra ở hai cấp độ: nó có thể tấn công một hệ thống, nơi mà kẻ tấn công đang cố gắng đoán mật khẩu ở dấu nhắc đăng nhập, hoặc nó có thể tấn công

một danh sách băm mật khẩu được chứa trong một tập tin mật khẩu. Cấp độ tấn công đầu tiên có thể khó khăn hơn nếu như tài khoản sẽ bị khóa sau vài lần đăng nhập thất bại. Cấp độ tấn công thứ hai có thể bị cản trở nếu như tập tin mật khẩu được duy trì một cách bảo mật để những người khác không thể có được một bản sao của nó.

## Ngoại tuyến

Các cuộc tấn công brute force *ngoại tuyến*, có thể được sử dụng để thực hiện so sánh băm với một tập tin mật khẩu đã bị đánh cắp. Việc này có một thách thức là đánh cắp tập tin mật khẩu, nhưng nếu được hoàn thành [*chỉ việc đánh cắp tập tin mật khẩu – người dịch*], sẽ có thể sử dụng các máy tính song song dựa-trên-GPU hiệu-suất-cao để thử các mật khẩu với tốc độ rất cao và chống lại nhiều tài khoản cùng một thời điểm.

## Trực tuyến

Khi một cuộc tấn công kiểu brute force diễn ra trong thực tế chống lại một hệ thống, nó thường được thực hiện để tấn công một tài khoản đơn lẻ với rất nhiều ví dụ về mật khẩu. Sự thành công hay thất bại được xác định bởi hệ thống đang bị tấn công, và kẻ tấn công có thể xâm nhập được hay không. Các cuộc tấn công brute force *trực tuyến* có khuynh hướng rất ồn ào và dễ dàng bị phát hiện bởi việc giám sát bảo mật mạng, và chúng cũng bị giới hạn bởi thời gian hồi đáp của hệ thống và băng thông.

## Bảng Cầu vồng (Rainbow Table)

*Bảng Cầu vồng* là các bảng được tính toán trước hoặc các giá trị băm được liên kết với mật khẩu. Việc sử dụng bảng cầu vồng có thể thay đổi việc tìm kiếm mật khẩu từ bài toán tính toán thành bài toán tra cứu. Điều này có thể làm giảm một cách đáng kể mức độ công việc cần thiết để bẻ khóa một mật khẩu nhất định. Cách bảo vệ tốt nhất chống lại các bảng cầu vồng là các *hàm băm được trộn muối* (*salted hashes*), vì việc bổ sung một giá trị muối làm tăng độ phức tạp của vấn đề bằng cách làm cho

quá trình tính toán trước không thể lặp lại giữa các hệ thống. *Muối* chỉ đơn thuần là một tập hợp các ký tự ngẫu nhiên được thiết kế để làm gia tăng độ dài của mục đang được băm, giúp tạo ra các bảng cầu vồng quá lớn để có thể tính toán một cách hiệu quả.

---



**MÁCH NƯỚC CHO KỲ THI** *Muối* là một bộ các ký tự ngẫu nhiên được thiết kế để làm gia tăng độ dài của mục đang được băm. Nó là một biện pháp phòng thủ hiệu quả chống lại các cuộc tấn công kiểu bảng cầu vồng.

### **Văn bản thô/Không được mã hóa (Plaintext/Unencrypted)**

Các mật khẩu được lưu trữ là đối tượng để truy xuất. Bất kỳ thời điểm nào mà một hệ thống có thể gửi cho bạn một bản sao của mật khẩu của bạn thì đó là một vấn đề bảo mật. Các cuộc tấn công mật khẩu dạng văn bản thô là những cuộc tấn công diễn ra để chống lại những vấn đề cụ thể này. Đểng để bắt cứ ai nghĩ rằng đây chỉ là vấn đề từ các hệ thống hoặc chương trình giả mạo, ngay cả các hệ thống chính thống cũng có thể trở thành con mồi của cái bẫy này. Microsoft cho phép quản trị viên đẩy ra mật khẩu cho các tài khoản cục bộ thông qua các tùy chọn chính sách nhóm. Để bảo vệ mật khẩu, chúng được mã hóa bằng Tiêu chuẩn Mã hóa Nâng cao (AES). Vì lý do tương thích với các hệ thống khác, Microsoft đã công bố khóa AES – và đây là vấn đề.

Trong các hệ thống Microsoft Windows, Mimikatz là một công cụ bảo mật có thể trích xuất các phiếu Kerberos từ bộ nhớ và nó cũng có khả năng trích xuất mật khẩu văn bản thô từ các kết xuất quy trình của quy trình LSASS. Điều này có nghĩa là bằng cách sử dụng các công cụ bảo mật ProcDump và Mimikatz, người ta có thể thu thập mật khẩu dạng văn bản thô từ một hệ thống.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy đảm bảo rằng bạn quen thuộc với các cuộc tấn công khác nhau, bao gồm phun (spraying), từ điển, cưỡng bức (brute force), bảng cầu vồng, và văn bản thô/không mã hóa. Hãy hiểu về sự khác biệt giữa chúng và cách nhận biết từng cuộc tấn công như thế nào.

### Tấn công Vật lý

Hầu hết các kiểu tấn công đã được liệt kê trong chương cho đến thời điểm này là các cuộc tấn công logic, trong đó chúng đang tấn công hệ thống từ khía cạnh logic máy tính. [Chương 1](#), “Các Kỹ thuật Kỹ thuật Xã hội”, đề cập đến những cuộc tấn công kỹ thuật xã hội – các cuộc tấn công được thiết kế để khiến người dùng thực hiện những hành động dẫn đến việc những lỗ hổng bị khai thác. Một lớp khác của các cuộc tấn công, tấn công vật lý, diễn ra khi một thành phần vật lý như một ổ đĩa flash bị để lại cho một ai đó sử dụng. Hành động sử dụng những thiết bị vật lý “bình thường” này khởi đầu cho một cuộc tấn công tiếp theo đó.

### Cáp USB Độc hại (Malicious Universal Serial Bus Cable)

Hầu hết người dùng đều coi cáp USB chỉ như một sợi cáp, nhưng trong thực tế, một sợi cáp USB có thể có những thiết bị điện được nhúng bên trong nó. Những sợi cáp “Độc hại” đã được phát hiện với những thiết bị điện để có thể lây nhiễm phần mềm độc hại vào trong máy móc. Việc này đã được phát hiện trong cả những cáp USB bình thường lẫn cáp lightning dành cho các thiết bị Apple. Cáp demo thậm chí đã được làm ra với các thiết bị Wi-Fi được nhúng, cho phép những cuộc tấn công vào một mạng Wi-Fi từ chính bản thân sợi cáp này.

## Ổ đĩa flash Độc hại

Các thiết bị lưu trữ USB độc hại đã có từ rất lâu. Chúng đã được sử dụng để lừa cho người dùng nhặt chúng, cắm chúng vào máy của họ và truy cập vào một thư mục hấp dẫn như "Dữ liệu Nhân sự" hoặc "Hình ảnh nhạy cảm". Việc nhấp vào các thư mục này là một sai lầm vì chúng sẽ được phân phối đến máy. Đánh rơi USB là một phương thức tấn công nổi tiếng, trong đó kẻ tấn công để lại các thiết bị USB đã bị nhiễm độc để mọi người nhặt và sử dụng chúng. Và một khi họ cắm chúng vào mạng, cuộc tấn công sẽ được tự động hóa. Một nghiên cứu gần đây được thực hiện trong khuôn viên trường đại học cho thấy 98% các thiết bị bị rơi đã được nhặt lại, và hơn 45% sau đó đã được sử dụng và gửi dữ liệu của về cho những kẻ tấn công.

Để thuận tiện cho người dùng, các hệ điều hành đã áp dụng tính năng Tự động Chạy (Auto Run) hoặc Tự động Phát (Auto Play) trên thiết bị USB, cho phép nội dung khởi chạy khi thiết bị được cắm vào. Vì đây là vấn đề bảo mật rõ ràng nên khả năng tự động thực thi tập tin autorun.inf trong USB đã bị vô hiệu hóa trong các phiên bản hệ điều hành sau-Windows XP. Bạn có thể bật lại thiết lập này trong Windows 10, thông qua Cài đặt|Thiết bị|Tự động Chạy (Settings|Devices|AutoPlay), mặc dù điều này không được khuyến khích. Trong doanh nghiệp, thiết lập cài đặt này có thể được kiểm soát thông qua các chính sách nhóm để hạn chế người dùng thay đổi cài đặt này.

## Nhân bản Thẻ

Nếu như một ai đó có được quyền sở hữu thẻ tín dụng của bạn về mặt vật lý, họ hoàn toàn có thể sao chép những thông tin trên các dải từ, sau đó cho phép họ nhân bản thẻ của bạn. Thẻ thông minh khiến cho việc này trở nên khó khăn hơn, khi bản thân con chip trên thẻ không thể được nhân bản. Nhưng trong trường hợp thẻ tín dụng có một con chip bị hỏng,

nhiều hệ thống sử dụng lại thông tin dải từ, khiến cho cuộc tấn công nhân bản vẫn là một trò lừa đảo tiềm năng có hiệu quả.

Một loại thẻ khác có thể được nhân bản là thẻ ID không tiếp xúc. Những thẻ này được sử dụng bởi hệ thống vận chuyển, hệ thống truy cập và thậm chí cả hộ chiếu. Chip NFC (giao tiếp trường gần – near field communications) có thể được đọc, sao chép thông tin và triển khai một bản sao. Thay vì triển khai thiết bị trên thẻ thực tế, các hệ thống hiện tại sử dụng một thiết bị điện tử nhỏ để tái tạo lại chức năng. Khi dữ liệu được lưu trữ trên thẻ, như đã được thực hiện trong nhiều hệ thống vận chuyển, việc nhân bản thẻ có thể giống như thu thập tiền vé chưa sử dụng. Các cuộc tấn công này đã được chứng minh là có hiệu quả ở một số thành phố lớn chống lại một số các hệ thống thẻ khác nhau

### **Skimming**

Các thiết bị skimming là những thiết bị vật lý được tạo ra để đánh chặn thẻ tín dụng. Những thiết bị này được đặt trong đầu đọc thẻ tín dụng để đọc lướt những dữ liệu từ thẻ tín dụng khi chúng đi qua đầu đọc hợp pháp. Các Skimmers có thể thu thập mọi thông tin từ một dải từ trên thẻ cũng như mã PIN đã được nhập vào, cho phép tạo ra một thẻ nhân bản. Mặc dù những thẻ tín dụng dựa-trên-thẻ-thông-minh rất khó, nếu không muốn nói là không thể nhân bản, tại Hoa Kỳ, việc chặn các tính năng của thẻ thông minh sẽ khiến cho hầu hết các hệ thống bị hạ cấp bởi việc chỉ sử dụng dữ liệu dải từ, do đó bỏ qua các tính năng bảo mật liên kết với phần chip thông minh của thẻ.



**LƯU Ý** Những skimmer thẻ tín dụng có thể được tìm thấy ở các trạm nhiên liệu và các cửa hàng tiện dụng. Lớp phủ, được trình bày ở đây, có

thể được phát hiện bằng cách xử lý máy móc theo cách để loại bỏ nó. Ví dụ: việc kéo nhẹ trên giao diện vật lý thường sẽ làm lộ ra skimmer.



### **Trí tuệ Nhân tạo Đối nghịch (Adversarial Artificial Intelligence)**

Trí tuệ nhân tạo (AI) là sử dụng các mô hình phức tạp để mô phỏng lại chức năng của não bộ - về bản chất, là một phương tiện để truyền khả năng phân tích cho những thứ mà chúng ta sử dụng, từ máy hút bụi robot đến ứng dụng điện thoại thông minh, đến các trợ lý kỹ thuật số. Trí tuệ nhân tạo mang lại sức mạnh cho các giải pháp máy tính vì các mô hình Trí tuệ nhân tạo có thể phân tích nhiều kết hợp đầu vào hơn con người, đồng thời làm như vậy nhanh hơn và chính xác hơn. Các hệ thống hỗ trợ Trí tuệ nhân tạo được sử dụng trong các sản phẩm chống phần mềm độc hại để tìm ra các mối đe dọa mới dựa trên phân tích phân tích các hành vi được lập chương trình. Trí tuệ nhân tạo cũng có thể được sử dụng để né tránh hàng phòng thủ không? Câu trả lời là có, và đây được gọi là *Trí tuệ nhân tạo đối nghịch*. Cũng giống như những người bảo vệ có thể viết ra các công cụ hỗ trợ AI, những kẻ tấn công có thể sử dụng Trí tuệ nhân

tạo để kích hoạt các cuộc tấn công của chúng, chẳng hạn như lừa đảo, để tránh việc bị máy móc phát hiện.

### **Dữ liệu Đào tạo Độc hại dành cho Máy Học (Machine Learning)**

Máy học (ML) là một trong những kỹ thuật được sử dụng trong Trí tuệ nhân tạo. Máy Học hoạt động bằng cách sử dụng một bộ dữ liệu đào tạo để hiệu chỉnh mô hình phát hiện để cho phép phát hiện trên dữ liệu mẫu. Một trong những điểm yếu của Máy học là sự phụ thuộc vào bộ dữ liệu [đào tạo] này. Khả năng của mô hình để phát hiện là một chức năng của hiệu quả của bộ dữ liệu đào tạo. Một bộ dữ liệu đào tạo tốt có thể xây dựng một mô hình phát hiện vững chắc. Một bộ dữ liệu huấn luyện thiếu hụt có thể xây dựng nên một mô hình với các lỗ hổng trong đó — các lỗ hổng cho phép các điều kiện trở nên không bị phát hiện. Việc làm nhiễm bẩn dữ liệu đào tạo là một trong những véc-tơ tấn công mà kẻ tấn công có thể sử dụng để chống lại hệ thống Máy Học. Theo thời gian, khi các điều kiện thay đổi, thuật toán Máy Học cần được đào tạo lại hoặc cập nhật lại để làm khiến nó trở nên hiệu quả với các đầu vào khác nhau. Mỗi bản cập nhật này đại diện cho một cơ hội để làm hư hỏng bộ dữ liệu đầu vào. Ngoài ra, nếu bạn huấn luyện thuật toán chống lại lưu lượng mạng thông thường, đánh dấu nó là tốt khi thực tế đã có kẻ thù trong tập dữ liệu huấn luyện đó, bạn sẽ làm cho thuật toán bị mù hiệu quả trước cuộc tấn công bằng cách gắn nhãn nó là tốt.

### **Bảo mật Thuật toán Máy Học**

Việc hiểu được chi tiết của thuật toán máy học khi nó đã được đào tạo là điều tối quan trọng đối với tính bảo mật của thuật toán. Nếu như một kẻ tấn công có khả năng tái sản xuất chính xác cùng một bộ tham số, chúng sẽ có khả năng tạo ra những bộ dữ liệu tấn công để có thể vượt qua thuật toán Máy Học. Việc duy trì tính bảo mật xoay quanh các tham số của một

thuật toán máy học là điều thiết yếu để duy trì tính hiệu quả của nó [thuật toán].

### **Tấn công Chuỗi-Cung ứng**

Tất cả mọi thứ đều có một chuỗi cung ứng. Các chuỗi cung ứng là mạng lưới các nhà cung cấp để cung cấp nguyên vật liệu để sản xuất nên một thứ gì đó. Trong trường hợp một chiếc máy tính, chuỗi cung ứng cung cấp các bộ phận. Trong trường hợp một chương trình, các nhà lập trình viên là một bộ phận, nhưng các thư viện mà họ sử dụng lại là một thành phần khác. Các bộ phận được sử dụng – có thể là vật lý như một ổ cứng hoặc luận lý như một mô-đun thư viện – có thể bị nhiễm bẩn, dù cho là vô tình hay cố ý. Tuy nhiên, kết quả là như nhau: sản phẩm cuối cùng có thể có lỗ hổng. Biết được điều này, những kẻ tấn công đã học cách tấn công vào các chuỗi cung ứng và khiến cho quá trình sản xuất bình thường khởi tạo nên véc-tơ tấn công. Các nhà sản xuất đã xuất xưởng những chiếc máy tính với phần mềm độc hại được cài đặt trước, do sự giúp đỡ của nhà sản xuất ổ cứng, vốn bản thân nó đã bị lây nhiễm bởi một trong số các nhà cung cấp của họ. Trường hợp vi phạm dữ liệu của Target đã được khởi đầu bằng một cuộc tấn công nhắm mục tiêu vào một công ty sưởi ấm, thông gió và điều hòa không khí (HVAC) là nhà cung cấp cho Target, và khi họ đã kết nối tới hệ thống mạng của Target, mục tiêu cuối cùng đã đạt được. Điều này có nghĩa là bề mặt tấn công thực sự không chỉ trong phạm vi công ty hay sản phẩm của bạn mà cuối cùng là một chức năng của mọi người và mọi thứ trong chuỗi cung ứng của bạn.

### **Tấn công Dựa trên-Đám mây so với Trực tiếp tại Cơ sở**

Các cuộc tấn công vào dữ liệu có thể diễn ra đối với các hệ thống trong nội bộ (tại-cơ-sở) hoặc trên đám mây (dựa trên đám mây). Việc sử dụng điện toán đám mây để gia tăng tính bảo mật chỉ hoạt động nếu bạn chọn một nhà cung cấp đám mây với một giải pháp bảo mật như là một phần

của gói [*gói dịch vụ đám mây – người dịch*]. Trong khi các nhà cung cấp có tên tuổi như Oracle, Microsoft, Google và Amazon có những nguồn lực và kiến thức bảo mật, không phải mọi nhà cung cấp đều có cùng mức độ bảo vệ như nhau. Bản thân việc chuyển đổi việc tính toán hoặc lưu trữ lên đám mây không làm thay đổi công thức bảo mật. Điện toán đám mây chỉ đơn thuần là sử dụng nguồn tài nguyên của một ai đó khác, và bạn sẽ có được những gì mà bạn đã thanh toán cho nó, như trong mọi hợp đồng. Bất kể bạn đang thực hiện bảo mật tại chỗ so với các hệ thống nội bộ hoặc so với các hệ thống dựa trên đám mây, các mục tiêu và phương pháp là hoàn toàn như nhau. Bạn phải xác định mức độ bảo mật bạn mong muốn và các phương pháp để đạt được điều này, và sau đó tuân thủ thông qua, hoặc bằng cách thực hiện công việc hoặc đi thuê bằng cách ký kết hợp đồng [với một bên khác]. Việc chỉ gắn một thứ gì đó vào đám mây hoàn toàn không làm gì nhiều để giải quyết các vấn đề về bảo mật.

### Tấn công Mật mã

Các cuộc tấn công chống lại hệ thống mật mã còn được gọi là *các cuộc tấn công mật mã*. Những cuộc tấn công này được thiết kế để tận dụng 2 điểm yếu cụ thể. Đầu tiên, người dùng coi mật mã là “ma thuật”, hay nói cách khác, là thứ không thể hiểu được, khiến họ tin tưởng vào kết quả mà không cần lý do chính đáng. Thứ hai, mặc dù đã được hiểu rõ bởi các nhà khoa học máy tính, những điểm yếu về mặt thuật toán có thể bị khai thác thường hay bị các nhà phát triển bỏ qua.

### Ngày sinh nhật

Cuộc tấn công *ngày sinh nhật* là một kiểu tấn công cưỡng bức brute force đặc biệt có tên gọi của nó từ một điều gì đó được gọi là nghịch lý ngày sinh nhật, vốn cho rằng trong một nhóm có ít nhất 23 người thì cơ hội để có hai cá nhân sẽ có cùng ngày sinh nhật là lớn hơn 50%. Về mặt toán học, chúng ta có thể sử dụng công thức  $1.25k^{1/2}$  (với  $k$  bằng kích thước

của bộ giá trị có thể có), và trong nghịch lý ngày sinh nhật,  $k$  sẽ bằng 365 (tổng số ngày sinh nhật có thể có). Hiện tượng tương tự cũng được áp dụng cho các mật khẩu, với  $k$  (số lượng mật khẩu) lớn hơn 50 một chút, nhưng vẫn là một con số có thể quản lý được bởi máy tính và dung lượng lưu trữ ngày nay.

### Xung đột (Collision)

Một cuộc tấn công *xung đột* là nơi mà hai đầu vào khác nhau mang lại cùng một kết quả đầu ra của một hàm băm. Thông qua việc thao túng dữ liệu, những thay đổi tinh vi được thực hiện mà người dùng không thể nhìn thấy được nhưng tạo ra các phiên bản khác nhau của một tập tin kỹ thuật số. Với việc tạo ra rất nhiều phiên bản khác nhau và sử dụng cuộc tấn công ngày sinh nhật để tìm kiếm sự xung đột giữa bất kỳ hai trong số rất nhiều phiên bản, một kẻ tấn công có một cơ hội để tạo ra một tập tin với nội dung hiển thị đã bị thay đổi nhưng có các hàm băm giống hệt nhau.

### Hạ cấp (Downgrade)

Là một phần của một thiết lập cài đặt Transport Layer Security/Secure Sockets Layer (TLS/SSL), một đặc tả kỹ thuật của bộ mật mã có thể được sử dụng. Điều này được thực hiện để cho phép hình thức cao nhất của mật mã mà cả máy chủ lẫn trình duyệt có thể hỗ trợ. Trong một cuộc tấn công *hạ cấp*, những kẻ tấn công lợi dụng một nguyên tắc được sử dụng một cách phổ biến để hỗ trợ cho tính tương thích ngược, để hạ cấp bảo mật xuống một trạng thái thấp hơn hoặc không tồn tại.



### MÁCH NƯỚC CHO KỲ THI

Mục tiêu của kỳ thi Security+ đối với các cuộc tấn công (1.2) là, "Đưa ra một kịch bản, phân tích các chỉ báo tiềm năng để xác định kiểu của cuộc tấn công". Điều này có nghĩa rằng bạn

cần phải có khả năng phân biệt được các cuộc tấn công dựa trên một tập hợp các triệu chứng và chỉ báo nhất định. Việc học hỏi về cách mà những cuộc tấn công đó được thực hiện, chúng trông như thế nào, và cách thức nhận ra những cuộc tấn công đó là điều yếu đõi với kỳ thi.

## Tóm tắt Chương

Chương này kiểm tra các phương pháp tấn công được sử dụng bởi tin tặc. Có 7 thể loại tấn công chính đã được đề cập: phần mềm độc hại, tấn công mật khẩu, tấn công vật lý, trí tuệ nhân tạo đối nghịch, tấn công chuỗi cung ứng, tấn công [hệ thống] dựa-trên-đám-mây so với tại-cơ-sở, và tấn công mật mã. Mỗi phần này lại liệt kê một số các cuộc tấn công cụ thể.

Phần về phần mềm độc hại kiểm tra về phần mềm tống tiền, trojan, sâu, các chương trình không mong muốn tiềm ẩn (PUP), tấn công vi-rút fileless, điều khiển và kiểm soát, các bot, phần-mềm-độc-hại-mã-hóa, bom logic, phần mềm gián điệp, keylogger, trojan truy-cập-từ-xa (RAT), rootkit, và cổng hậu. Phần tấn công mật khẩu đề cập đến các cuộc tấn công phun-mật-khẩu, từ điển, và tấn công cưỡng bức brute force, các cuộc tấn công ngoại tuyến và trực tuyến, bảng cầu vồng, và các cuộc tấn công vào những mật khẩu thô/không được mã hóa.

Phần nói về các cuộc tấn công vật lý đề cập đến các cuộc tấn công kiểm soát [thiết bị] vật lý, bao gồm các cuộc tấn công cáp USB độc hại, thiết bị USB độc hại, nhân bản thẻ, và skimmer. Phần về sử dụng đối nghịch trí tuệ nhân tạo đề cập đến khái niệm về việc nhiễm độc một hệ thống máy học thông qua việc làm hư hỏng bộ dữ liệu đào tạo. Phần này cũng đề cập đến tầm quan trọng của bảo mật đối với các thuật toán và tham số máy học.

Chương này kết thúc với phần nói về các cuộc tấn công chuỗi-cung-ứng và tấn công [hệ thống] dựa-trên-đám-mây so với tại-cơ-sở. Phần cuối cùng nói về các cuộc tấn công mật mã, bao gồm tấn công ngày sinh nhật, tấn công xung đột, và tấn công hạ cấp. Điều quan trọng cần ghi nhớ là tài liệu này được thiết kế để giúp bạn hiểu được mục tiêu 1.2 của kỳ thi CompTIA Security+: Đưa ra một kịch bản, phân tích các chỉ báo tiềm năng

để xác định kiểu của cuộc tấn công. Bạn cần phải được chuẩn bị để phân biệt các kiểu tấn công khác nhau.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Một quản trị viên bất mãn bị sa thải do lỗi sơ sót tại tổ chức của bạn. 30 ngày sau, máy chủ lưu trữ tập tin nội bộ và máy chủ sao lưu của tổ chức của bạn đều bị hư hỏng cùng một thời điểm. Khi kiểm tra các máy chủ, bạn xác định được rằng các tập tin tối quan trọng của hệ điều hành đã bị xóa bỏ từ cả hai hệ thống. Nếu như quản trị viên bất mãn kia đã từng chịu trách nhiệm cho việc quản trị những máy chủ đó trong quá trình làm việc của mình thì đây có nhiều khả năng nhất là một ví dụ của kiểu phần mềm độc hại nào?  
**A.** Crypto-malware  
**B.** Trojan  
**C.** Sâu  
**D.** Bom logic.
2. Một đồng nghiệp đã thúc giục bạn tải xuống trình bảo vệ màn hình hoạt hình mới mà anh ta đã từng sử dụng trong vài tuần. Trong khi anh ấy đang chỉ cho bạn chương trình, con trỏ trên màn hình của anh ấy tự di chuyển và một cửa sổ dấu nhắc lệnh sẽ mở ra và nhanh chóng đóng lại. Bạn không thể biết điều gì sẽ xảy ra nếu như có bất kỳ thứ gì được hiển thị trong cửa sổ nhắc lệnh đó. Đồng nghiệp của bạn nói, "Nó đã làm diễn ra trong một thời gian, nhưng nó không có vấn đề gì lớn". Dựa trên những gì bạn đã thấy, bạn nghi ngờ trình bảo vệ màn hình động thực sự là loại phần mềm độc hại nào?  
**A.** Sâu

- B. Trojan**
- C. Ransomware**
- D. Phần mềm gián điệp.**
- 3.** Một số máy tính để bàn trong tổ chức của bạn đang hiển thị màn hình màu đỏ với thông báo “Các tập tin của bạn đã bị mã hóa. Hãy trả 1 bitcoin để thu hồi chúng”. Các máy tính để bàn này rất có thể đã bị ảnh hưởng bởi loại phần mềm độc hại nào?
- A. Phần mềm gián điệp**
- B. Phun**
- C. Ransomware**
- D. Phần mềm độc hại tiền điện tử.**
- 4.** Trong khi quét cổng mạng của bạn để phát hiện các hệ thống trái phép, bạn nhận thấy một trong các máy chủ lưu trữ tập tin của bạn có cổng TCP 31337 đang mở. Khi bạn kết nối với cổng bằng công cụ bảo mật netcat, bạn sẽ thấy một lời nhắc với nội dung “Hãy nhập mật khẩu để truy cập:”. Máy chủ của bạn có thể bị nhiễm loại phần mềm độc hại nào?
- A. PUP**
- B. Vi-rút fileless**
- C. Cổng hậu**
- D. Tấn công người trung gian.**
- 5.** Trong khi thực hiện việc quét-cổng-mạng của bạn để phát hiện các hệ thống trái phép, bạn nhận thấy một trong các máy chủ lưu trữ tập tin của mình có cổng TCP 61337 đang mở. Khi bạn sử dụng Wireshark và kiểm tra các gói, bạn sẽ thấy lưu lượng được mã hóa, trong các gói duy nhất, quay đi quay lại sau mỗi năm phút. Kết nối bên ngoài là một máy chủ nằm bên ngoài phạm vi của tổ chức của bạn. Kết nối này là gì?
- A. Kiểm soát và điều khiển**

- B. Cổng hậu**
- C. Vị trí sao lưu bên ngoài**
- D. Đăng nhập từ xa.**
- 6.** Một người dùng trong tổ chức của bạn đang gặp sự cố với máy tính xách tay của họ. Mỗi khi mở trình duyệt web, cô ấy sẽ thấy các quảng cáo pop-up khác nhau vài phút một lần. Dường như không quan trọng là trang web nào đang được truy cập - cửa sổ pop-up vẫn xuất hiện. Kiểu tấn công này là gì?
- A. Một chương trình không mong muốn tiềm ẩn (PUP)**
- B. Ransomware**
- C. Sâu**
- D. Virus.**
- 7.** Người dùng tại tổ chức của bạn đang phàn nàn về việc các hệ thống bị chậm. Khi kiểm tra một số trong số chúng, bạn thấy rằng việc sử dụng CPU là rất cao và một quá trình có tên là "btmine" đang hoạt động trên mỗi hệ thống bị ảnh hưởng. Bạn cũng nhận thấy mỗi hệ thống bị ảnh hưởng đang giao tiếp với một địa chỉ IP nằm bên ngoài quốc gia của bạn trên cổng UDP 43232. Nếu bạn ngắt kết nối mạng trên các hệ thống bị ảnh hưởng, việc sử dụng CPU sẽ giảm đáng kể. Dựa trên những gì bạn đã quan sát được, bạn nghi ngờ các hệ thống này bị nhiễm loại phần mềm độc hại nào?
- A. Bảng cầu vồng**
- B. Crypto-malware**
- C. Từ điển**
- D. Tấn công hỗn hợp.**
- 8.** Một phần mềm độc hại đang lây nhiễm vào máy tính để bàn trong tổ chức của bạn. Mỗi giờ, càng có nhiều hệ thống bị nhiễm hơn. Sự lây nhiễm đang xảy ra ở các bộ phận khác nhau và trong

trường hợp mà người dùng không chia sẻ bất kỳ tập tin, chương trình hoặc thậm chí là email nào. Loại phần mềm độc hại nào có thể gây ra loại lây nhiễm này?

- A. Virus**
  - B. Trojan**
  - C. RAT**
  - D. Sâu.**
- 9.** Những đặc điểm nào sau đây là đặc điểm của trojan truy cập từ xa?
- A. Chúng có thể được triển khai thông qua phần mềm độc hại như sâu**
  - B. Chúng cho phép các cuộc tấn công kết nối với hệ thống từ xa,**
  - C. Chúng cung cấp cho những kẻ tấn công khả năng sửa đổi tập tin và thay đổi các thiết lập cài đặt**
  - D. Tất cả những điều trên.**
- 10.** Để kiểm tra hệ thống của bạn chống lại các mật khẩu yếu, với tư cách là quản trị viên (có quyền thích hợp) bạn kiểm tra tất cả các tài khoản bằng cách sử dụng 100 mật khẩu thường được sử dụng phổ biến. Kiểm nghiệm này là một ví dụ về điều gì?
- A. Từ điển**
  - B. Phun mật khẩu**
  - C. Bảng cầu vồng**
  - D. Trực tuyến**

## Đáp án

1. **D.** Vì cả hai máy chủ đều bị hư hỏng tại chính xác cùng một thời điểm, đây có nhiều khả năng nhất là một bom logic. Một bom logic là một đoạn mã phần mềm nằm im trong một khoảng thời gian cho đến khi một vài sự kiện hoặc ngày tháng triệu hồi tải trọng độc hại của nó – trong trường hợp này là 30 ngày sau khi nhân viên bắt mẫn bị sa thải.
2. **B.** Trình bảo vệ màn hình hoạt hình có nhiều khả năng là một trojan. Phần mềm trông có vẻ như thực hiện một điều gì đó nhưng có chứa chức năng bổ sung và bị ẩn giấu. Đồng nghiệp của bạn đã mang trojan “vào bên trong bức tường” khi anh ta đã tải về và cài đặt phần mềm trên máy tính để bàn của mình.
3. **C.** Đây rõ ràng là một ransomware. Phần mềm độc hại đã mã hóa các tập tin trên các hệ thống bị lây nhiễm và đang yêu cầu đòi thanh toán cho việc khôi phục các tập tin.
4. **C.** Dấu nhắc này có nhiều khả năng thuộc về một cổng hậu – một cách thức thay thế để truy cập vào hệ thống. Dịch vụ TCP đang lắng nghe các kết nối vào và nhắc một mật khẩu khi các kết nối được thiết lập. Việc cung cấp đúng mật khẩu sẽ cấp quyền truy cập bằng dòng lệnh vào hệ thống.
5. **A.** Lưu lượng định kỳ trông có vẻ như nhịp tim trên các cổng cao đi đến một máy chủ không rõ năm bên ngoài phạm vi hệ thống mạng là đáng ngờ, và đây chính là về việc các tín hiệu điều-khiển-và-kiểm-soát trông như thế nào.
6. **A.** Hành vi này thường được trông thấy trong một chương trình không mong muốn tiềm ẩn – một kiểu ứng dụng được kết hợp với các ứng dụng khác và đang thực hiện các tác vụ không được mong muốn.

7. **B.** Những hệ thống này có nhiều khả năng bị nhiễm crypto-malware và giờ đây trở thành một phần của một botnet đang khai thác tiền mã hóa. Các hệ thống đang chạy một tiến trình không rõ/không được phép, giao tiếp với một địa chỉ IP bên ngoài và sử dụng nguồn tài nguyên đáng kể. Tất cả đều là những dấu hiệu cổ điển của crypto-malware.
8. **D.** Đây có nhiều khả năng là một tấn công kiểu sâu. Các cuộc tấn công di chuyển qua toàn bộ hệ thống mạng, có vẻ như không cần sự can thiệp của người dùng, thường là sâu.
9. **D.** Tất cả những điều này đều là đặc điểm của trojan truy-cập-từ-xa (RAT). RAT thường được triển khai thông qua phần mềm độc hại khác, cho phép truy cập từ xa vào hệ thống bị lây nhiễm, và mang lại cho những kẻ tấn công khả năng thao túng và sửa đổi hệ thống đã bị nhiễm.
10. **B.** Sử dụng những mật khẩu đặt trước cho mọi tài khoản là một ví dụ về phun mật khẩu.

## Chương 3     Các Chỉ báo Tấn công Ứng dụng

### **Chỉ báo Tấn công Ứng dụng**

Trong chương này, bạn sẽ

- Khám phá các hình mẫu tấn công khác nhau,
- Kết nối các chỉ báo tấn công với một hình thức tấn công cụ thể.

Chương này kiểm tra các kiểu tấn công và những thuộc tính của chúng, với mục tiêu minh chứng về cách thức mà người ta có thể kết nối các điểm giữa một loạt các chỉ báo tấn công tiềm năng và một kiểu tấn công ứng dụng cụ thể.

#### **Mục tiêu Chứng nhận**

Chương này đề cập đến mục tiêu kỳ thi CompTIA Security+ 1.3: Đưa ra một kịch bản, phân tích các chỉ báo tiềm năng tương ứng với các cuộc tấn công ứng dụng.

## Leo thang Đặc quyền

Một cuộc tấn công mạng là một quy trình nhiều bước. Hầu hết các cuộc tấn công đều bắt đầu với một mức độ đặc quyền tương ứng với một người dùng bình thường. Từ cấp độ này, kẻ tấn công khai thác những lỗ hổng cho phép chúng có được quyền truy cập cấp độ root hoặc quản trị viên. Bước này trong chuỗi tấn công còn được gọi là *leo thang đặc quyền* và là điều thiết yếu đối với rất nhiều nỗ lực tấn công.

Có một số cách để đạt được sự leo thang đặc quyền. Một cách là sử dụng những đặc quyền hiện hữu để thực hiện một hành động để đánh cắp một bộ các thông tin đăng nhập tốt hơn. Bạn có thể có được những thông tin đăng nhập “tốt hơn” bằng cách sử dụng sniffers để chiếm đoạt những thông tin đăng nhập hoặc bằng cách có được tập tin Security Account Manager (SAM) của Windows hoặc etc/passwd của Linux/Unix. Một phương pháp khác là khai thác những lỗ hổng hoặc điểm yếu trong các tiến trình đang chạy với những đặc quyền đã được leo thang. Việc chèn một đoạn mã độc vào trong những tiến trình này cũng có thể đoạt được đặc quyền được leo thang.



## MÁCH NƯỚC CHO KỲ THI

Việc ngăn chặn leo thang đặc quyền là một bước phòng thủ quan trọng trong một hệ thống. Đây chính là nhân tố cơ bản đứng sau việc gần đây, Microsoft cắt giảm các tiến trình và dịch vụ chạy ở chế độ nâng cao (elevated). Điều này đã làm giảm đáng kể bề mặt tấn công sẵn có để một kẻ tấn công thực hiện tác vụ thiết yếu này.

## Chèn lệnh script độc hại (Cross-Site Scripting)

*Cross-site scripting (XSS)* là một trong những phương pháp tấn công trang web phổ biến nhất. Nguyên nhân của lỗ hổng này là xác thực đầu vào của

người dùng kém. Nếu đầu vào không được xác thực một cách đúng đắn, một kẻ tấn công có thể bao gồm một tập lệnh kịch bản trong đầu vào của họ và hiển thị nó như một phần của tiến trình web. Có một số kiểu tấn công XSS khác nhau, được phân biệt bởi tác động của tập lệnh kịch bản:

- **Tấn công XSS không dài dằng** - Tập lệnh kịch bản được chèn vào không liên tục hoặc không được lưu trữ lại mà thay vào đó, ngay lập tức được thực thi và chuyển trả lại thông qua máy chủ web.
- **Tấn công XSS dài dằng** – Tập lệnh kịch bản được lưu trữ lại trên máy chủ web hoặc một vài vị trí lưu trữ back-end. Điều này cho phép tập lệnh kịch bản được sử dụng để chống lại những người khác, những người sau đó đăng nhập vào hệ thống.
- **Tấn công XSS dựa-trên-DOM** – Tập lệnh kịch bản được thực thi trong trình duyệt thông qua tiến trình Mô hình Đối tượng Tài liệu (Document Object Model – DOM) để chống lại máy chủ web.

Các cuộc tấn công Cross-site scripting có thể dẫn đến một loạt các hậu quả, và trong một số trường hợp, danh sách có thể là bất kỳ điều gì mà một kẻ lập trình tập lệnh kịch bản thông minh có thể nghĩ ra. Dưới đây là một số cách sử dụng phổ biến đã được phát hiện trong tự nhiên:

- Đánh cắp thông tin xác thực từ một ứng dụng web,
- Chiếm đoạt phiên,
- Triển khai nội dung bất lợi,
- Thay đổi những thiết lập cài đặt người dùng, bao gồm cả những người dùng tương lai,
- Mạo danh một người dùng,
- Phishing hoặc đánh cắp những thông tin nhạy cảm.

Các biện pháp kiểm soát để phòng chống lại những cuộc tấn công XSS bao gồm việc sử dụng các thư viện chống-XSS để bóc tách các tập lệnh

kịch bản ra khỏi chuỗi trình tự đầu vào. Một số cách khác để giảm thiểu các cuộc tấn công XSS bao gồm việc giới hạn các kiểu tải lên (upload), sàng lọc kích cỡ của những gì được tải lên, và liệt kê danh sách trắng những đầu vào. Tuy nhiên, việc cố gắng loại bỏ các tập lệnh kịch bản khỏi các đầu vào có thể là một nhiệm vụ nan giải. Chức năng thư viện đầu vào chống-XSS được thiết kế tốt đã được chứng minh là biện pháp phòng thủ tốt nhất. Những lỗ hổng cross-site scripting được kiểm nghiệm một cách dễ dàng và nên là một phần của kế hoạch kiểm tra cho từng ứng dụng. Việc kiểm tra nhiều loại đầu vào đã được và không được mã hóa để tìm lỗ hổng scripting là một yếu tố kiểm tra thiết yếu.

---



## MÁCH NƯỚC CHO KỲ THI

Xác minh đầu vào là rất hữu ích để ngăn

ngừa các cuộc tấn công XSS.

---



**LƯU Ý** Xác thực đầu vào, hay còn được gọi là *xác thực dữ liệu* là việc kiểm nghiệm có cấu trúc và hợp lý bất kỳ đầu vào nào được cung cấp bởi một ứng dụng hoặc người dùng. Xác thực đầu vào ngăn chặn dữ liệu được định dạng không phù hợp (định dạng kỳ dị) khỏi việc nhập vào một hệ thống.

## Tấn công Chèn lệnh (Injection Attack)

Đầu vào của người dùng không được xác thực đầu vào sẽ mở ra một cơ hội cho một kẻ tấn công tạo ra đầu vào để gây ra những sự kiện cụ thể diễn ra khi đầu vào được phân tích và sử dụng bởi một ứng dụng. Tấn công chèn lệnh vào Ngôn ngữ Truy vấn Có cấu trúc (SQL) liên quan đến việc thao túng đầu vào, dẫn đến việc một câu lệnh SQL khác với câu lệnh như dự định của người thiết kế. Các cuộc tấn công chèn lệnh vào Ngôn

ngữ Đánh dấu Có thể mở rộng (XML) và Giao thức Truy cập Danh bạ Hạng nhẹ (LDAP) được thực hiện theo cùng một cách thức. Vì SQL, XML và LDAP được sử dụng để lưu trữ dữ liệu nên điều này có thể cấp cho kẻ tấn công quyền truy cập vào dữ liệu chống lại các quy tắc nghiệp vụ. Các cuộc tấn công chèn dòng lệnh có thể diễn ra khi đầu vào được sử dụng theo một cách thức cho phép thao túng giao diện dòng-lệnh. Điều này có thể mang lại cho kẻ tấn công quyền truy cập dòng-lệnh tại cấp độ có đặc quyền của một ứng dụng.

### **Ngôn ngữ Truy vấn có Cấu trúc (SQL)**

Một cuộc tấn công chèn lệnh SQL là một hình thức chèn một đoạn mã nhắm đến bất kỳ cơ sở dữ liệu dựa-trên-SQL nào, bất kể nhà cung cấp. Một ví dụ của kiểu tấn công này là nơi mà chức năng bắt lấy các đầu vào tên người dùng và mật khẩu do người-dùng-cung-cấp và thay thế chúng trong một điều kiện **where** trong một câu lệnh SQL với mục đích rõ ràng là thay đổi mệnh đề **where** thành một mệnh đề đưa ra một câu trả lời sai cho một truy vấn.

Ví dụ, giả sử câu lệnh SQL được mong muốn là:

```
select count(*) from users_table where username = 'JDoe'  
and password = 'newpass'
```

Giá trị JDoe và newpass được cung cấp bởi người dùng và chỉ đơn giản là chèn vào chuỗi ký tự. Mặc dù trông có vẻ an toàn về mặt chức năng, điều này có thể bị phá hoại một cách dễ dàng bằng cách sử dụng trình tự

```
' or 1=1      -
```

vốn thay đổi mệnh đề **where** thành một mệnh đề sẽ trả lại toàn bộ các bản ghi, như được thể hiện ở đây:

```
select count(*) from users_table where username = 'JDoe'  
and password = '' or 1=1 -'
```

Ngoài điều kiện **or**, cùng với một mệnh đề luôn luôn đúng và việc bắt đầu một dòng lệnh để khóa chặn dấu ngoặc kép ở cuối [dòng lệnh], thay thế câu lệnh SQL bằng một câu lệnh mà theo đó mệnh đề **where** không thể hoạt động được. Nếu mệnh đề **where** bị thay thế để trả về mọi bản ghi, việc này có thể dẫn đến một sự vi phạm dữ liệu.

*Các thủ tục lưu trữ* là những phương pháp được biên dịch trước đã được triển khai trong phạm vi một công cụ cơ sở dữ liệu. Các thủ tục lưu trữ đóng vai trò như một cơ chế bảo mật mã phần mềm vì chúng cô lập đầu vào của người dùng từ các câu lệnh SQL thực tế đang được thực thi. Đây là cơ chế phòng thủ chủ yếu để chống lại các cuộc tấn công chèn lệnh SQL – hay nói cách khác, phân tách đầu vào của người dùng khỏi các câu lệnh SQL. Dữ liệu đầu vào được-cung-cấp-bởi-người-dùng là rất quan trọng trong các ứng dụng tương tác sử dụng các cơ sở dữ liệu, những kiểu ứng dụng này cho phép người dùng xác định tính cụ thể của tìm kiếm, khớp nối, v.v... Nhưng điều không thể xảy ra là cho phép một người dùng viết đoạn mã SQL thực tế được thực thi – có quá nhiều thứ có thể sai và nó cung cấp cho người dùng quá nhiều quyền năng để được phép sử dụng trực tiếp. Do đó, việc loại bỏ các cuộc tấn công chèn lệnh SQL bằng cách “sửa chữa” đầu vào chưa bao giờ có hiệu quả.

Mọi công cụ cơ sở dữ liệu chính đều hỗ trợ các thủ tục lưu trữ. Các thủ tục lưu trữ có một lợi thế về hiệu suất so với những hình thức truy cập dữ liệu khác. Nhược điểm là các thủ tục lưu trữ được viết bằng một ngôn ngữ khác với SQL và thường phải cần một lập trình viên cơ sở dữ liệu để triển khai các thủ tục phức tạp hơn.

## Kiểm nghiệm Lỗ hổng Chèn lệnh SQL

Có hai bước chính được liên kết với kiểm nghiệm lỗ hổng chèn lệnh SQL. Bước đầu tiên là xác nhận rằng hệ thống hoàn toàn dễ bị tổn thương. Việc này có thể được thực hiện bằng cách sử dụng các dấu vào khác nhau để kiểm tra xem liệu một biến đầu vào có thể được sử dụng để thao túng câu lệnh SQL hay không. Dưới đây là các véc-tơ kiểm tra phổ biến được sử dụng:

```
' or 1=1 -  
" or 1=1 -  
or 1=1 -  
' or 'a'='a  
" or "a"="a  
) or ('a'='a
```

Hãy lưu ý rằng việc sử dụng dấu ngoặc đơn hoặc ngoặc kép phụ thuộc vào việc triển khai SQL vì có sự khác biệt về mặt cú pháp giữa các công cụ cơ sở dữ liệu chính.

Bước thứ hai là sử dụng thông tin thông điệp lỗi để cố gắng thực hiện một khai thác thực tế đối với cơ sở dữ liệu.



## MÁCH NƯỚC CHO KỲ THI

Các thủ tục lưu trữ là tiêu chuẩn vàng để ngăn chặn các cuộc tấn công chèn lệnh SQL và được đặc biệt đề cập đến trong các mục tiêu Security+.

## Thư viện Liên-kết-Động (DLL)

Một *thư viện liên-kết-động (DLL)* là một đoạn mã có thể bổ sung thêm tính năng cho một chương trình thông qua việc bao gồm các thủ tục thư viện được liên kết tại thời điểm chương trình hoạt động. *Chèn lệnh DLL*

là một tiến trình bổ sung vào chương trình - tại thời điểm hoạt động – một DLL có một lỗ hổng chức năng cụ thể có thể bị lợi dụng bởi kẻ tấn công. Một ví dụ điển hình là Microsoft Office, một bộ các chương trình sử dụng các DLL được tải lên tại thời điểm chương trình hoạt động. Việc bổ sung DLL “ác quỷ” vào đúng thư mục, hoặc qua một khóa registry, có thể dẫn đến phát sinh thêm chức năng bổ sung.

### **Giao thức Truy cập Danh bạ Hạng nhẹ (LDAP)**

Các hệ thống dựa-trên-LDAP cũng là đối tượng của các cuộc tấn công chèn lệnh. Khi một ứng dụng đưa ra một yêu cầu LDAP dựa trên đầu vào của người dùng, một lỗi xác thực đầu vào có thể dẫn đến một yêu cầu LDAP sai. Giống như chèn lệnh SQL có thể được sử dụng để thực thi những câu lệnh tùy ý trong một cơ sở dữ liệu, chèn lệnh LDAP có thể thực hiện điều tương tự trong một hệ thống danh bạ. Một điều gì đó chỉ đơn giản như việc một ký tự đại diện (\*) trong một hộp tìm kiếm có thể trả về những kết quả sẽ thường vượt quá phạm vi tìm kiếm. Xác thực đầu vào thích hợp là điều quan trọng trước khi một yêu cầu được chuyển cho một công cụ LDAP.

### **Ngôn ngữ Đánh dấu có Khả năng mở rộng (XML)**

XML cũng có thể bị can thiệp thông qua tấn công chèn lệnh. Các cuộc tấn công chèn lệnh XML có thể được sử dụng để thao túng một hệ thống dựa-trên-XML. Vì XML gần như phổ biến trong thế giới ứng dụng web nên hình thức tấn công này có rất nhiều mục tiêu. XML bị thay đổi một cách độc hại có thể ảnh hưởng đến những thay đổi trong cấu hình, những thay đổi trong luồng dữ liệu, những thay đổi về kết quả đầu ra — tất cả đều do việc chèn lệnh [XML].



**MÁCH NƯỚC CHO KỲ THI** Đối với kỳ thi, bạn nên tìm hiểu về các cuộc tấn công kiểu-chèn-lệnh và cách thức mà chúng thao túng các hệ thống mà chúng đang chèn vào, bao gồm SQL, DLL, LDAP và XML.

### **Giải tham chiếu Con trỏ/Đối tượng (Pointer/Object Dereference)**

Một số ngôn ngữ máy tính sử dụng một cấu trúc được gọi là *con trỏ* (*pointer*), một cấu trúc để cập đến vị trí bộ nhớ đang chứa biến số, trái ngược với một biến số, nơi giá trị được lưu trữ trực tiếp trong vị trí của bộ nhớ. Để nhận giá trị tại vị trí bộ nhớ được biểu thị bằng một biến con trỏ, người ta phải tham chiếu đến con trỏ. Hành động giải tham chiếu đến một con trỏ bây giờ thay đổi ý nghĩa của đối tượng thành nội dung của vị trí bộ nhớ chứ không phải vị trí bộ nhớ như đã được xác định bởi con trỏ. Con trỏ có thể rất mạnh và cho phép hoạt động nhanh chóng trên nhiều loại cấu trúc. Tuy nhiên, chúng cũng có thể rất nguy hiểm, vì sai lầm khi sử dụng có thể dẫn đến những hậu quả không mong muốn. Ví dụ: khi một lập trình viên sử dụng đầu vào của người dùng kết hợp với con trỏ, điều này cho phép người dùng chọn một vị trí trong một mảng và sử dụng một con trỏ để tham chiếu giá trị. Sai lầm trong xác thực đầu vào có thể dẫn đến lỗi trong tham chiếu con trỏ, điều này có thể gây ra hoặc không thể gây ra lỗi, vì vị trí sẽ chứa dữ liệu và nó sẽ được trả về. Vì con trỏ được kết nối với một đối tượng, CompTIA Security+ đề cập đến chủ đề này như là *giải tham chiếu con trỏ/đối tượng*, vì việc giải tham chiếu con trỏ dẫn đến giải tham chiếu đến đối tượng.

### **Xâm nhập Danh bạ (Directory Traversal)**

Một cuộc tấn công *xâm nhập danh bạ* là khi một kẻ tấn công sử dụng những đầu vào đặc biệt để phá vỡ cấu trúc cây thư mục của một hệ thống lưu trữ tập tin. Việc bổ sung thêm các ký hiệu đã được mã hóa cho ".." trong hộp đầu vào chưa được xác thực có thể dẫn đến việc bộ phân

tích cú pháp phân giải mã hóa thành mã truyền tải, bỏ qua rất nhiều phần tử nhận diện và chuyển đầu vào cho hệ thống tập tin. Sau đó, chương trình thực hiện các lệnh ở một vị trí khác với vị trí đã được thiết kế. Khi được kết hợp với một tấn công chèn lệnh, đầu vào có thể dẫn đến việc thực thi mã theo cách trái phép. Được phân loại là lỗi xác thực đầu vào, chúng có thể khó được phát hiện nếu không thực hiện diễn tập mã và tìm kiếm chúng một cách cụ thể. Điều này minh họa cho tính hữu ích của danh sách kiểm tra 25 Lỗi Phần mềm Nguy hiểm Nhất của CWE trong quá trình đánh giá mã phần mềm vì nó cảnh báo cho các nhà phát triển về vấn đề này trong quá trình phát triển.

Việc xâm nhập thư mục có thể được che giấu bằng cách sử dụng mã hóa các luồng đầu vào. Nếu như việc kiểm tra bảo mật được thực hiện trước khi chuỗi được giải mã bởi trình phân tích cú pháp hệ thống thì việc nhận dạng hình thức tấn công có thể bị hư hại. Có rất nhiều cách để trình bày một dạng đầu vào cụ thể, trong đó đơn giản nhất là dạng kinh điển (ví dụ: xem Chương 11: "A Rose Is a Rose Is a r%6fse"). Các trình phân tích cú pháp được sử dụng để diễn tả biểu mẫu chuẩn đổi với hệ điều hành (OS), nhưng các trình phân tích cú pháp nhúng này có thể hoạt động sau khi xác thực đầu vào, khiến cho việc phát hiện một số cuộc tấn công chỉ từ việc khớp một chuỗi trở nên khó khăn hơn.

### **Tràn Bộ nhớ đệm (Buffer Overflow)**

Nếu có một mục nào có thể được gắn nhãn là "được mong muốn nhất" trong bảo mật mã phần mềm, thì đó sẽ là lỗi tràn bộ đệm. CERT/CC tại Đại học Carnegie Mellon ước tính rằng gần một nửa số lần khai thác các chương trình máy tính trong lịch sử bắt nguồn từ một số dạng tràn bộ đệm. Việc tìm ra một loại vắc-xin để ngăn chặn sự cố tràn bộ đệm sẽ loại bỏ đi một nửa số sự cố liên quan đến bảo mật này theo loại, và có lẽ là 90% tính theo khối lượng. Sâu ngón tay Morris vào năm 1988 là một sự

khai thác việc tràn bộ đệm, cũng như các sự kiện tên tuổi gần đây như Code Red và Slammer. Sự phân loại chung về lỗi tràn bộ đệm bao gồm nhiều biến thể, chẳng hạn như ghi đè bộ đệm tĩnh, lỗi chỉ mục, lỗi chuỗi định dạng, kích thước bộ đệm Unicode và ANSI không khớp, và vượt quá heap.

Khái niệm đầu sau những lỗi hổng này tương đối đơn giản. Bộ đệm đầu vào được sử dụng để giữ cho đầu vào chương trình bị ghi đè bằng dữ liệu lớn hơn kích thước mà bộ đệm có thể chứa. Nguyên nhân sâu xa của lỗi hổng này là sự kết hợp của hai yếu tố: thực tiễn lập trình kém và điểm yếu của ngôn ngữ lập trình. Ví dụ, điều gì sẽ xảy ra nếu một chương trình yêu cầu số điện thoại từ 7 đến 10 ký tự nhưng thay vào đó nhận được một chuỗi dài 150 ký tự? Rất nhiều chương trình sẽ cung cấp một số kiểm tra lỗi để đảm bảo rằng điều này sẽ không gây ra sự cố. Tuy nhiên, một số chương trình không thể xử lý lỗi này và các ký tự thừa tiếp tục lấp đầy bộ nhớ, ghi đè lên các phần khác của chương trình. Điều này có thể dẫn đến một số vấn đề, bao gồm cả việc khiến cho chương trình bị hủy bỏ hoặc hệ thống gặp sự cố. Dưới những hoàn cảnh nhất định, chương trình có thể thực hiện một lệnh do kẻ tấn công cung cấp. Tràn bộ đệm thường kẽm thừa mức đặc quyền mà chương trình đang bị khai thác. Đây là lý do tại sao các chương trình sử dụng quyền truy cập mức root lại rất nguy hiểm khi bị khai thác với lỗi tràn bộ đệm, vì mã sẽ thực thi ở quyền truy cập mức root.

Các ngôn ngữ lập trình như C được thiết kế cho những ràng buộc về không gian và hiệu suất. Rất nhiều hàm trong C, ví dụ như hàm **get()**, không an toàn ở chỗ chúng sẽ chấp thuận các hoạt động không an toàn, chẳng hạn như thao túng chuỗi không bị ràng buộc vào các vị trí bộ đệm cố định. Ngôn ngữ C cũng cho phép truy cập bộ nhớ trực tiếp thông qua con trỏ, một chức năng cung cấp nhiều sức mạnh lập trình nhưng lại

mang theo những gánh nặng về các biện pháp bảo vệ thích hợp được cung cấp bởi lập trình viên.



**MÁCH NƯỚC CHO KỲ THI** Tràn bộ đệm có thể xảy ra trong bất kỳ mã nào, và mã có thể chạy với đặc quyền có một mức rủi ro thậm chí còn lớn hơn nhiều. Vào năm 2014, một lỗi tràn bộ đệm trong thư viện OpenSL, được gọi là Heartbleed, đã khiến cho hàng trăm nghìn hệ thống bị tổn thương và phát lộ dữ liệu tối quan trọng của hàng triệu khách hàng trên toàn cầu.

Tràn bộ đệm chính là các cuộc tấn công xác thực đầu vào, được thiết kế để tận dụng các thủ tục đầu vào đã không được xác thực độ dài của đầu vào. Cách giải quyết đơn giản một cách đáng ngạc nhiên, tất cả những gì cần thiết là xác thực độ dài của mọi đầu vào trường khi ghi chúng vào bộ nhớ. Việc này có thể được thực hiện theo nhiều cách khác nhau, bao gồm sử dụng các chức năng thư viện an toàn cho các đầu vào. Đây là một trong những lỗ hổng đã được chứng minh là có thể giải quyết được, và trong thực tế, mức độ phổ biến đang giảm một cách đáng kể giữa các công ty phần mềm quan-tâm-đến-bảo-mật.

### **Điều kiện Cạnh tranh (Race Condition)**

Một *điều kiện cạnh tranh* là một điều kiện lỗi xảy ra khi kết quả đầu ra của một chức năng phụ thuộc vào trình tự hoặc thời điểm của đầu vào. Nó trở thành một lỗi khi đầu vào không diễn ra theo trình tự mà lập trình viên đã định. Thuật ngữ *điều kiện cạnh tranh* liên quan đến ý tưởng về việc nhiều đầu vào ganh đua với nhau để gây ảnh hưởng đến kết quả đầu ra trước nhất. Các điều kiện cạnh tranh có thể xảy ra trong các chương trình phân tán hoặc đa luồng khi mà trình tự hoặc thời điểm của các tiến trình hoặc các luồng là điều tối quan trọng đối với sự hoạt động một cách

đúng đắn của chương trình. Một điều kiện cạnh tranh cổ điển là khi một luồng phụ thuộc vào một giá trị (A) từ một hàm khác đã bị thay đổi một cách chủ động bởi một tiến trình tách biệt. Tiến trình đầu tiên không thể hoàn tất công việc của nó cho đến khi tiến trình thứ hai thay đổi giá trị của A. Nếu như hàm thứ hai vẫn đang đợi hàm thứ nhất kết thúc, một khóa sẽ được tạo ra bởi cả hai tiến trình và các phụ thuộc của chúng. Những điều kiện này có thể rất khó để dự đoán và tìm kiếm. Nhiều luồng đã không được đồng bộ, thỉnh thoảng trên nhiều hệ thống, tạo ra các vòng lặp logic phức tạp để dành cho các hàm nguyên tử trông có vẻ như đơn giản. Việc hiểu được và quản lý các khóa hồ sơ là một thành phần thiết yếu trong một môi trường lập trình hướng đối tượng hiện đại và đa dạng.

Các điều kiện cạnh tranh được xác định theo các cửa sổ cạnh tranh, một khoảng thời gian cơ hội khi các luồng đồng thời có thể cạnh tranh để cõ gắng thay đổi cùng một đối tượng. Bước đầu tiên để tránh các điều kiện cạnh tranh là xác định các cửa sổ cạnh tranh. Sau đó, khi các cửa sổ đã được xác định, hệ thống có thể được thiết kế để từ đó, chúng không bị gọi lên đồng thời, một tiến trình được gọi là *loại trừ lẫn nhau*. Tác động của điều kiện cạnh tranh thường là sự cố của một hệ thống dưới dạng một tai nạn. Điều kiện cạnh tranh có thể được kết hợp với bộ đếm tham chiếu, khóa nhân và đồng bộ hóa luồng. Bộ đếm tham chiếu là những cấu trúc trong nhân để chi tiết hóa việc tài nguyên có đang được sử dụng một cách tích cực ở thời điểm hiện tại hay không. Việc khóa nhân là một phương pháp ban đầu, nhưng nó gây ra các vấn đề về hiệu suất. Đồng bộ hóa luồng ngăn chặn luồng truy cập vào dữ liệu được chia sẻ tại cùng một thời điểm.

Một vấn đề thời gian khác là vòng lặp vô hạn. Khi logic chương trình trở nên phức tạp - ví dụ: xử lý ngày tháng năm nhuận - cần phải cẩn trọng

để đảm bảo rằng tất cả các điều kiện được bảo vệ và các lỗi cũng như các cơ chế phá vòng lặp khác không cho phép chương trình đi vào trạng thái mà các kiểm soát vòng lặp sẽ bị lỗi. Việc không quản lý được thuộc tính chính xác này dẫn đến việc các thiết bị Microsoft Zune bị lỗi khi chúng được bật vào năm mới sau năm nhuận. Logic kiểm soát đã đi vào một trình tự trong đó một vòng lặp sẽ không được thỏa mãn, dẫn đến việc thiết bị gặp sự cố khi đi vào một vòng lặp vô hạn và trở nên không có phản hồi.

---



**MÁCH NƯỚC CHO KỲ THI** Các điều kiện cạnh tranh có thể được sử dụng cho các cuộc tấn công đặc quyền nâng cao và từ-chối-dịch-vụ. Các lập trình viên có thể sử dụng tham chiếu bộ đếm, khóa nhân và đồng bộ luồng để ngăn ngừa điều kiện cạnh tranh.

### **Thời gian Kiểm tra/Thời gian Sử dụng**

Trong mô hình hoạt động đồng thời và được phân luồng ngày nay, một điều khả thi là các hệ thống khác nhau cỗ gắng tương tác với cùng một đối tượng tại cùng một thời điểm. Một điều khác cũng khả thi để các sự kiện xảy ra ngoài phạm vi trình tự dựa trên sự khác biệt về thời điểm giữa các luồng khác nhau của một chương trình. Các vấn đề về trình tự và thời điểm chẵng hạn như điều kiện cạnh tranh và vòng lặp vô hạn ảnh hưởng đến cả thiết kế lẫn việc triển khai các hoạt động dữ liệu. Việc hiểu được cách thức và địa điểm mà những điều kiện đó có thể xảy ra là điều quan trọng đối với các thành viên của nhóm phát triển. Về mặt thuật ngữ kỹ thuật, những gì phát triển nên điều gì được gọi là điều kiện cạnh tranh, hoặc hình thành nên một quan điểm tấn công, hệ thống dễ bị tổn thương đối với một cuộc tấn công thời điểm kiểm tra/thời điểm sử dụng (TOC/TOU).

---



**MÁCH NƯỚC CHO KỲ THI** Một cuộc tấn công thời điểm kiểm tra/thời điểm sử dụng là một cuộc tấn công để tận dụng sự phân tách giữa thời gian mà một chương trình kiểm tra một giá trị và khi nó sử dụng giá trị đó, cho phép một sự thao túng trái phép có thể ảnh hưởng đến kết quả đầu ra của một tiến trình.

### Xử lý Lỗi Không thích hợp (Improper Error Handling)

Mọi ứng dụng sẽ gặp các lỗi và ngoại lệ, và chúng cần phải được xử lý theo một cách an toàn. Một phương pháp tấn công bao gồm việc bắt buộc các lỗi để chuyển một ứng dụng từ hoạt động bình thường thành xử lý ngoại lệ. Trong một trường hợp ngoại lệ, một thực tiễn phổ biến là ghi nhận/báo cáo về các điều kiện, thường là trong một tập tin nhật ký, bao gồm việc hỗ trợ cho những thông tin chẵng hạn như dữ liệu đã gây ra lỗi. Thông tin này có thể trở nên vô giá trong quá trình chẩn đoán nguyên nhân của điều kiện lỗi. Thách thức là thông tin này được nắm bắt tại đâu. Phương pháp tốt nhất là nắm bắt nó trong một tập tin nhật ký, nơi nó có thể được bảo vệ bằng một danh sách kiểm soát truy cập (ACL). Phương pháp tồi nhất là lặp lại thông tin cho phía người dùng. Việc lặp lại các điều kiện lỗi cho người dùng có thể cung cấp những thông tin vô giá cho những kẻ tấn công khi chúng gây ra lỗi có mục đích.

*Xử lý Lỗi Không thích hợp* có thể dẫn đến một loạt các tiết lộ. Các lỗi tương ứng với các câu lệnh SQL có thể làm lộ các cấu trúc và thành phần dữ liệu. Các lỗi cuộc gọi thủ tục từ xa (remote procedure call – RPC) có thể đưa ra những thông tin nhạy cảm như tên tập tin, đường dẫn, và tên máy chủ. Các lỗi lập trình có thể tiết lộ số thứ tự của dòng lệnh, nơi xảy ra ngoại lệ, phương pháp đã được viện dẫn, và những thông tin chẵng hạn như các thành phần ngăn xếp. Những kẻ tấn công có thể sử dụng

những thông tin mà chúng thu thập được từ các lối để tiếp tục tấn công thêm vào một hệ thống, vì thông tin thường cung cấp chi tiết cho chúng về thành phần và hoạt động bên trong của hệ thống mà chúng có thể khai thác.

### **Xử lý đầu vào không thích hợp (Improper Input Handling)**

*Xử lý đầu vào không thích hợp* là nguyên nhân số một của những lỗ hổng phần mềm. Việc xử lý đầu vào hoặc xác thực đầu vào không thích hợp là nguyên nhân gốc rễ đằng sau hầu hết các cuộc tấn công tràn bộ đệm, tấn công chèn lệnh và các lỗi cấu trúc kinh điển. Những người dùng có khả năng thao túng đầu vào, nhà phát triển phải xử lý đầu vào một cách thích hợp để ngăn chặn việc các mục nhập độc hại có hiệu lực. Tràn bộ đệm (đã được thảo luận trước đây trong chương) đã được thừa nhận rất lâu như là một lớp xử lý đầu vào không thích hợp. Các cuộc tấn công xử lý đầu vào mới hơn bao gồm các cuộc tấn công chuẩn hóa và tấn công số học. Cơ chế phòng vệ tốt nhất khả dĩ mà bạn có thể sử dụng là xác thực đầu vào. Việc cân nhắc tất cả các đầu vào là thù địch cho đến khi được xác thực một cách thích đáng có thể giảm thiểu rất nhiều cuộc tấn công dựa trên các lỗ hổng phổ biến. Đây là một thách thức, vì những nỗ lực xác thực cần diễn ra sau khi mọi phân tích cú pháp đã hoàn tất việc kiểm soát các luồng đầu vào, một tính năng phổ biến trong các ứng dụng dựa-trên-nền-web sử dụng Unicode và các bộ ký tự quốc tế khác.

Xác thực đầu vào là đặc biệt thích hợp đối với những lỗ hổng sau: tràn bộ đệm, phụ thuộc vào đầu vào không đáng tin cậy trong một quyết định bảo mật, cross-site scripting (XSS), yêu cầu cross-site giả mạo (XSRF), xâm nhập đường dẫn, và tính toán kích thước bộ đệm sai. Xác thực đầu vào có vẻ thích hợp với các cuộc tấn công chèn lệnh khác, nhưng do sự phức tạp của đầu vào và sự phân nhánh từ các luồng đầu vào không phù

hợp nhưng hợp pháp, phương pháp này thất bại với hầu hết các cuộc tấn công chèn lệnh.

Những gì có thể hoạt động được là một dạng phương pháp tiếp cận nhận dạng và danh sách trắng, nơi đầu vào được xác thực và sau đó phân tích cú pháp thành một cấu trúc tiêu chuẩn để sau đó được thực thi.

Tác động của việc xử lý đầu vào không phù hợp có thể rất nghiêm trọng, cho phép một kẻ tấn công có được chỗ đứng trên một hệ thống hoặc gia tăng mức độ đặc quyền của chúng. Do kiểu lỗi này phụ thuộc vào tiến trình đang bị tấn công, kết quả có thể khác nhau nhưng hầu hết luôn dẫn đến việc những kẻ tấn công gia tăng chuỗi phá hoại của chúng.



**MÁCH NƯỚC CHO KỲ THI** Xác thực đầu vào là đặc biệt thích hợp đối với những lỗi hổng sau: tràn bộ đệm, phụ thuộc vào đầu vào không đáng tin cậy trong một quyết định bảo mật, cross-site scripting (XSS), yêu cầu cross-site giả mạo (XSRF), xâm nhập đường dẫn, và tính toán kích thước bộ đệm sai. Khi tham gia kỳ thi Security+, hãy tìm kiếm những câu hỏi xác định một số lượng lớn các vấn đề liên quan đến nguyên nhân tiềm năng phổ biến.

### Tấn công Phát lại (Replay Attack)

*Tấn công phát lại* hoạt động chống lại các ứng dụng bằng cách cố gắng tái tạo lại những điều kiện đã từng tồn tại khi chuỗi trình tự của các sự kiện xảy ra lần đầu tiên. Nếu như một kẻ tấn công có thể ghi lại một chuỗi các gói tin và sau đó phát lại chúng, những gì có hiệu lực trước đó có thể vẫn còn có hiệu lực. Một ví dụ của việc này sẽ là việc lặp lại chuỗi giao dịch trước đó, giống như việc thanh toán hai lần hoặc vượt qua kiểm tra an ninh tại một sự kiện đăng nhập. Có một loạt các biện pháp phòng

thủ chống lại các cuộc tấn công phát lại, và vì vậy, kiểu tấn công này không phải là một vấn đề. Tuy nhiên, các nhà phát triển không tuân thủ những thực tiễn tốt nhất có thể tạo ra những bản triển khai bị thiếu khuyết biện pháp bảo vệ phát lại, cho phép kiểu tấn công này tiếp tục tồn tại.

### **Phát lại Phiên (Session Replay)**

Khi một người dùng kết nối tới một hệ thống thông qua trang web, kết nối hình thành nên một “phiên” liên quan đến các phần tử khác nhau được truyền tải qua lại và hình thành nên một cuộc hội thoại giữa máy khách và máy chủ. Một sự kiện *phát lại phiên* là việc tái tạo lại tương tác này sau khi nó đã thực sự diễn ra. Điều này có thể tốt hoặc xấu, tùy thuộc vào tình huống. Nếu như phiên là một giao dịch giữa người dùng và một ngân hàng, khả năng phát lại (nghĩa là, tái tạo lại) phiên sau khi nó đã diễn ra trong thực tế sẽ là một điều tồi tệ. Do đó, đối với các hệ thống giao dịch, ngăn chặn phát lại là điều rất quan trọng và cần phải được tích hợp vào trong hệ thống. Đối với các tương tác web, phát lại có thể cung cấp những thông tin về những gì hoạt động và những gì không trên một cơ sở tương tác máy khách/máy chủ dựa-trên-web.

Để phát lại hoạt động được, cần phải có công cụ đo lường bởi vì hầu hết nội dung và giao dịch đều không có trạng thái, do đó chúng không có thông tin về người dùng đến từ đâu hoặc chúng đã đi đến đâu. Phát lại có thể được quản lý từ phía máy khách hoặc máy chủ, mỗi loại đều có ưu và nhược điểm riêng. Phía máy chủ có thể được nắm bắt lại dựa trên lịch sử các yêu cầu, nhưng sẽ không hiển thị các chuyển động của con chuột và các hoạt động như vậy chỉ dành cho phía-máy-khách. Về phía máy khách, các thẻ gắn nhãn cho phép bạn nắm bắt thông tin chi tiết của các trang. Nhưng giống như mọi giải pháp phía-máy-khách, bất kỳ dữ liệu nào đến từ máy khách đều có thể bị chặn lại và bị thao túng

## Tràn Bộ số nguyên (Integer Overflow)

Một *tràn bộ số nguyên* là một điều kiện lập trình lỗi xảy ra khi một chương trình cố gắng lưu trữ một giá trị số, là một số nguyên, trong một biến có kích thước quá nhỏ để lưu giữ nó. Kết quả sẽ khác nhau tùy theo ngôn ngữ [lập trình] và kiểu số. Trong một số trường hợp, giá trị làm bão hòa biến, giả sử giá trị lớn nhất cho kiểu đã được xác định và không có giá trị nào khác. Trong các trường hợp khác, đặc biệt là với số nguyên có dấu, nó có thể bị chuyển đổi thành giá trị âm vì bit quan trọng nhất thường được dành cho dấu của số. Điều này có thể gây ra các lỗi logic đáng kể trong một chương trình.

Tràn bộ số nguyên được kiểm nghiệm một cách dễ dàng, và các nhà phân tích mã [phần mềm] tinh có thể chỉ ra nơi mà chúng có khả năng xảy ra. Do đó, không có lý do gì để những lỗi này tồn tại trong mã [phần mềm] sản xuất.

## Giả mạo Yêu cầu (Request Forgery)

Giả mạo yêu cầu là một lớp tấn công khi một người dùng thực hiện một hành động thay-đổi-trạng-thái dưới danh nghĩa của một người dùng khác, mà thường là họ không hề hay biết. Điều này giống như việc ai đó bổ sung thêm thông tin vào phản hồi của trang web của bạn. Những cuộc tấn công này sử dụng các đặc điểm mang tính hành vi của các giao thức dựa-trên-web và trình duyệt, và chúng xảy ra do các vấn đề phía-máy-khách nhưng cũng có thể được xem là cả phía máy khách lẫn máy chủ.

## Giả mạo Yêu cầu Phía Máy chủ

Giả mạo yêu cầu phía-máy-chủ là khi một kẻ tấn công gửi các yêu cầu đến ứng dụng phái-máy-chủ để khiến cho các yêu cầu HTTP được gửi đến một miền tùy ý mà kẻ tấn công lựa chọn. Các cuộc tấn công này khai thác mối quan hệ đáng tin cậy giữa máy chủ và mục tiêu, bắt buộc ứng dụng dễ bị tổn thương phải thực hiện các hành động trái phép. Các mối quan

hệ đáng tin cậy điển hình được khai thác là những mối quan hệ tồn tại liên quan đến chính máy chủ hoặc liên quan đến các hệ thống back-end khác trong cùng một tổ chức. Các cuộc tấn công phổ biến bao gồm việc máy chủ tự tấn công hoặc tấn công một máy chủ khác trong tổ chức.

### **Giả mạo Yêu cầu Chéo-Trang (Cross-Site)**

Các cuộc tấn công giả mạo yêu cầu chéo trang (XSRF) sử dụng những hành vi không mong muốn phù hợp với mục đích sử dụng đã xác định nhưng được thực hiện trong các trường hợp nằm ngoài mục đích sử dụng đã được cho phép. Đây là một ví dụ về vấn đề “cấp phó nhầm lẫn”, một nhóm các vấn đề trong đó một thực thể thực hiện một hành động một cách sai lầm dưới danh nghĩa một thực thể khác. Một cuộc tấn công XSRF dựa vào một vài điều kiện để có hiệu quả. Nó được thực hiện dựa trên các trang web có người dùng được xác thực và khai thác sự tin cậy của trang trong sự kiện xác thực trước đó. Sau đó, bằng cách đánh lừa trình duyệt của người dùng gửi một yêu cầu HTTP đến trang web mục tiêu, sự tin cậy sẽ bị lợi dụng. Hãy giả sử ngân hàng của bạn cho phép bạn đăng nhập và thực hiện các giao dịch tài chính nhưng không xác minh tính xác thực cho mỗi giao dịch tiếp theo. Nếu người dùng đã đăng nhập và chưa đóng trình duyệt của họ, thì một hành động trong tab trình duyệt khác có thể gửi một yêu cầu ẩn đến ngân hàng, dẫn đến một giao dịch trông có vẻ như đã được ủy quyền nhưng trên thực tế lại không được thực hiện bởi người dùng.



### **MÁCH NƯỚC CHO KỲ THI**

Có hai kiểu giả mạo yêu cầu: giả mạo yêu cầu phía-máy-chủ và giả mạo yêu cầu chéo-trang. Đưa ra một kịch bản, hãy đảm bảo bạn có thể phân biệt được chúng dựa trên một mô tả về những gì đã xảy ra.

Rất nhiều kỹ thuật giảm nhẹ khác nhau có thể được sử dụng, từ việc giới hạn thời gian xác thực, đến hết hạn cookie, đến quản lý các phần tử đặc biệt của một trang web (ví dụ, kiểm tra tiêu đề). Phương pháp mạnh mẽ nhất là sử dụng các token CSRF ngẫu nhiên theo hình thức thuê bao. Các yêu cầu tiếp theo đó không thể hoạt động bởi vì một token đã không được thiết lập trước. Việc kiểm nghiệm CSRF tiêu tốn nhiều kế hoạch hơn một chút so với các cuộc tấn công kiểu-chèn-lệnh khác, nhưng điều này cũng có thể được thực hiện như một phần của quá trình thiết kế.

### **Tấn công Giao diện Lập trình Ứng dụng (API)**

Phương pháp “thông thường” của việc tương tác với một dịch vụ web là thông qua một loạt các câu lệnh được thực thi trên máy chủ, với các kết quả được gửi ngược lại cho ứng dụng – trình duyệt. Tuy nhiên, với sự gia tăng của điện thoại thông minh, máy tính bảng, và các thiết bị di động khác, cùng với ứng dụng. Một ứng dụng (hoặc app) thường tương tác với dịch vụ thông qua một giao diện lập trình ứng dụng (API). Như với tất cả các điểm nhập, API đều là đối tượng của các cuộc tấn công và lạm dụng. Một *cuộc tấn công giao diện lập trình ứng dụng* là một cuộc tấn công mà kẻ tấn công đặc biệt tấn công API và dịch vụ đăng sau nó bằng cách thao túng các đầu vào. Các API dành cho các dịch vụ web đòi hỏi mức độ quan tâm bảo mật tối thiểu giống như giao diện web tiêu chuẩn, nhưng trong một số trường hợp, chúng có thể yêu cầu mức độ [quan tâm bảo mật] nâng cao. Lý do đăng sau các cấp độ nâng cao rất đơn giản: API được sử dụng để cung cấp dữ liệu cho một ứng dụng, vì vậy một vài trong số các tiến trình xử lý được thực hiện trong ứng dụng. Điều này có nghĩa là giao diện giống như một nguồn cấp dữ liệu thô vào máy chủ, với ít công việc hơn và ít kiểm tra hơn, được thực hiện trên máy chủ. Các giao diện API không được giám sát hoặc kiểm duyệt ở phía máy chủ có thể dẫn đến vi phạm và tiết lộ dữ liệu, giữa các rủi ro bảo mật khác.

## Cạn kiệt Tài nguyên

Mọi hệ thống được định nghĩa như là một tiến trình tạo ra những kết quả đầu ra cụ thể từ kết quả của một tập hợp các đầu vào đã được xác định. Bên trong hệ thống sử dụng một loạt các tài nguyên khác nhau để chuyển đổi được trạng thái đầu vào thành trạng thái đầu ra. *Cạn kiệt tài nguyên* là trạng thái khi một hệ thống không có đủ tất cả các tài nguyên mà nó cần để tiếp tục hoạt động. Hai nguồn tài nguyên phổ biến là dung lượng và bộ nhớ, vốn phụ thuộc lẫn nhau trong một số tình huống nhưng lại hoàn toàn tách biệt trong những trường hợp khác. Dung lượng được xác định bằng việc hệ thống có đủ lượng băng thông giao tiếp, băng thông xử lý cần thiết, và lượng bộ nhớ để quản lý các trạng thái trung gian. Khi một trong số những tài nguyên này bị cạn kiệt, lỗi có thể xảy ra. Ví dụ, nếu một hệ thống có nhiều yêu cầu TCP SYN hơn lượng yêu cầu mà nó có thể xử lý, nó sẽ không thể hoàn thành việc bắt tay và cho phép các kết nối bổ sung. Nếu như một chương trình bị hết bộ nhớ, nó sẽ thất bại trong việc hoạt động một cách đúng đắn. Đây là một ví dụ về cuộc tấn công cạn kiệt tài nguyên, khi đích nhắm mục tiêu của kẻ tấn công là làm suy yếu các nguồn tài nguyên.



## MÁCH NƯỚC CHO KỲ THI

Giống như [tấn công] điều kiện cạnh tranh, những lỗ hổng cạn kiệt tài nguyên có khuynh hướng dẫn đến một sự cố hệ thống. Những cuộc tấn công này có thể ít thiệt hại hơn nhưng xét từ khía cạnh kẻ tấn công luôn coi trọng sự kiên trì như một chiến lược, nó cần phải thay đổi các chức năng của hệ thống như một phần của chiến lược tấn công tổng thể. Tuy nhiên, trong một số trường hợp, sự cố ngừng hoạt động có thể làm dừng các dịch vụ thiết yếu, bao gồm các hệ thống giao-tiếp-với-khách-hàng.

## Rò rỉ bộ nhớ

Quản lý bộ nhớ cấu thành từ những hoạt động được sử dụng để kiểm soát và điều phối bộ nhớ máy tính, cấp phát bộ nhớ cho các biến, và thu hồi nó khi không còn được sử dụng. Các lỗi trong quản lý bộ nhớ có thể dẫn đến *rò rỉ bộ nhớ*, vốn có thể gia tăng theo thời gian, làm tiêu tốn rất nhiều tài nguyên. Một thủ tục thu gom rác được sử dụng để giải phóng bộ nhớ đã được cấp phát cho một chương trình nhưng không còn được cần đến nữa. Trong ngôn ngữ lập trình C++, khi không có bộ thu gom rác, nhà lập trình phải cấp phát và giải phóng bộ nhớ một cách rõ ràng. Một trong những ưu điểm của các ngôn ngữ lập trình mới hơn như Java, C#, Python và Ruby là rằng chúng cung cấp quản lý bộ nhớ tự động hóa cùng với việc thu gom rác. Điều này có thể không có hiệu quả bằng việc lập trình một cách cụ thể trong C nhưng nó có vẻ như có ít lỗi hơn một cách đáng kể.

## Tước bỏ SSL (Secure Socket Layer Stripping)

*Tước bỏ secure socket layer* là một cuộc tấn công kiểu người trung gian chống lại tất cả các kết nối SSL và TLS những phiên bản ban đầu. Cuộc tấn công được thực hiện bất kỳ nơi đâu mà một cuộc tấn công người trung gian có thể diễn ra, khiến cho các trạm phát sóng không dây trở nên một vị trí đắc địa. Cuộc tấn công hoạt động bằng cách can thiệp vào yêu cầu kết nối ban đầu đối với HTTPS, chuyển hướng nó đến một trang HTTP, và sau đó, dàn xếp ở giữa. Nguyên nhân của việc cuộc tấn công này hoạt động là bởi vì việc bắt đầu một bắt tay SSL hoặc TLS (v1.0 hoặc v1.1) là một lỗ hổng đối với cuộc tấn công. Biện pháp phòng thủ chính là kỹ thuật: chỉ sử dụng TLS v1.2 hoặc 1.3, vì những phiên bản này được bảo vệ chống lại phương pháp tấn công cụ thể.

## Thao túng Trình điều khiển (Driver Manipulation)

Trình điều khiển là một phần của phần mềm nằm giữa hệ điều hành và một thiết bị ngoại vi. Xét về một khía cạnh nào đó, các trình điều khiển

là một phần của hệ điều hành, như là một phần mở rộng. Theo một khía cạnh khác, các trình điều khiển là mã [lập trình] không phải là một phần của hệ điều hành và được phát triển bởi các công ty khác thay vì nhà phát triển Hệ điều hành. *Thao túng trình điều khiển* là một cuộc tấn công vào một hệ thống bằng cách thay đổi các trình điều khiển, từ đó thay đổi hành vi của hệ thống. Các trình điều khiển có thể không được bảo vệ tốt như các phần khác của hệ thống lõi, nhưng chúng tham gia vào hệ thống lõi khi được gọi đến. Điều này đã dẫn đến việc các trình điều khiển được ký kết và thắt chặt đáng kể môi trường của các trình điều khiển và các chương trình phụ trợ.

### **Chèn (Shimming)**

*Chèn* là một tiến trình đặt một lớp mã [phần mềm] giữa trình điều khiển và Hệ điều hành. Chèn cho phép sự mềm dẻo và linh động bằng cách cho phép những thay đổi giữa các phiên bản khác nhau của Hệ điều hành mà không cần phải sửa đổi mã [phần mềm] trình điều khiển nguyên thủy. Việc chèn cũng giới thiệu một phương tiện mà theo đó, mã [phần mềm] độc hại có thể thay đổi hành vi của một trình điều khiển mà không cần thay đổi bản thân trình điều khiển.

### **Tái cấu trúc**

*Tái cấu trúc* là tiến trình tái cấu trúc lại mã [phần mềm] máy tính mà không cần thay đổi hành vi bên ngoài của nó. Việc tái cấu trúc được hoàn thành để cải thiện những thuộc tính phi chức năng của phần mềm, chẳng hạn như cải thiện độ tin cậy của mã [phần mềm] và/hoặc giảm độ phức tạp. Việc tái cấu trúc có thể phát lộ những khuyết trong thiết kế dẫn đến những lỗ hổng có thể khai thác được, cho phép những lỗ hổng đó có thể được đóng lại mà không cần thay đổi hành vi của mã [phần mềm]. Tái cấu trúc là một phương tiện mà theo đó, một kẻ tấn công có thể bổ sung thêm chức năng cho một trình điều khiển trong khi vẫn duy

trì được chức năng mong muốn của nó. Mặc dù điều này đi ngược lại nguyên tắc ban đầu của tái cấu trúc – cải thiện tính hiệu quả của mã [phần mềm] – nhưng nó nói lên sự khéo léo của những kẻ tấn công.



**MÁCH NƯỚC CHO KỲ THI** Ví dụ, hãy nhớ rằng chèn là một tiến trình về việc đặt một lớp mã [phần mềm] vào giữa trình điều khiển và Hệ điều hành và rằng tái cấu trúc là tiến trình tái cấu trúc lại mã [phần mềm] máy tính hiện hữu mà không làm thay đổi hành vi bên ngoài của nó.

### **Vượt qua Băm (Pass the Hash)**

*Vượt qua băm* là một kỹ thuật bẻ khóa khi kẻ tấn công bắt lấy hàm băm được sử dụng để xác thực một tiến trình. Sau đó, chúng (*những kẻ tấn công – người dịch*) có thể sử dụng hàm băm này bằng cách chèn nó vào trong một tiến trình đang sử dụng liên quan đến mật khẩu. Đây là một cuộc tấn công kỹ thuật cao cấp mà đích nhắm mục tiêu là tiến trình xác thực của Windows bằng cách chèn một bản sao của mật khẩu băm trực tiếp vào trong hệ thống. Kẻ tấn công không cần phải biết mật khẩu, mà thay vào đó, có thể sử dụng một hàm băm đã được bắt lại và chèn nó một cách trực tiếp, vốn khi đã được xác minh một cách chính xác sẽ cấp quyền truy cập cho kẻ tấn công. Vì đây là một cuộc tấn công cụ thể về mặt kỹ thuật, các công cụ đã được phát triển để tạo điều kiện cho hoạt động của nó.

## Tóm tắt Chương

Chương này giới thiệu những tài liệu tương ứng với các cuộc tấn công vào ứng dụng. Chương được mở đầu với một cuộc thảo luận về leo thang đặc quyền và chèn tập lệnh chéo-trang và tiếp theo bằng các cuộc tấn công chèn lệnh, bao gồm các biến thể SQL, DLL, LDAP và XML. Chủ đề tiếp theo đề cập đến giải tham chiếu con trỏ/giải tham chiếu đối tượng và xâm nhập danh bạ. Tràn bộ nhớ đệm, điều kiện cạnh tranh, và xử lý lỗi không thích hợp tiếp theo ngay sau đó, và chương cũng giải quyết vấn đề xử lý đầu vào không thích hợp. Các kỹ thuật tấn công như tấn công phát lại, tràn bộ số nguyên, và giả mạo yêu cầu cũng được đề cập. Ngay dưới giả mạo yêu cầu là các biến thể phía-máy-chủ và chéo-trang.

Các cuộc tấn công vào các giao diện API, cạn kiệt tài nguyên, và rò rỉ bộ nhớ cũng đã được nhắc đến. Ngoài ra, phương pháp tấn công kẻ trung gian về tước bỏ SSL cũng như là thao túng trình điều khiển thông qua chèn và tái cấu trúc cũng đã được đề cập. Chương kết thúc với một cuộc thảo luận về cuộc tấn công vượt-quá-băm.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Khi một kẻ tấn công bắt được lưu lượng mạng và truyền nó lại tại một thời điểm sau đó thì chúng [kẻ tấn công] đang cố gắng thực hiện kiểu tấn công nào?

  - A. Tấn công từ-chối-dịch-vụ
  - B. Tấn công phát lại
  - C. Tấn công Bluejacking
  - D. Tấn công kẻ trung gian.
2. Kiểu tấn công nào liên quan đến việc kẻ tấn công đặt một lớp mã [phần mềm] giữa một trình điều khiển thiết bị nguyên thủy và hệ điều hành?

  - A. Tái cấu trúc
  - B. Ngựa Trojan
  - C. Chèn (Shimming)
  - D. Vượt qua băm
3. Bạn đang xem xét một ứng dụng web tùy chỉnh và vô tình nhập một số vào trong trường văn bản. Ứng dụng trả về một thông báo lỗi chứa tên gọi của biến, tên tập tin và đường dẫn đầy đủ của ứng dụng. Đây là một ví dụ về kiểu tấn công nào dưới đây?

  - A. Cạn kiệt tài nguyên
  - B. Xử lý lỗi không thích hợp
  - C. Thông điệp lỗi chung
  - D. Cấu hình sai phổ biến.
4. Bạn đang làm việc với một nhóm đang kiểm nghiệm một ứng dụng mới. Bạn nhận thấy rằng khi ba hoặc nhiều người trong số các

bạn nhấp vào nút Gửi trên một biểu mẫu cụ thể tại cùng một thời điểm, ứng dụng luôn bị treo trong mỗi lần. Đây rất có thể là một ví dụ về điều nào sau đây?

- A.** Một điều kiện cạnh tranh
  - B.** Một lỗi không xác định
  - C.** Một tính năng không được lập thành tài liệu
  - D.** Một chèn lệnh DLL.
- 5.** Máy chủ web hướng ra bên ngoài trong tổ chức của bạn liên tục gặp phải sự cố. Khi xem xét máy chủ sau khi khởi động lại, bạn nhận thấy rằng mức sử dụng CPU được chốt và mức sử dụng bộ nhớ đang gia tăng một cách nhanh chóng. Nhật ký lưu lượng cho thấy một lượng lớn các yêu cầu HTTP và HTTPS đi đến máy chủ. Máy chủ web này đang trải qua kiểu tấn công nào?
- A.** Xác thực đầu vào
  - B.** Xử lý lỗi bị phân tán
  - C.** Cạn kiệt tài nguyên
  - D.** Điều kiện cạnh tranh.
- 6.** Tổ chức của bạn đang xem xét sử dụng một bộ mã định danh vé phiếu [hỗ trợ] với hệ thống hỗ trợ dịch vụ hiện tại của bạn. Mã định danh mới sẽ là một số nguyên gồm có 16 chữ số được tạo bằng cách kết hợp ngày, giờ và Mã định danh của nhân viên vận hành. Đáng tiếc, khi bạn đã thử sử dụng số nhận dạng mới trong trường "số phiếu" trên hệ thống hiện tại của mình, ứng dụng này luôn bị lỗi. Phương pháp cũ sử dụng số nguyên có năm chữ số hoạt động tốt. Đây rất có thể là một ví dụ về kiểu tấn công nào dưới đây?
- A.** Cấu hình sai phổ biến
  - B.** Lỗi hổng zero-day
  - C.** Rò rỉ bộ nhớ

- D. Tràn bộ số nguyên.**
7. Trong khi kiểm tra máy tính xách tay đã bị nhiễm phần mềm độc hại, bạn phát hiện ra rằng phần mềm độc hại tải lên khi khởi động và cũng tải một tập tin có tên là netutilities.dll mỗi khi Microsoft Word được mở. Đây là một ví dụ về kiểu tấn công nào dưới đây?
- A. Điều kiện cạnh tranh**  
**B. Chèn tập lệnh DLL**  
**C. Nhiễm trùng hệ thống**  
**D. Tràn bộ nhớ.**
8. Một ứng dụng web bạn đang xem xét có một trường đầu vào dành cho tên người dùng và chỉ ra rằng tên người dùng phải chứa từ 6 đến 12 ký tự. Bạn đã phát hiện ra rằng nếu bạn nhập tên người dùng có độ dài 150 ký tự trở lên, ứng dụng sẽ bị lỗi. Đây là một ví dụ về cái gì?
- A. Rò rỉ bộ nhớ**  
**B. Tràn bộ đệm**  
**C. Xâm nhập danh bạ**  
**D. Tràn bộ số nguyên.**
9. Tổ chức của bạn đang gấp sự cố với một ứng dụng web tùy chỉnh. Ứng dụng trông có vẻ như hoạt động tốt trong một thời gian nhưng bắt đầu bị khóa hoặc bị lỗi sau bảy đến mười ngày sử dụng liên tục. Khi kiểm tra máy chủ, bạn nhận thấy rằng việc sử dụng bộ nhớ dường như tăng lên mỗi ngày cho đến khi máy chủ hết bộ nhớ. Ứng dụng có nhiều khả năng bị lỗi nào sau đây?
- A. Rò rỉ bộ nhớ**  
**B. Rò rỉ tràn (overflow leak)**  
**C. Khai thác Zero-day**  
**D. Giải tham chiếu con trỏ.**

- 10.** Máy chủ cơ sở dữ liệu của bạn đang trả lại một tập dữ liệu lớn cho người dùng trực tuyến gây ra sự bão hòa mạng. Việc trả lại hồ sơ bình thường hầu hết sẽ là một vài trường hợp. Đây là một ví dụ về hình thức tấn công nào?
- A.** Rò rỉ bộ nhớ
  - B.** Chèn tập lệnh LDAP
  - C.** Tấn công kẻ trung gian
  - D.** Chèn tập lệnh SQL.

## Đáp án

1. **B.** Một *cuộc tấn công phát lại* diễn ra khi kẻ tấn công bắt được một phần của giao tiếp giữa hai bên và truyền lại nó ở một thời điểm sau đó. Ví dụ, một kẻ tấn công có thể phát lại một loạt các câu lệnh và mã [phần mềm] được sử dụng trong một giao dịch tài chính để khiến cho giao dịch đó được thực hiện nhiều lần. Nói chung, các cuộc tấn công phát lại được kết hợp với những nỗ lực để phá hoại các cơ chế xác thực, chẳng hạn như bắt lại và tái sử dụng một chứng chỉ hoặc một phiếu.
2. **C.** *Chèn* là tiến trình đặt thêm một lớp mã [phần mềm] giữa trình điều khiển thiết bị và hệ điều hành.
3. **B.** Khi một ứng dụng không bẫy được lỗi một cách chính xác và tạo ra các thông điệp lỗi chứa những thông tin nhạy cảm tiềm tàng thì đây còn được gọi là *xử lý lỗi không thích hợp*.
4. **A.** Đây có nhiều khả năng là một điều kiện cạnh tranh. Một *điều kiện cạnh tranh* là một điều kiện lỗi xảy ra khi kết quả đầu ra của một chức năng phụ thuộc vào trình tự hoặc thời gian của đầu vào. Trong trường hợp này, ứng dụng bị lỗi khi nhiều đầu vào được gửi đi tại cùng một thời điểm bởi vì ứng dụng đang không nhận được các đầu vào hoặc xử lý các đầu vào theo thứ tự đã được kỳ vọng.
5. **C.** *Cạn kiệt tài nguyên* là trạng thái khi mà một hệ thống không có đủ mọi tài nguyên mà nó cần để tiếp tục hoạt động. Trong trường hợp này, máy chủ không có đủ dung lượng bộ nhớ hoặc CPU để xử lý một lượng lớn các yêu cầu HTTP/HTTPS đang được gửi đến.
6. **D.** Một *tràn bộ số nguyên* là một điều kiện lỗi lập trình xảy ra khi một chương trình cố gắng lưu trữ một giá trị số, một số nguyên, trong một biến quá nhỏ để lưu giữ nó. Trong trường

hợp này, số nguyên gồm 16-chữ-số là quá lớn cho trường, vốn chỉ hoạt động tốt với số nguyên gồm 5-chữ-số.

7. **B.** Đây là một ví dụ về *chèn tập lệnh DLL*, là một tiến trình bổ sung thêm vào một chương trình, tại thời điểm hoạt động, một DLL có một lỗ hổng chức năng cụ thể có thể bị lợi dụng bởi một kẻ tấn công.
8. **B.** Đây là một ví dụ tương đối cơ bản về *tràn bộ đệm*. Thủ tục đầu vào không xác thực được đầu vào đã được cung cấp để đảm bảo tối đa 12 ký tự được nhận và xử lý. Trong trường hợp này, ứng dụng đã cố gắng lưu trữ toàn bộ 150 (hoặc hơn) ký tự của tên người dùng, dẫn đến việc khu vực bộ nhớ bị ghi đè lên và gây ra lỗi ứng dụng.
9. **A.** *Rò rỉ bộ nhớ* là các lỗi lập trình xảy ra khi một chương trình máy tính không xử lý tài nguyên bộ nhớ một cách đúng đắn. Theo thời gian, mặc dù chương trình vẫn hoạt động nhưng nó không giải phóng tài nguyên bộ nhớ khi chúng không còn được cần đến, một loạt các phần bộ nhớ chết (*không còn được cần đến – người dịch*) trở nên rải rác trên dấu vết của chương trình trong bộ nhớ. Nếu một chương trình thực thi trong một thời gian dài, những khu vực bộ nhớ chết này có thể phình to và tiêu tốn tài nguyên, gây ra lỗi hệ thống.
10. **D.** Quá nhiều bản ghi được trả về từ một truy vấn SQL là một dấu hiệu của tấn công *chèn tập lệnh SQL*.

## Chương 4      Các Chỉ báo Tấn công (hệ thống) Mạng

---

### Các Chỉ báo Tấn công (hệ thống) Mạng

Trong chương này, bạn sẽ

- Tìm hiểu về các cuộc tấn công hệ thống mạng khác nhau,
  - Phân tích các chỉ báo tiềm năng tương ứng với các cuộc tấn công hệ thống mạng.
- 

Chương này sẽ khám phá các chỉ báo tương ứng với các cuộc tấn công hệ thống mạng. Những chỉ báo này có thể cung cấp những thông tin như cuộc tấn công là gì, điều gì đang diễn ra, và những biện pháp nào là cần thiết để chống lại nó (cuộc tấn công mạng).

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 1.4 của kỳ thi CompTIA Security+: Đưa ra một kịch bản, phân tích các chỉ báo tiềm năng tương ứng với các cuộc tấn công vào hệ thống mạng.

## **Không dây**

Mạng không dây là một công nghệ kết nối mạng phổ biến có một lượng đáng kể các tiêu chuẩn và quy trình để kết nối người dùng với các mạn thông qua các tín hiệu vô tuyến, từ đó, giải phóng máy móc khỏi các cáp truyền dẫn. Như trong mọi hệ thống phần mềm, kết nối mạng không dây là một đích nhắm mục tiêu cho tin tặc. Điều này phần lớn là do thực tế đơn giản là mạng không dây loại bỏ các rào cản về mặt vật lý.

## **Quỷ Song sinh (Evil Twin)**

Một cuộc tấn công *quỷ song sinh* là một cuộc tấn công chống lại giao thức không dây thông qua phần cứng thay thế. Kiểu tấn công này sử dụng một điểm truy cập (Access Point – AP) được sở hữu bởi một kẻ tấn công thường được khuếch đại với các râu ăng-ten có công-suất-cao-hơn, lợi-lộc-nhiều-hơn để trông giống như một kết nối tốt hơn đối với người dùng và những máy tính đang kết nối với nó. Bằng cách khiến cho người dùng kết nối vào điểm truy cập “ma quỷ”, những kẻ tấn công có thể phân tích và thực hiện những cuộc tấn công kiểu-người-trung-gian một cách dễ dàng hơn. Đối với tấn công từ chối dịch vụ (DoS) đơn giản, một kẻ tấn công có thể sử dụng sự can thiệp để làm nhiễu tín hiệu không dây, không cho phép bất kỳ máy tính nào kết nối vào điểm truy cập một cách thành công.

## **Điểm Truy cập Giả mạo (Rogue Access Point)**

Bằng cách thiết lập một *điểm truy cập giả mạo*, một kẻ tấn công có thể cố gắng khiến cho các máy khách kết nối vào nó như thể nó đã được cấp phép và sau đó chỉ đơn giản là xác thực với AP thực – một cách đơn giản để có được quyền truy cập vào trong hệ thống mạng và thông tin đăng nhập của các máy khách. Các AP giả mạo có thể đóng vai trò như một người trung gian và dễ dàng đánh cắp thông tin đăng nhập của người

dùng. Các công ty với các AP không dây nên quét định kỳ để tìm và loại bỏ các AP giả mạo, vì người dùng rất khó tránh khỏi chúng.



**MÁCH NƯỚC CHO KỲ THI** Một AP giả mạo là một AP thường được đặt trên một mạng nội bộ do ngẫu nhiên hoặc vì một lý do bất chính. Nó không được quản lý bởi chủ sở hữu hoặc quản trị viên của mạng. Một “quỷ song sinh” là một AP giả mạo để trông như hợp pháp nhưng không phải vậy và thường được sử dụng để nghe lén các giao tiếp mạng không dây.

### **Bluesnarfing**

*Bluesnarfing* tương tự như bluejacking (sẽ được thảo luận tiếp theo) ở chỗ nó sử dụng cùng một giao thức truyền tải liên hệ. Sự khác biệt là thay vì gửi một tin nhắn không mong muốn đến điện thoại của nạn nhân, kẻ tấn công sao chép những thông tin của nạn nhân, có thể bao gồm email, danh sách liên hệ, lịch và bất kỳ thứ gì khác tồn tại trên thiết bị đó. Các điện thoại gần đây hơn với khả năng đa phương tiện có thể bị đánh cắp các hình ảnh quay video riêng tư. Bluesnarfing đã từng yêu cầu một máy tính xách tay có bộ điều hợp Bluetooth, giúp cho việc xác định kẻ tấn công có thể tương đối dễ dàng, nhưng các ứng dụng bluesnarfing hiện đã có sẵn cho các thiết bị di động. Bloover, một sự kết hợp của Bluetooth và Hoover, là một trong những ứng dụng chạy như một ứng dụng Java. Phần lớn điện thoại Bluetooth cần phải được phát hiện để cuộc tấn công bluesnarf hoạt động được và các điện thoại không nhất thiết phải được ghép nối [với nhau qua Bluetooth]. Về lý thuyết, một kẻ tấn công cũng có thể tấn công cưỡng bức (brute force) tên gọi dài 48-bit duy nhất của thiết bị. Một chương trình có tên gọi là RedFang cố gắng

thực hiện cuộc tấn công cưỡng bức này bằng cách gửi tất cả những tên gọi khả dĩ và xem xem những ai phản hồi. Phương pháp tiếp cận này đã được giải quyết trong Bluetooth 1.2 với một chế độ nặc danh.



## MÁCH NƯỚC CHO KỲ THI

Mục tiêu kỳ thi Security+ là phân tích các cuộc tấn công dựa-trên-mạng, và trong trường hợp bluesnarfing và bluejacking, cả hai đều là các cuộc tấn công đối với Bluetooth. Chúng khác nhau ở chỗ bluejacking là gửi dữ liệu trái phép thông qua Bluetooth, trong khi bluesnarfing là chiếm lấy dữ liệu trái phép thông qua một kênh Bluetooth. Hiểu được sự khác biệt là điều rất quan trọng.

### Bluejacking

*Bluejacking* là một thuật ngữ được sử dụng để chỉ việc gửi những thông điệp trái phép cho thiết bị Bluetooth khác. Điều này liên quan đến việc gửi một thông điệp như là một danh sách liên hệ điện thoại:



Kẻ tấn công sau đó gửi thông điệp cho người nhận khả dĩ thông qua Bluetooth. Ban đầu, điều này liên quan đến việc gửi đi một tin nhắn văn bản, nhưng những điện thoại mới gần đây cũng có thể gửi cả hình ảnh hoặc âm thanh. Một biến thể phổ biến của việc này là việc truyền tải những hình ảnh “gây sốc”, có chứa những hình ảnh đáng lo ngại hoặc thô tục. Vì Bluetooth là một giao thức tầm ngắn nên cuộc tấn công và nạn nhân phải ở trong phạm vi cách nhau khoảng 10 mét. Điện thoại của nạn nhân cũng phải được bật Bluetooth và phải ở chế độ có thể phát hiện được. Trên một số điện thoại đời đầu, đây là cấu hình mặc định và mặc dù nó giúp kết nối các thiết bị bên ngoài dễ dàng hơn, nhưng nó cũng cho phép các cuộc tấn công chöng lại điện thoại. Nếu Bluetooth bị tắt hoặc nếu thiết bị được đặt ở chế độ không thể phát hiện, có thể tránh bị bluejacking.

### **Ngắt kết nối (Disassociation)**

Các cuộc tấn công *ngắt kết nối* chống lại một hệ thống không dây là những cuộc tấn công được thiết kế để ngắt kết nối một máy vật chủ khỏi điểm truy cập không dây và khỏi mạng không dây. Các cuộc tấn công bắt nguồn từ khuôn khổ hủy xác thực theo tiêu chuẩn IEEE 802.11 (Wi-Fi). Khuôn khổ hủy xác thực được thiết kế như một công cụ để loại bỏ các máy trạm trái phép ra khỏi điểm truy cập Wi-Fi, nhưng do thiết kế của giao thức, hầu như bất kỳ ai cũng có thể thực hiện các khuôn khổ này. Một kẻ tấn công chỉ cần có địa chỉ MAC của nạn nhân đã được dự định, vốn cho phép chúng gửi một thông điệp giả mạo đến điểm truy cập, đặc biệt là giả mạo địa chỉ MAC của máy nạn nhân. Điều này dẫn đến việc máy nạn nhân bị ngắt kết nối, khiến cho cuộc tấn công này trở thành một hình thức từ chối dịch vụ.

Các cuộc tấn công ngắt kết nối thường không được sử dụng một mình mà thay vào đó kết hợp với một mục tiêu tấn công khác. Ví dụ, nếu bạn ngắt

kết nối và sau đó đánh hơi kết nối lại, bạn có thể đánh được cắp mật khẩu. Sau khi một máy bị ngắt kết nối, người dùng đang cố gắng thiết lập lại một phiên WPA/WPA2/WPA3 sẽ cần lặp lại quá trình bắt tay bốn-chiều. Điều này cho phép tin tặc có cơ hội đánh hơi sự kiện này, bước đầu tiên để thu thập thông tin cần thiết cho một cuộc tấn công bẻ khóa mật khẩu WPA dựa trên từ điển hoặc tấn công cưỡng bức. Việc buộc người dùng phải kết nối lại sẽ tạo ra cơ hội cho một cuộc tấn công người trung gian chöng lại nội dung đã được cung cấp trong quá trình kết nối. Điều này đã được sử dụng bởi công cụ Wifiphisher để thu thập mật khẩu.



**LƯU Ý** Wifiphisher là một công cụ bảo mật thường được sử dụng bởi nhóm đỏ (red team) trong kiểm nghiệm xâm nhập để gắn kết các cuộc tấn công lừa đảo được tự động hóa chống lại các mạng Wi-Fi nhằm thu thập những thông tin đăng nhập hoặc lây nhiễm phần mềm độc hại cho nạn nhân.

### Sự nhồi nhét (Jamming)

*Sự nhồi nhét* là một hình thức tấn công từ chối dịch vụ nhằm mục tiêu cụ thể vào khía cạnh dài phổ vô tuyến của mạng không dây. Cũng giống như các cuộc tấn công DoS khác có thể thao túng mọi thứ đãng sau hậu trường, cũng có thể nhồi nhét trên một AP không dây, cho phép thực hiện các hành động chẳng hạn như gắn vào một AP giả mạo.

### Nhận diện Tần số Vô tuyến (RFID)

Các thẻ gắn *nhận diện tần số vô tuyến (RFID)* được sử dụng trong nhiều trường hợp. Từ thiết bị theo dõi đến chìa khóa, việc tuân tự hóa độc đáo của các thiết bị cảm biến từ xa này đã khiến chúng trở nên rất hữu ích trong một loạt các ứng dụng. Thẻ RFID có nhiều hình thức khác nhau và

có thể được phân loại là chủ động hoặc thụ động. Các thẻ chủ động có một nguồn điện, trong khi các thẻ thụ động sử dụng năng lượng RF (tần số vô tuyến) được truyền tải cho chúng để tạo ra năng lượng. Thẻ RFID được sử dụng như một phương tiện nhận dạng và chúng có lợi thế hơn mã vạch ở chỗ không cần phải nhìn thấy, chỉ trong phạm vi sóng vô tuyến (vài cm đến 200 mét, tùy thuộc vào loại thẻ). Thẻ RFID được sử dụng trong một loạt các tình huống bảo mật, bao gồm cả các hệ thống nhận dạng không tiếp xúc như các hệ thống thẻ thông minh.

Thẻ RFID có rất nhiều mối quan tâm về bảo mật. Đầu tiên và quan trọng nhất, bởi vì chúng được kết nối thông qua năng lượng RF nên bảo mật vật lý là một thách thức. Bảo mật là một vấn đề quan trọng đối với hệ thống thẻ RFID vì chúng tạo thành một phương tiện nhận dạng, và cần phải xác thực và bảo mật đối với việc truyền dữ liệu. Một số tiêu chuẩn có liên quan đến việc đảm bảo luồng dữ liệu RFID bao gồm ISO/IEC 18000 và ISO/IEC 29167 cho các phương pháp mã hóa để hỗ trợ tính bảo mật, không thể truy xuất, xác thực thẻ và đầu đọc và quyền riêng tư qua mạng, trong khi ISO/IEC 20248 chỉ định cấu trúc dữ liệu chữ ký số để sử dụng trong các hệ thống RFID.

Một số kiểu tấn công khác nhau có thể được thực hiện đối với hệ thống RFID bao gồm:

- Tấn công chính bản thân các thiết bị RFID (các con chip và đầu đọc),
- Tấn công các kênh giao tiếp giữa thiết bị và đầu đọc,
- Tấn công đầu đọc và các thiết bị back-end.

Loại cuối cùng là tấn công Công nghệ Thông tin/Hệ thống Thông tin tiêu chuẩn, tùy thuộc vào các giao diện được sử dụng (web, cơ sở dữ liệu, v.v...) và không được đề cập thêm. Các cuộc tấn công chống lại các kênh

giao tiếp tương đối dễ dàng bởi vì các tần số vô tuyến đã được biết và các thiết bị tồn tại để giao tiếp với các thẻ. Hai hình thức tấn công chính là phát lại và nghe trộm. Trong một cuộc tấn công phát lại, thông tin RFID được ghi lại và được phát lại sau đó. Trong trường hợp huy hiệu truy cập dựa-trên-RFID, nó có thể được đọc trong một nhà hàng từ xa và sau đó được phát lại tại điểm đi vào thích hợp để được vào cửa. Trong trường hợp nghe trộm, dữ liệu có thể được thu thập, giám sát chuyển động của các thẻ cho bất kỳ mục đích nào được cần đến bởi một bên trái phép. Cả hai cuộc tấn công này đều dễ dàng bị đánh bại bằng cách sử dụng các tiêu chuẩn bảo mật ISO/IEC đã được liệt kê trước đó.

Nếu tấn công nghe trộm là điều khả thi, vậy còn cuộc tấn công người trung gian thì sao? Đây điều chắc chắn là điều khả thi, vì chúng sẽ là sự kết hợp của một hành động đánh hơi (nghe trộm) và tiếp theo sau đó là một cuộc tấn công phát lại (giả mạo). Điều này dẫn đến câu hỏi liệu RFID có thể được nhân bản hay không. Câu trả lời là có, nếu thông tin RFID không được bảo vệ thông qua một thành phần mật mã.

Đánh cắp RFID, hoặc đọc lướt (skimming), đã là một chủ đề an ninh trong tin tức. Kẻ trộm có thể sử dụng các thiết bị nhỏ sẽ quét thẻ của bạn, khai thác công nghệ không tiếp xúc để lấy thông tin từ đó, sau đó có thể được sử dụng để tạo nên thẻ sao chép hoặc các cách truy cập tiền khác. Không rõ chính xác mức độ phổ biến của thực tế này, nhưng người ta cho rằng nó đang gia tăng khi công nghệ không tiếp xúc trở nên phổ biến hơn và các thiết bị sử dụng công nghệ này trở nên rẻ tiền hơn.



**LƯU Ý** Rất nhiều ví tiền (điện tử) trên thị trường hiện nay cung cấp một số hình thức bảo vệ RFID. Việc này khác nhau giữa các ví tiền nhưng

nói chung, chúng hoạt động bằng cách chặn tần số được sử dụng để truy cập vào dữ liệu, do đó, bảo vệ thẻ của bạn.

### **Giao tiếp Trưởng Gần bên (Near Field Communication - NFC)**

*Giao tiếp trường gần bên (NFC)* là một bộ các công nghệ không dây cho phép điện thoại thông minh và những thiết bị khác thiết lập một giao tiếp qua sóng vô tuyến qua một khoảng cách ngắn, thường là 10cm (3.9 inch) hoặc ít hơn. Công nghệ này đã không được sử dụng nhiều cho đến thời gian gần đây, khi nó bắt đầu được sử dụng để chuyển dữ liệu giữa các điện thoại di động và trong các hệ thống thanh toán di động. Giờ đây, NFC đã trở thành phương thức chính để thanh toán qua điện thoại di động, nó đang trở nên phổ biến và trong rất nhiều trường hợp, được kết nối trực tiếp với những thông tin tài chính. Vì vậy, tầm quan trọng của việc hiểu và bảo vệ kênh giao tiếp này là điều tối quan trọng.



### **MÁCH NƯỚC CHO KỲ THI**

Điều quan trọng là biết được rằng RFID là một tiến trình mà theo đó, một thẻ tín dụng hoặc giao tiếp điện thoại với một đầu đọc bằng cách sử dụng sóng vô tuyến và rằng NFC là một tập con tần số cao của RFID và hoạt động ở một khoảng cách ngắn hơn nhiều.

### **Véc-tơ Khởi tạo (Initiation Vector - IV)**

*Véc-tơ khởi tạo (IV)* được sử dụng trong các hệ thống không dây như là phần tử ngẫu nhiên tại thời điểm bắt đầu một kết nối. Các cuộc tấn công chống lại nó nhằm mục đích xác định IV, từ đó tìm ra chuỗi trình tự khóa lặp lại.

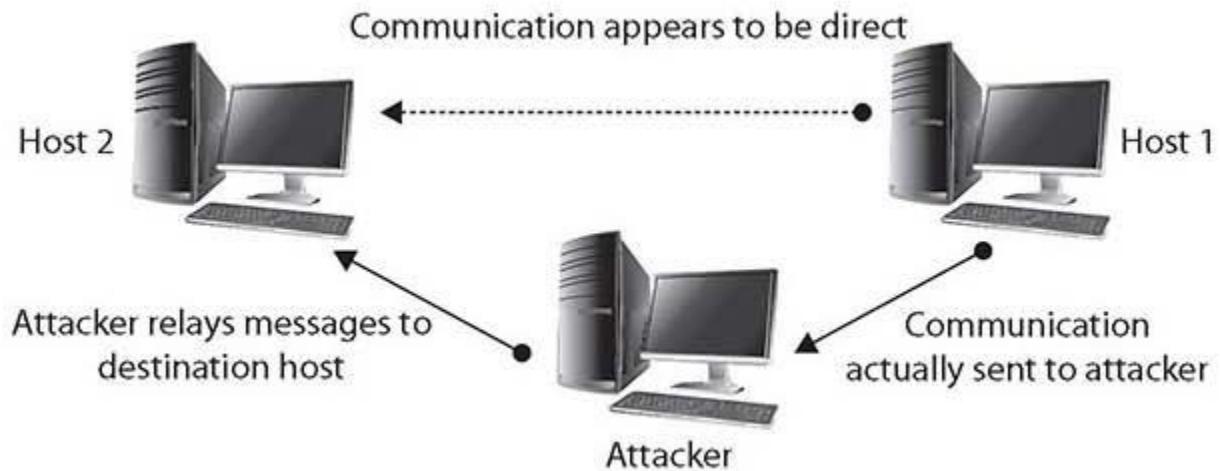
IV là lý do chính cho những điểm yếu trong Quyền riêng tư Tương đương Mạng có dây (Wired Equivalent Privacy - WEP). IV được gửi trong phần

văn bản rõ ràng của thông điệp, và bởi vì tổng không gian phím là khoảng 16 triệu phím, sẽ có cùng một phím được sử dụng lại. Khi khóa đã được lặp lại, kẻ tấn công có hai mật mã đã được mã hóa với cùng một dòng khóa. Điều này cho phép kẻ tấn công kiểm tra bản mã hóa và truy xuất được khóa. Cuộc tấn công này có thể được cải thiện bằng cách chỉ kiểm tra các gói có IV yếu, giảm số lượng gói cần thiết để bẻ khóa. Khi chỉ có các gói với IV yếu được kiểm tra, số lượng gói được bắt cần thiết giảm xuống còn khoảng bốn hoặc năm triệu, có thể chỉ mất vài giờ để bắt được trên một AP tương đối bận rộn. Để tham khảo, điều này có nghĩa là thiết bị có khóa WEP được quảng cáo là 128 bit có thể bị bẻ khóa trong vòng chưa đầy một ngày, trong khi để bẻ khóa một khóa 128 bit thông thường sẽ mất khoảng 2.000.000.000.000.000.000 năm trên một máy tính có thể thử một nghìn tỷ khóa một giây. Nói cách khác, IV yếu có nghĩa là mức độ bảo mật thực sự không bằng 128 bit. AirSnort là một chương trình đánh hơi đã được sửa đổi, lợi dụng điểm yếu này để bắt lấy các khóa WEP. Điểm yếu lớn nhất của WEP là vấn đề IV tồn tại bất kể độ dài khóa là bao nhiêu vì IV luôn duy trì ở mức 24 bit.

### Tấn công Trên đường (On-path Attack)

Một cuộc tấn công *người trung gian (MITM)*, như hàm ý của tên gọi, thường xảy ra khi một kẻ tấn công có khả năng đặt chính mình vào giữa hai hoặc nhiều máy vật chủ đang giao tiếp với nhau. Lý tưởng nhất (từ quan điểm của kẻ tấn công), điều này được thực hiện bằng cách đảm bảo rằng mọi giao tiếp đến hoặc đi từ các máy vật chủ mục tiêu được định tuyến đi qua máy vật chủ của kẻ tấn công (vốn có thể được thiết lập nếu như kẻ tấn công có thể xâm phạm bộ định tuyến của máy vật chủ được nhắm mục tiêu). Sau đó, kẻ tấn công có thể quan sát tất cả lưu lượng trước khi chuyển tiếp nó và thực tế có thể sửa đổi hoặc chặn lưu lượng lại. Đối với máy vật chủ được nhắm mục tiêu, nó trông có vẻ như giao

tiếp đang diễn ra một cách bình thường, vì tất cả mọi phản hồi được mong đợi đều được nhận. [Hình 4-1](#) minh họa cho kiểu tấn công này.



**Hình 4-1 – Một cuộc tấn công người trung gian**

Có rất nhiều phương pháp để khởi tạo một cuộc tấn công kiểu người trung gian. Một trong số các phương pháp phổ biến nhất là thông qua việc *chiếm quyền điều khiển phiên*, có thể xảy ra khi những thông tin như cookie bị đánh cắp, cho phép kẻ tấn công mạo danh phiên hợp pháp. Cuộc tấn công này có thể là kết quả của một cuộc tấn công tập lệnh kịch bản chéo-trang, đánh lừa người dùng thực thi mã [phần mềm] dẫn đến đánh cắp cookie. Số lượng thông tin có thể thu được trong cuộc tấn công người trung gian sẽ bị hạn chế nếu thông tin liên lạc được mã hóa. Tuy nhiên, ngay cả trong trường hợp này, thông tin nhạy cảm vẫn có thể thu được, vì việc biết được giao tiếp nào đang được thực hiện và giữa những cá nhân nào, trên thực tế có thể cung cấp thông tin có giá trị trong một số trường hợp nhất định.

Cuộc tấn công *kẻ trong trình duyệt* (*man in the browser* – MITB) là một biến thể của một cuộc tấn công kẻ trung gian. Trong một cuộc tấn công MITB, phần tử đầu tiên là một cuộc tấn công bằng phần mềm độc hại đưa

một phần tử trojan có thể hoạt động như một proxy vào máy mục tiêu. Phần mềm độc hại này thay đổi hành vi của trình duyệt thông qua các đối tượng hoặc tiện ích mở rộng của trình trợ giúp trình duyệt. Ví dụ, khi người dùng kết nối với ngân hàng của họ, phần mềm độc hại nhận ra mục tiêu (một giao dịch tài chính) và tự đưa nó vào giữa luồng của cuộc hội thoại. Ví dụ, khi người dùng chấp thuận chuyển khoản 150 đô la để thanh toán cho hóa đơn tiện ích, phần mềm độc hại sẽ chặn các lần nhấn phím của người dùng và sửa đổi chúng để thực hiện một giao dịch khác. Một ví dụ nổi tiếng về cuộc tấn công MITB là phần mềm độc hại tài chính Zeus, nhắm mục tiêu vào các giao dịch tài chính trên máy của người dùng, thao túng và thay đổi chúng sau khi người dùng đã nhập thông tin đăng nhập mật khẩu [vào trình duyệt].

---



**MÁCH NƯỚC CHO KỲ THI** MITM và MITB là tương tự nhau, nhưng cũng vẫn có điểm khác. Có khả năng phân biệt giữa hai điều này dựa trên các chi tiết của câu hỏi.

### Tấn công Lớp 2

Lớp 2 của một mạng là nơi mà các quyết định đánh địa chỉ cục bộ được đưa ra. Các bộ chuyển mạch hoạt động ở lớp 2, hoặc các địa chỉ kiểm soát truy cập phương tiện (MAC). Có rất nhiều cách giả mạo cấp độ địa chỉ này [địa chỉ lớp 2], và Security+ xác định 3 cách thức đáng kể: nhiễm độc Giao thức Phân giải Địa chỉ (ARP), ngập lụt kiểm soát truy cập phương tiện (MAC) và nhân bản MAC.

---



**MÁCH NƯỚC CHO KỲ THI** Việc hiểu được cách thức lớp 2 hoạt động giúp bạn hiểu được cách nó bị lạm dụng như thế nào. Các cuộc tấn công

tại lớp 2 chỉ sử dụng hệ thống khác với như đã được dự định, nhưng vẫn theo một cách thức thích đáng. Do đó, việc tìm hiểu cách thức hoạt động của lớp 2 cho phép bạn xem xét cách các cuộc tấn công hoạt động như thế nào.

### **Nhiễm độc Giao thức Phân giải địa chỉ (ARP)**

Khi truyền các gói tin giữa các máy, một thiết bị thỉnh thoảng cần phải biết đâu là nơi để gửi một gói tin đến bằng cách sử dụng MAC hoặc địa chỉ lớp 2. Giao thức Phân giải Địa chỉ (ARP) giải quyết vấn đề này thông qua 4 kiểu thông điệp cơ bản:

- **Yêu cầu ARP** "Ai có địa chỉ IP này?"
- **Phản hồi ARP** "Tôi có địa chỉ IP đó, địa chỉ MAC của tôi là..."
- **Đảo ngược yêu cầu ARP (RARP)** "Ai có địa chỉ MAC này?"
- **Phản hồi RARP** "Tôi có địa chỉ MAC đó, địa chỉ IP của tôi là..."

Các thông điệp này được sử dụng cùng với một bảng ARP của thiết bị, nơi một dạng bộ nhớ ngắn-hạn được liên kết với các phần tử dữ liệu này đang lưu trú. Các câu lệnh được sử dụng như một dạng thức tra cứu đơn giản. Khi một máy gửi yêu cầu ARP đến mạng, phản hồi sẽ được nhận và được nhập vào tất cả các thiết bị nghe được câu phản hồi. Điều này tạo điều kiện thuận lợi cho việc tra cứu địa chỉ hiệu quả, nhưng cũng khiến cho hệ thống trở thành đối tượng bị tấn công.

Khi bảng ARP nhận được phản hồi, nó sẽ tự động tin tưởng vào câu trả lời và cập nhật vào bảng. Một số hệ điều hành thậm chí sẽ chấp nhận dữ liệu phản hồi ARP nếu chúng chưa bao giờ nghe thấy yêu cầu ban đầu. Không có cơ chế xác minh tính xác thực của dữ liệu đã nhận được. Kẻ tấn công có thể gửi thông điệp, làm hỏng bảng ARP và khiến các gói bị định tuyến sai. Hình thức tấn công này được gọi là *nhiễm độc ARP* và dẫn đến chuyển hướng địa chỉ độc hại. Điều này có thể cho phép một cơ chế mà

theo đó, kẻ tấn công có thể tự đưa mình vào giữa cuộc hội thoại giữa hai thiết bị —tấn công người trung gian.

### **Gây ngập lụt Media Access Control (MAC)**

Việc định địa chỉ tại giao diện lớp 2 được thực hiện bởi các địa chỉ kiểm soát truy cập phương tiện (MAC) và các bộ chuyển mạch và các hub. Các hub gửi tất cả các gói tin đến cho mọi người, nhưng bộ chuyển mạch tìm kiếm địa chỉ trong một bảng được lưu trữ và chỉ gửi đến cho địa chỉ đó. *Gây ngập lụt MAC* là một cuộc tấn công trong đó kẻ tấn công làm tràn ngập bảng với các địa chỉ, khiến cho bộ chuyển mạch không thể tìm thấy địa chỉ chính xác cho một gói tin. Bộ chuyển mạch phản hồi bằng cách gửi gói tin đến mọi địa chỉ, và khi này về bản chất nó hoạt động giống như một hub. Bộ chuyển mạch cũng yêu cầu thiết bị chính xác cung cấp địa chỉ của nó, do đó thiết lập bộ chuyển mạch để nhiễm độc ARP, như đã được mô tả trong phần trước.

### **Nhân bản MAC**

*Nhân bản MAC* là hành động thay đổi một địa chỉ MAC để vượt qua kiểm tra bảo mật dựa trên địa chỉ MAC. Điều này có thể hoạt động khi các gói tin trả về đang được định tuyến theo địa chỉ IP và có thể được liên kết một cách chính xác đến đúng địa chỉ MAC. Không phải tất cả mọi nhân bản MAC đều là một cuộc tấn công, những bộ định tuyến tường lửa loại nhỏ đều có một chức năng nhân bản MAC, theo đó thiết bị có thể nhân bản một địa chỉ MAC để khiến cho nó trông như có vẻ trong suốt đối với các thiết bị khác chẳng hạn như kết nối cáp bộ điều giải (modem).

### **Hệ thống Tên Miền (Domain Name System – DNS)**

Hệ thống Tên Miền (DNS) là danh bạ điện thoại dành cho việc đánh địa chỉ. Khi bạn cần phải biết nơi để gửi gói tin đến nhưng không nằm trên mạng cục bộ của bạn, DNS sẽ cung cấp địa chỉ chính xác để gửi gói tin đến đích đến của nó. Điều này khiến cho DNS trở thành một đích nhắm

mục tiêu chủ yếu của những kẻ tấn công, bởi vì nếu bạn làm sai lệch DNS, bạn có thể kiểm soát nơi mà mọi gói tin sẽ đi đến. Một vài cuộc tấn công kỹ thuật và một cuộc tấn công vận hành ở cấp độ định địa chỉ này được đề cập đến trong mục tiêu này.

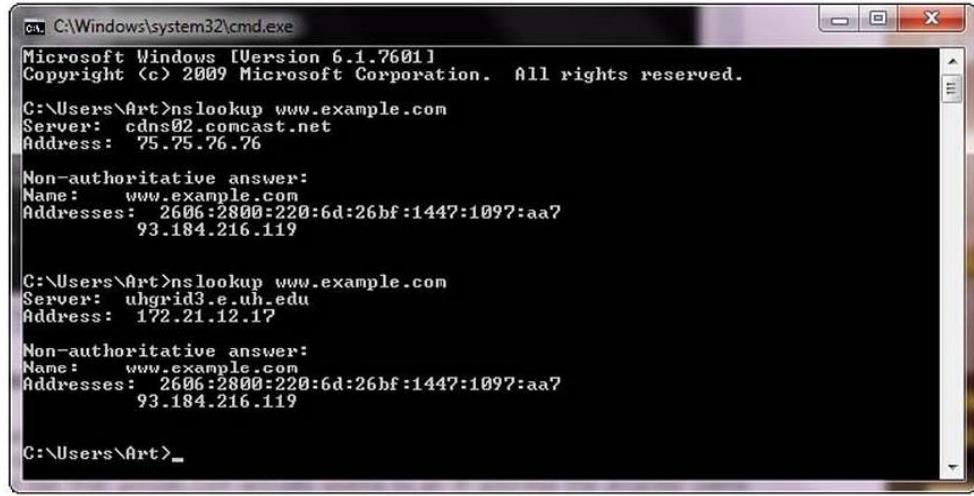
### **Chiếm đoạt Tên miền**

*Chiếm đoạt tên miền* là hành động thay đổi thông tin đăng ký của một tên miền mà không được ủy quyền từ người đăng ký ban đầu. Về mặt kỹ thuật, đây là một hành vi phạm tội, hành động này có thể gây ra hậu quả nghiêm trọng vì hệ thống DNS sẽ lan truyền vị trí tên miền sai lệch đi xa một cách tự động. Chủ sở hữu ban đầu có thể yêu cầu sửa đổi nó, nhưng điều này có thể sẽ mất thời gian.

### **Nhiễm độc DNS**

Hệ thống Tên Miền (DNS) được sử dụng để chuyển đổi một tên miền thành một địa chỉ IP. Không phải chỉ có một hệ thống DNS đơn lẻ mà thay vào đó là một cấu trúc phân cấp các máy chủ DNS – từ các máy chủ root trên trực xương sống của Internet đến các bản sao tại ISP của bạn, bộ định tuyến gia đình của bạn cho đến máy tính cục bộ của bạn, tại mỗi thiết bị đều dưới dạng bộ nhớ đệm DNS. Để kiểm tra một truy vấn DNS cho một địa chỉ cụ thể, bạn có thể sử dụng câu lệnh **nslookup**. [Hình 4-2](#) cho thấy một loạt các truy vấn DNS được thực thi trên một máy tính Windows. Trong yêu cầu đầu tiên, máy chủ DNS là từ một ISP, trong khi trong yêu cầu thứ hai, máy chủ DNS là từ một kết nối mạng riêng ảo (VPN). Giữa hai yêu cầu, các kết nối mạng đã được thay đổi, dẫn đến việc tra cứu DNS khác nhau. Việc thay đổi nơi DNS được phân giải có thể là một cuộc tấn công *nhiễm độc DNS*. Thách thức trong việc phát hiện các cuộc tấn công này là biết mục nhập DNS có căn cứ đích xác (authoritative) nên là gì và sau đó phát hiện khi nào nó thay đổi theo một cách trái phép. Việc

sử dụng VPN có thể làm thay đổi nguồn DNS và điều này có thể được mong muốn, nhưng những thay đổi trái phép có thể bị tấn công.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Art>nslookup www.example.com
Server: cdns02.comcast.net
Address: 75.75.76.76

Non-authoritative answer:
Name: www.example.com
Addresses: 2606:2800:220:6d:26bf:1447:1097:aa7
93.184.216.119

C:\Users\Art>nslookup www.example.com
Server: uhgrid3.e.uh.edu
Address: 172.21.12.17

Non-authoritative answer:
Name: www.example.com
Addresses: 2606:2800:220:6d:26bf:1447:1097:aa7
93.184.216.119

C:\Users\Art>_
```

**Hình 4-2 – nslookup của một truy vấn DNS**

Đôi khi, **nslookup** sẽ trả về một kết quả nonauthoritative, như được minh họa trong [Hình 4-3](#). Điều này thường có nghĩa là kết quả đến từ một bộ đệm thay vì từ một máy chủ có câu trả lời có căn cứ đích xác (nghĩa là, câu trả lời được biết đến là đang hiện hành).



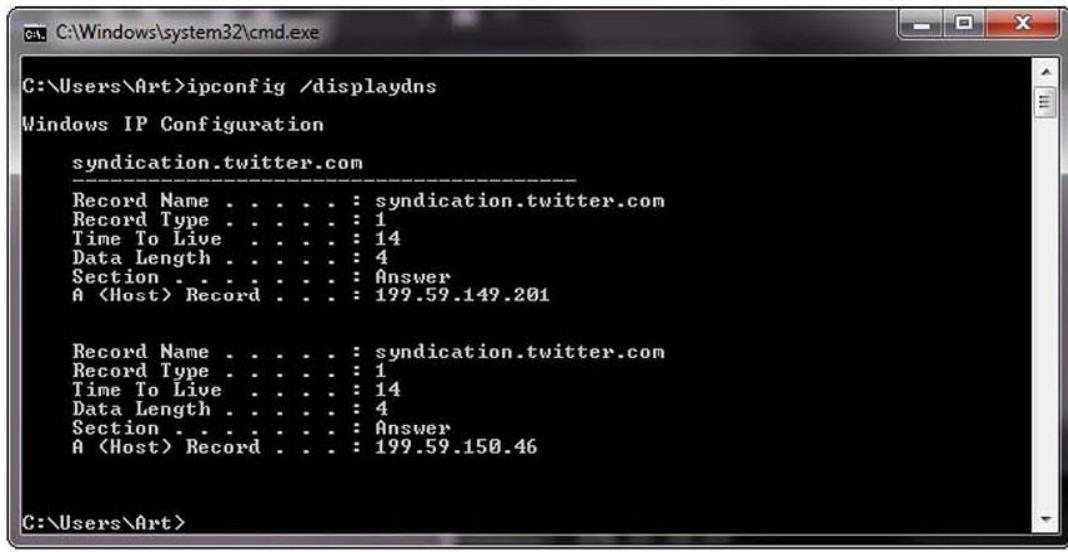
```
C:\Windows\system32\cmd.exe
C:\Users\Art>nslookup www.google.com
Server: uhgrid3.e.uh.edu
Address: 172.21.12.17

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f810:4001:c05::63
74.125.193.105
74.125.193.147
74.125.193.104
74.125.193.103
74.125.193.99
74.125.193.106

C:\Users\Art>_
```

**Hình 4-3 – Phản hồi bộ đệm cho một truy vấn DNS**

Có một số câu lệnh khác mà bạn có thể sử dụng để kiểm tra và xử lý bộ nhớ đệm DNS trên một hệ thống. Trong Windows, câu lệnh **ipconfig/displaydns** sẽ cho thấy bộ nhớ đệm DNS hiện hành trên một máy. [Hình 4-4](#) minh họa cho một bộ đệm DNS nhỏ. Bộ đệm này gần đây đã được làm trống bằng cách sử dụng câu lệnh **ipconfig/flushdns** để làm cho nó vừa với màn hình.



```
C:\> C:\Windows\system32\cmd.exe
C:\> C:\Users\Art>ipconfig /displaydns
Windows IP Configuration

syndication.twitter.com
-----
Record Name . . . . . : syndication.twitter.com
Record Type . . . . . : 1
Time To Live . . . . . : 14
Data Length . . . . . : 4
Section . . . . . : Answer
A <Host> Record . . . . : 199.59.149.201

Record Name . . . . . : syndication.twitter.com
Record Type . . . . . : 1
Time To Live . . . . . : 14
Data Length . . . . . : 4
Section . . . . . : Answer
A <Host> Record . . . . : 199.59.150.46

C:\> C:\Users\Art>
```

**Hình 4-4 – Phản hồi bộ đệm cho một truy vấn bảng DNS**

Việc xem xét DNS như là một hệ thống hoàn chỉnh cho thấy rằng có các cấu trúc phân cấp từ trên đỉnh (máy chủ root) xuống đến bộ đệm trong một máy riêng lẻ. Nhiễm độc DNS có thể xảy ra tại bất kỳ cấp độ nào trong số này, với tác động của sự nhiễm độc ngày càng rộng hơn khi nó xảy ra càng nhiều hơn. Năm 2010, một sự kiện nhiễm độc DNS đã dẫn đến việc “Great Firewall of China” kiểm duyệt lưu lượng truy cập Internet tại Hoa Kỳ cho đến khi các bộ nhớ đệm được giải quyết.

Nhiễm độc DNS là một biến thể của một lớp tấn công lớn hơn được gọi là *giả mạo DNS*. Trong tấn công giả mạo DNS, kẻ tấn công thay đổi một bản ghi DNS thông qua bất kỳ trong số rất nhiều phương tiện nào. Có rất

nhiều cách để tiến hành tấn công giả mạo DNS, một vài trong số đó bao gồm việc xâm phạm một máy chủ DNS, sử dụng cuộc tấn công Kaminsky và sử dụng nút mạng sai quảng cáo địa chỉ DNS sai. Kẻ tấn công thậm chí có thể sử dụng nhiễm độc bộ nhớ cache DNS để dẫn đến giả mạo DNS. Bằng cách nhiễm độc một bộ đệm DNS ngược dòng (upstream), tất cả người dùng xuôi dòng (downstream) sẽ nhận được các bản ghi DNS đã bị giả mạo.

Do tầm quan trọng của tính toàn vẹn đối với các yêu cầu và phản hồi DNS, một dự án đã bắt đầu để bảo mật cơ sở hạ tầng DNS bằng cách sử dụng chữ ký số cho các bản ghi DNS. Dự án này do chính phủ Hoa Kỳ khởi xướng và được gọi là Phần mở rộng Bảo mật Hệ thống Tên miền (Domain Name System Security Extensions - DNSSEC), hoạt động bằng cách ký kỹ thuật số vào các bản ghi. Điều này được thực hiện bằng cách bổ sung thêm các bản ghi vào DNS, một khóa và một chữ ký chứng thực tính hợp lệ của khóa. Với thông tin này, người yêu cầu có thể yên tâm rằng thông tin mà họ nhận được là chính xác. Sẽ phải mất một khoảng thời gian đáng kể (hàng năm) để hệ thống mới này phổ biến thông qua toàn bộ cơ sở hạ tầng DNS, nhưng cuối cùng, hệ thống sẽ có sự đảm bảo lớn hơn nhiều.

## **Chuyển hướng Bộ định vị Tài nguyên Toàn cầu (Universal Resource Locator – URL)**

*Bộ định vị tài nguyên toàn cầu (URL)* là phương pháp mô tả nơi mà bạn muốn trình duyệt đi đến đó, và nó là giao diện chính đối với một tiến trình DNS để chuyển đổi nó thành một địa chỉ mà máy-có-thể-đọc-được. Vì vậy, làm thế nào mà bạn có thể giả mạo điều này? Những kỹ sư xã hội sử dụng khoa học hành vi và nhận thức để lừa người dùng thực hiện những việc đó. Ví dụ, một sự khác biệt nhỏ trong tên được hiển thị trong một email hoặc một liên kết có thể bị bỏ sót trong trí não của bạn. Nếu như kẻ tấn công đã đăng ký trang khác biệt này trong DNS và đã nhân

bản trang mà bạn nghĩ là trang mà bạn đang đi đến, khi bạn nhấp chuột mà không đọc một cách cẩn thận, cuối cùng bạn sẽ đi đến một trang trông giống như trang mà bạn đang muốn đi đến. Tại sao đây lại là vấn đề? Chà, đây là một cuộc tấn công người trung gian khi tất cả lưu lượng của bạn đang được đọc và chuyển hướng – mật khẩu và tất cả mọi thứ. Vậy làm thế nào để chống lại nó? Có rất nhiều nhà cung cấp bảo mật và nhà cung cấp email đã tích hợp sẵn sự hỗ trợ tìm kiếm những khác biệt và cảnh báo một người dùng trước khi đi đến một trang web có thể có vấn đề.

### Danh tiếng Tên miền

Địa chỉ IP của bạn là một địa chỉ, giống như một địa chỉ của ngôi nhà của bạn, và giống như mọi địa chỉ khác, nó có thể có một tiếng tăm nhất định. Bạn có đang sống chung với một người hàng xóm tốt không, hay là một người xấu? Ngôi nhà của bạn có hoạt động nào khiến hàng xóm lo lắng đến mức phải gọi cho cảnh sát hoặc có các vấn đề khác không? Địa chỉ IP cũng có danh tiếng, và nếu bạn không bảo vệ địa chỉ [IP] của mình, danh tiếng của nó cũng có thể bị ảnh hưởng. Các công ty bảo mật theo dõi thư rác đến từ đâu và nếu địa chỉ IP của bạn bị liên kết với thư rác, botnet hoặc các hành vi xấu khác, *danh tiếng tên miền* của bạn sẽ bị ảnh hưởng. Ngoài ra, rất nhiều dịch vụ được kết nối với nhau sẽ ngừng hoạt động theo đúng nghĩa đen nếu điểm của bạn đủ thấp. Vì vậy, cũng giống như điểm tín dụng của bạn, bạn phải thực hiện một số hành động tích cực nhất định để duy trì điểm danh tiếng IP của mình. Nếu bạn vi phạm các quy tắc đối với API của Google hoặc API của Dịch vụ Web Amazon (AWS) hoặc một dịch vụ dựa-trên-Internet khác, đừng ngạc nhiên khi dịch vụ đó không còn khả dụng để bạn sử dụng.

Làm thế nào để bạn ngăn chặn điều này xảy ra? Hãy bắt đầu bằng việc đảm bảo một số người khác không theo dõi địa chỉ của bạn. Chuyển hướng

(relay) thư mở có thể dẫn đến việc gửi thư rác. Các bots có thể lạm dụng API. Những kẻ tấn công sử dụng các kênh này mà không quan tâm đến danh tiếng tên miền của bạn, khi nó xuống quá thấp, chúng chuyển sang nạn nhân khác. Việc duy trì một hệ thống an toàn là cách bạn ngăn điều này xảy ra.

---

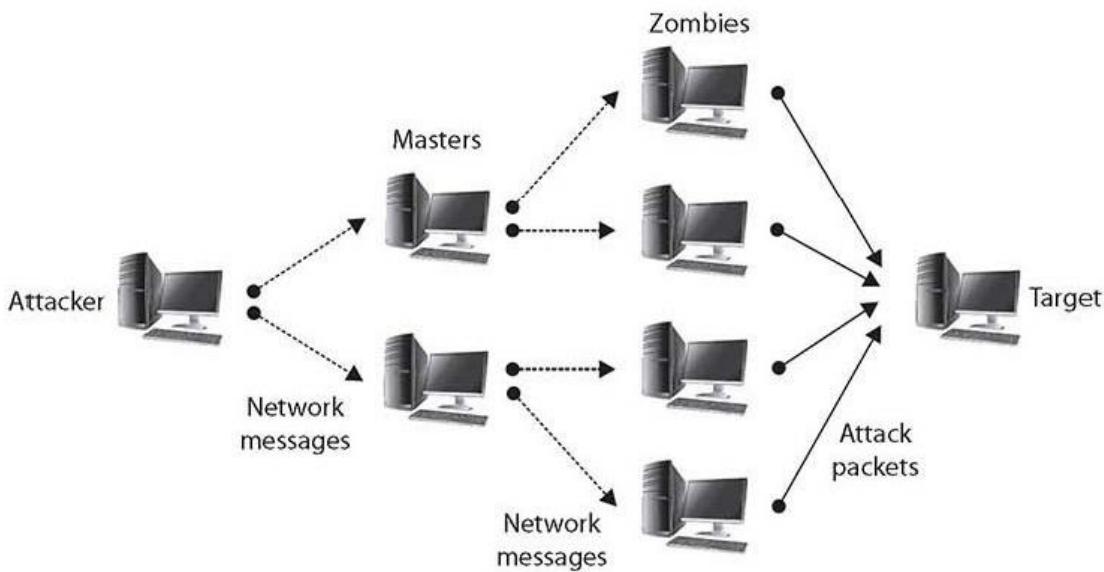


**MÁCH NƯỚC CHO KỲ THI** Các phương pháp thay đổi địa chỉ của thông điệp cho phép rất nhiều cuộc tấn công và cách thức chúng được thay đổi chính là chìa khóa. Tác động cuối cùng của mọi cuộc tấn công địa chỉ là tương tự nhau, nhưng cách mà chúng diễn ra sẽ là một phần tử của câu hỏi. Hãy xem xét các cuộc tấn công nhiễm độc DNS, chiếm đoạt tên miền, chuyển hướng URL và danh tiếng để phân biệt bằng những chi tiết nhỏ trong mô tả của câu hỏi.

### **Từ chối Dịch vụ được Phân tán (Distributed Denial-of-Service – DDoS)**

Trong một cuộc tấn công từ-chối-dịch-vụ (DoS), kẻ tấn công cố gắng từ chối quyền truy cập hợp pháp của người dùng đến những thông tin cụ thể hoặc đến một hệ thống máy tính hoặc đến chính bản thân hệ thống mạng. Điều này có thể được thực hiện bằng cách gây lỗi hệ thống - khiến cho nó ngoại tuyến – hoặc bằng cách gửi rất nhiều yêu cầu để máy bị quá tải. Một cuộc tấn công DoS sử dụng rất nhiều hệ thống tấn công còn được biết đến như là tấn công *từ-chối-dịch-vụ được phân tán (DDoS)*. Mục tiêu của một cuộc tấn công DDoS cũng là để từ chối việc sử dụng hoặc truy cập vào một hệ thống hoặc dịch vụ cụ thể. Các cuộc tấn công DDoS đã trở nên nổi tiếng trong năm 2000 với các cuộc tấn công đã được công bố rộng rãi đến eBay, CNN, Amazon và Yahoo!

Việc tạo ra một mạng DNS không hề đơn giản. Các tác nhân tấn công không phải là các tác nhân sẵn sàng — chúng là các hệ thống đã bị xâm nhập và trên đó phần mềm tấn công DDoS đã được cài đặt. Để xâm phạm các tác nhân này, kẻ tấn công phải có được quyền truy cập trái phép vào hệ thống hoặc lừa người dùng đã được ủy quyền chạy chương trình đã cài đặt phần mềm tấn công. Trên thực tế, việc tạo ra mạng tấn công có thể là một quá trình bao gồm nhiều bước, trong đó kẻ tấn công đầu tiên xâm phạm một vài hệ thống mà sau đó được sử dụng như là bộ xử lý hoặc bộ kiểm soát, và đến lượt nó sẽ xâm phạm các hệ thống khác. Khi mạng đã được tạo ra, các tác nhân (thây ma) sẽ đợi một thông điệp tấn công sẽ bao gồm dữ liệu về đích nhắm mục tiêu cụ thể trước khi phát động cuộc tấn công. Một khía cạnh quan trọng của một cuộc tấn công DDoS là chỉ với một vài tin nhắn gửi đến các tác nhân, kẻ tấn công có thể có một loạt các thông điệp được gửi đến hệ thống đã được nhắm mục tiêu. Hình 4-5 minh họa một mạng DDoS với các tác nhân và bộ xử lý.



**Hình 4-5 - Các cuộc tấn công DDoS**

Đây là cách mà mạng botnet Mirai đã tạo ra một DDoS chống lại một nhà nghiên cứu bảo mật nổi tiếng vào tháng 9 năm 2016 và sau đó là dịch vụ DNS Dyn vào tháng 10. Mạng botnet Mirai đã sử dụng hàng triệu thiết bị IoT (Internet Vạn vật - Internet of Things) đơn giản bị thiếu cơ chế bảo mật cơ bản để thực hiện việc khuếch đại cuộc tấn công.

Một phương pháp tiếp cận phòng thủ bao gồm việc thay đổi tùy chọn hết giờ cho các kết nối TCP để các cuộc tấn công như cuộc tấn công gây ngập lụt SYN trở nên khó thực hiện hơn, vì các kết nối không sử dụng sẽ bị kết thúc nhanh hơn.

Đối với các cuộc tấn công DDoS, người ta đã viết nhiều về việc phân tán khống lượng công việc của riêng bạn trên một vài hệ thống để bất kỳ cuộc tấn công nào chống lại hệ thống của bạn sẽ phải nhắm mục tiêu vào một số máy chủ để hoàn toàn thành công. Mặc dù điều này là đúng, nhưng nếu các mạng DDoS đủ lớn được tạo ra (với hàng chục nghìn thây ma chẳng hạn), thì bất kỳ mạng nào, cho dù tải trọng được phân phối đến đâu, đều có thể bị tấn công một cách thành công. Phương pháp tiếp cận như vậy cũng liên quan đến chi phí bổ sung cho tổ chức của bạn để thiết lập nên môi trường phân tán này. Việc giải quyết vấn đề theo cách này thực sự là một nỗ lực để giảm thiểu tác động của cuộc tấn công chứ không phải là ngăn chặn hoặc dừng một cuộc tấn công.

Để ngăn chặn một cuộc tấn công DDoS, bạn phải có khả năng chặn đứng hoặc ngăn chặn được những thông điệp tấn công hoặc giữ cho mạng DDoS không được thiết lập ngay từ ban đầu. Các công cụ đã được phát triển để sẽ quét qua các hệ thống của bạn, tìm kiếm các thây ma đang ngủ yên và chờ đợi tín hiệu tấn công. Rất nhiều trong số các bộ công cụ bảo mật chống vi-rút/chống-phần-mềm-độc-hại sẽ phát hiện các lây nhiễm kiểu-thây-ma đã biết. Tuy nhiên, vẫn đề với kiểu phương pháp tiếp cận ngăn

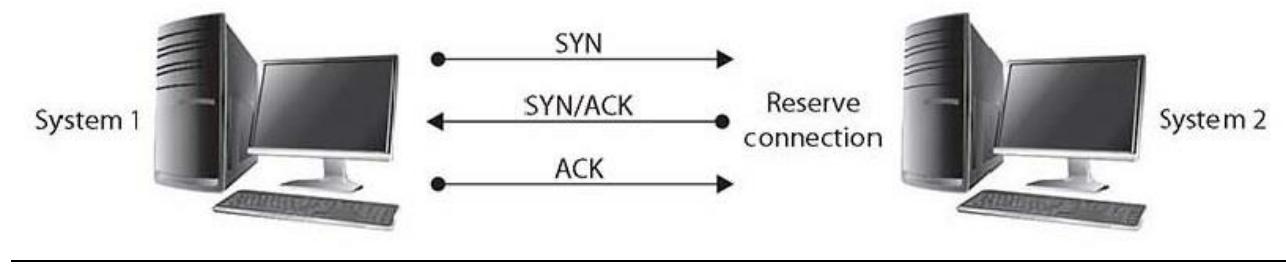
ngừa này là rằng bạn không thể làm gì để ngăn chặn một cuộc tấn công vào hệ thống mạng của mình – đó chỉ là điều mà bạn có thể thực hiện để giữ cho mạng của bạn khỏi bị sử dụng để tấn công các mạng hoặc các hệ thống khác. Bạn phải dựa vào cộng đồng các quản trị viên mạng để kiểm tra các hệ thống của riêng họ để ngăn chặn các cuộc tấn công vào hệ thống của bạn.

## Hệ thống Mạng

Trong một cuộc tấn công DDoS, dịch vụ bị từ chối bằng cách làm quá tải đích nhắm mục tiêu với lưu lượng từ rất nhiều hệ thống khác nhau. Một mạng các tác nhân tấn công (đôi khi được gọi là các thây ma) được tạo ra bởi kẻ tấn công, và khi nhận được lệnh tấn công từ kẻ tấn công, các tác nhân tấn công bắt đầu gửi một kiểu lưu lượng cụ thể chống lại mục tiêu. Nếu như mạng tấn công đủ lớn, thậm chí ngay cả lưu lượng truy cập web thông thường cũng có thể nhanh chóng làm quá tải các trang web lớn nhất, chẳng hạn như cuộc tấn công CloudFlare 400Gbps vào đầu năm 2014. Kể từ năm 2016, một kỹ thuật phản ánh mới hơn bằng cách sử dụng Giao thức Truy cập Danh bạ Hạng nhẹ Không kết nối (Connectionless Lightweight Directory Access Protocol - CLDAP) đã làm tăng khối lượng thêm nữa, với cuộc tấn công 1,35Tbps vào GitHub, cuộc tấn công 1,7Tbps đã được Abor giảm thiểu vào năm 2018 và cuộc tấn công 2,3Tbps được Amazon Web Services (AWS) giảm thiểu vào năm 2020.

Mục đích của một cuộc tấn công DDoS/DoS là ngăn chặn sự truy cập vào hệ thống mục tiêu và việc chặn các kết nối mạng sẽ thực hiện điều này. Một phương pháp, một cuộc tấn công gây ngập lụt SYN, có thể được sử dụng để ngăn chặn dịch vụ đối với một hệ thống một cách tạm thời nhằm tận dụng mối quan hệ đáng tin cậy tồn tại giữa hệ thống đó và hệ thống khác. Gây ngập lụt SYN là một ví dụ về cuộc tấn công DoS lợi dụng cách thức mà mạng TCP/IP đã được thiết kế để hoạt động và nó có thể được

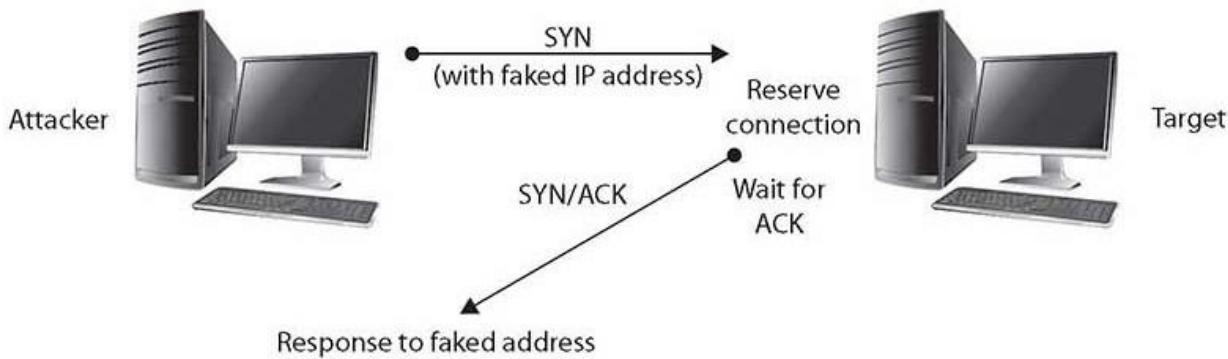
sử dụng để minh họa cho các nguyên tắc cơ bản của bất kỳ cuộc tấn công DoS nào. Gây ngập lụt SYN sử dụng bắt tay ba-chiều TCP để thiết lập kết nối giữa hai hệ thống. Trong trường hợp bình thường, hệ thống đầu tiên gửi một gói SYN đến hệ thống mà nó muốn giao tiếp. Hệ thống thứ hai phản hồi lại bằng SYN/ACK nếu nó có thể chấp nhận yêu cầu. Khi hệ thống ban đầu nhận được SYN/ACK từ hệ thống thứ hai, nó sẽ phản hồi bằng một gói ACK và sau đó giao tiếp có thể được tiến hành. Quá trình này được thể hiện trong [Hình 4-6](#).



**Hình 4-6** Bắt tay TCP/IP ba-chiều

Trong một cuộc tấn công gây ngập lụt SYN, kẻ tấn công gửi đi các yêu cầu giao tiếp giả mạo đến hệ thống được nhắm mục tiêu. Mỗi một trong số các yêu cầu này sẽ được phản hồi lại bởi hệ thống đã được nhắm mục tiêu, vốn sau đó chờ đợi phần thứ ba của tiến trình bắt tay. Vì các yêu cầu là giả mạo (một địa chỉ IP không nhất quán được sử dụng trong các yêu cầu, do đó hệ thống mục tiêu đang phản hồi lại một hệ thống không hề tồn tại), hệ thống mục tiêu sẽ đợi những phản hồi không bao giờ được gửi đến, như được minh họa trong Hình 4-7. Hệ thống mục tiêu sẽ ngắt các kết nối này sau một khoảng thời gian chờ nhất định, nhưng nếu kẻ tấn công tiếp tục gửi các yêu cầu nhanh hơn khoảng thời gian chờ để loại bỏ chúng, hệ thống sẽ nhanh chóng bị tràn ngập bởi các yêu cầu. Số lượng các kết nối mà một hệ thống có thể hỗ trợ là có giới hạn, do đó khi có nhiều yêu cầu hơn số lượng có thể được xử lý, hệ thống sẽ sớm

dành các kết nối của nó cho các yêu cầu giả mạo. Tại thời điểm này, bất kỳ yêu cầu thêm nào cũng sẽ bị ngắt (bỏ qua), và những người dùng hợp lệ muốn kết nối tới hệ thống mục tiêu sẽ không có khả năng thực hiện điều đó, bởi vì việc sử dụng hệ thống đã bị từ chối đối với họ.



**Hình 4-7** Một cuộc tấn công gây ngập lụt SYN

Một cuộc tấn công DoS đơn giản khác là ping of death (POD) khét tiếng, và nó minh họa cho một kiểu tấn công khác – một kiểu tấn công được nhắm mục tiêu đến một ứng dụng hoặc hệ điều hành cụ thể, đối ngược với tấn công gây ngập lụt SYN, vốn nhắm mục tiêu đến một giao thức. Trong cuộc tấn công POD, kẻ tấn công gửi một gói tin ping Giao thức Thông điệp Kiểm soát Internet (ICMP) bằng hoặc vượt quá 64KB (nghĩa là bằng hoặc lớn hơn  $64 \times 1.024 = 65.536$  byte). Về bản chất, kiểu gói tin này không nên xuất hiện (không có lý do gì để một gói tin ping lớn hơn 64KB). Những hệ thống nhất định không có khả năng xử lý kích cỡ gói tin này và hệ thống sẽ bị treo hoặc bị lỗi.

Như đã được đề cập trước đây, một hình thức mới hơn phản ảnh cuộc tấn công sử dụng Giao thức Truy cập Danh bạ Hạng nhẹ Không kết nối (CLDAP). Trong kiểu tấn công này, kẻ tấn công yêu cầu tất cả những thông tin của tất cả các tài khoản trong Active Directory, trả thông tin đến máy nạn nhân. Bởi vì cuộc tấn công được giả mạo để trông như có

về đến từ một người yêu cầu hợp pháp, dữ liệu được gửi đi đến máy nạn nhân. Kiểu tấn công này rõ ràng là có thể ngăn chặn được, vì yêu cầu cổng 389 UDP sẽ có một địa chỉ IP nguồn từ bên trong mạng, nhưng nó sẽ đến từ bên ngoài mạng. Việc chặn cổng này trên tường lửa gửi đến sẽ ngăn chặn cuộc tấn công này.

## Ứng dụng

Các ứng dụng cũng là đối tượng của tấn công DDoS, vì giống như tất cả các hệ thống, chúng đều nhận đầu vào của người dùng, xử lý dữ liệu và tạo kết quả đầu ra của người dùng. Hoạt động này chiếm tài nguyên và mục tiêu của cuộc tấn công DDoS ở cấp ứng dụng là tiêu tốn tất cả tài nguyên hoặc đưa hệ thống vào trạng thái bị lỗi. Một trong những đích nhắm mục tiêu phổ biến nhất của cuộc tấn công lớp ứng dụng là HTTP. Do bản chất của giao thức và vì những người yêu cầu ứng dụng thường nằm bên ngoài mạng cục bộ, các gói không bị giả mạo và việc phát hiện các gói tin tấn công so với các gói tin hợp pháp thực sự là một thách thức. Tường lửa ứng dụng web thế-hệ-tiếp-theo nâng cao có một số khả năng phục hồi được tích hợp sẵn để phát hiện ra kiểu tấn công này, nhưng trong những trường hợp nghiêm trọng, vấn đề của DoS chỉ được chuyển sang tường lửa.

Các kiểu tấn công này cũng hoạt động để chống lại các giao diện API. Các nguyên tắc cơ bản đằng sau cuộc tấn công xuất phát từ sự chênh lệch giữa mức tài nguyên mà nó cần để tấn công so với mức tài nguyên cần thiết để giảm thiểu hành động này. Vì tài nguyên bị tấn công thường là năng lực xử lý nên đây không phải là kiểu tấn công băng thông. Để kiểm tra điều này, hãy xem xét các tài nguyên để đăng nhập vào tài khoản trực tuyến, chẳng hạn như GMail. Khi kẻ tấn công gửi yêu cầu đăng nhập vào tài khoản, lượng dữ liệu và tài nguyên mà máy tính của kẻ tấn công phải xử lý là tối thiểu. Công việc trên máy chủ không tương xứng

với điều này, vì nó phải kiểm tra thông tin đăng nhập, mở phiên, tải bất kỳ dữ liệu người dùng có liên quan nào từ cơ sở dữ liệu, sau đó gửi lại phản hồi có chứa trang web được yêu cầu. Sự chênh lệch giữa công việc của kẻ tấn công và khối lượng công việc của nạn nhân là điều dẫn đến việc thực hiện cuộc tấn công này thành công.

### Công nghệ Vận hành (Operational Technology – OT)

*Công nghệ hoạt động (OT)* là tên gọi được đặt cho các mạng thiết bị công nghiệp trong các hệ thống mạng-vật-lý. Các thiết bị này sử dụng máy tính để điều khiển các tiến trình vật lý - từ đèn giao thông, đến nhà máy lọc dầu, nhà máy sản xuất, v.v... Thực sự có hàng nghìn các quy trình công nghiệp khác nhau được đặt dưới sự điều khiển của máy tính. Một điểm khác biệt lớn giữa OT và hệ thống CNTT là các giao thức. Các hệ thống OT có các giao thức dành riêng cho OT được sử dụng để thực hiện các giao tiếp điều khiển thiết bị. Một trong những đặc điểm hệ thống của những tiến trình này là sự phụ thuộc vào các tín hiệu được hẹn giờ thích hợp. Các hệ thống này sẽ không hoạt động một cách chính xác khi thông tin liên lạc bị gián đoạn, do đó, các cuộc tấn công DoS dưới bất kỳ hình thức nào, bao gồm cả DDoS, đều có thể dẫn đến các vấn đề nghiêm trọng. Vì những lý do này và hơn thế nữa, các hệ thống OT không được kết nối trực tiếp với Internet và có những rào cản đáng kể ngăn các gói tin bên ngoài xâm nhập vào các mạng này.



**MÁCH NƯỚC CHO KỲ THI** Các cuộc tấn công từ-chối-dịch-vụ được sử dụng như một phần của một bộ công cụ tấn công. Những cuộc tấn công này có thể là tạm thời chống lại một dịch vụ như DNS hoặc các thành phần khác của một cơ sở hạ tầng. Chúng không chỉ là các sự kiện "ngừng mọi thứ". Chúng có thể được sử dụng như một phần của một chiến

lực tấn công, do đó, hãy tìm hiểu cách thức mà chúng tương tác với các bộ phận khác của doanh nghiệp của bạn: mạng, ứng dụng, và các hệ thống.

### **Thực thi Tập lệnh và Mã Phần mềm độc hại**

Có rất nhiều nguyên nhân để sử dụng các tập lệnh và tự động hóa trong các hệ thống: chúng thúc đẩy tốc độ, độ chính xác, khả năng tái tạo và tính linh hoạt cũng như mang lại một loạt các ưu điểm khác. Rất nhiều trong số những nguyên nhân này chính là lý do tại sao những kẻ tấn công cũng sử dụng chúng. Trong môi trường ngày nay, *Mã phần mềm độc hại* và *thực thi tập lệnh* là những mối đe dọa thực sự. Những kẻ tấn công có một loạt các công nghệ để lựa chọn khi tự động hóa các cuộc tấn công của chúng – PowerShell, Python, Bash, macro, và thậm chí Visual Basic dành cho các Ứng dụng là một số véc-tơ cần phải được bảo vệ để chống lại chúng.

#### **PowerShell**

*PowerShell* là một bộ công cụ dòng-lệnh được tích hợp sẵn và bao gồm một loạt các dòng lệnh phong phú của Microsoft Windows. PowerShell được tích hợp một cách hoàn chỉnh với môi trường Windows, cho phép các quản trị viên lập trình hầu như bất kỳ chức năng nào có thể được thực hiện trong Hệ điều hành. Đây là lý do vì sao những kẻ tấn công rất thích PowerShell – nó có sẵn ở đó, đã được kích hoạt, mạnh mẽ, và không bị giám sát bởi hầu hết các hệ thống bảo mật. Một loạt các bộ công cụ đã được xây dựng để tận dụng sức mạnh của PowerShell có thể được sử dụng để tấn công một hệ thống. Một công cụ được sử dụng rất phổ biến là PowerSploit, bao gồm các thủ tục như Invoke-Mimikatz.

#### **Python**

*Python* là một ngôn ngữ tập lệnh/ngôn ngữ lập trình được sử dụng một cách rộng rãi. Python là một công cụ tập lệnh hiệu quả dễ học, được hỗ

trợ rộng rãi, và thích hợp cho các tác vụ tự động hóa và phân tích dữ liệu. Điều này khiến cho nó trở nên rất hữu ích cho các nhóm an ninh mạng cũng như với những kẻ tấn công. Tin tặc sử dụng Python cho các lý do giống nhau, và trên GitHub có rất nhiều thư viện bao gồm các công cụ và tiện ích tấn công theo-hướng-Python.

## Bash

*Bash* (hay là Bourne Again Shell) là một trình biên dịch để xử lý các câu lệnh Shell trên các hệ thống Linux. Bash giữ các câu lệnh dưới dạng văn bản thô và gọi các dịch vụ của Hệ điều hành để thực hiện các tác vụ được chỉ định. Điều này cho phép tự động hóa hoàn toàn của một môi trường Linux và do đó, nó rất có giá trị đối với các quản trị viên cũng như với những kẻ tấn công. Một trong số những sức mạnh của Linux là dễ dàng lập trình những tập lệnh phức tạp để tự động hóa những thay đổi hệ thống quan trọng và xử lý dữ liệu. Tin tặc sử dụng Bash để tìm kiếm trên các hệ thống và thực hiện các tác vụ trên các hệ thống Linux.



## MÁCH NƯỚC CHO KỲ THI

Việc phân biệt giữa PowerShell, Python và Bash chủ yếu dựa vào các dòng hệ điều hành. PowerShell được sử dụng cho Windows, Bash được sử dụng cho Linux và Python có thể được sử dụng cho cả hai.

## Macro

Các *macro* là các tập hợp các chỉ lệnh được ghi lại, thường được trình bày cho một ứng dụng để tự động hóa chức năng của chúng. Thuật ngữ *macro* được sử dụng cho các ứng dụng tập lệnh. Hầu như mọi máy tính để bàn đều có chức năng PDF hoặc chức năng Microsoft Office, và việc sử dụng các macro trong những sản phẩm này cho phép rất nhiều chức năng. Tuy nhiên, cùng với chức năng này là những rủi ro dưới hình thức

các macro không mong muốn và thực hiện các hoạt động của hệ thống. Vì lý do này, việc hạn chế các macro trong các ứng dụng này và các ứng dụng khác là một phần quan trọng của việc quản lý an ninh mạng của một máy trạm.

### **Visual Basic dành cho Ứng dụng (VBA)**

*Visual Basic dành cho Ứng dụng (VBA)* là một công nghệ cũ hơn từ Microsoft đã từng được sử dụng để tự động hóa rất nhiều tiến trình nội bộ trong các ứng dụng. Đây là một hình thức cũ hơn của macro có năng lực lập trình đáng kể nhưng hầu như không được ưa chuộng. Tuy nhiên, nó vẫn có hiệu lực trên nhiều nền tảng và do vậy, vẫn là một véc-tơ cho những kẻ tấn công. Do đó, bạn nên bảo vệ các hệ thống khỏi bị tấn công bằng cách vô hiệu hóa các macro hoặc VBA chạy trong các ứng dụng trừ khi bạn chắc chắn rằng nguồn gốc của tài liệu có chứa mã [phần mềm] là có thể đáng tin cậy.



### **MÁCH NƯỚC CHO KỲ THI**

Các macro và VBA có vị trí của chúng trong doanh nghiệp, vì đây là cách mà các ứng dụng được tự động hóa. Tuy nhiên, chúng nên được hạn chế chỉ cho những nguồn đáng tin cậy.

## Tóm tắt Chương

Trong chương này, bạn đã tìm hiểu về những chỉ báo tấn công tiềm năng tương ứng với các cuộc tấn công vào hệ thống mạng. Chương bắt đầu với các cuộc tấn công [mạng] không dây, bao gồm các cuộc tấn công quý song sinh, điểm truy cập giả mạo, bluesnarfing và bluejacking, hủy kết nối, jamming, RFID, NFC và IV. Tiếp theo là tấn công kiểu người trung gian và người trong trình duyệt cũng được thảo luận. Phần kế tiếp xem xét các cuộc tấn công định địa chỉ mạng, với các cuộc tấn công lớp 2 như nhiễm độc ARP, gây ngập lụt MAC và nhân bản MAC. Các cuộc tấn công DNS tiếp nối, bao gồm các cuộc tấn công chiếm đoạt tên miền, nhiễm độc DNS, chuyển hướng URL, và danh tiếng tên miền.

Các cuộc tấn công từ-chối-dịch-vụ được kiểm tra đối với ba kiểu dịch vụ khác nhau: mạng, ứng dụng và các hệ thống OT. Chương này kết thúc với một xem xét về mã phần mềm độc hại và thực thi tập lệnh từ PowerShell, Python, Bash, macro và Visual Basic dành cho Ứng dụng.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Một người dùng báo cáo rằng những cảnh báo chứng nhận "kỳ quặc" xuất hiện trên trình duyệt của cô vào sáng nay mỗi khi cô mở trang Google. Khi xem xét trình duyệt của cô ấy, bạn trông thấy những cảnh báo chứng nhận đó. Khi xem xét lưu lượng mạng, bạn nhận ra rằng mọi yêu cầu HTTP và HTTPS từ hệ thống đó đang được định tuyến đến cùng một địa chỉ IP bất kể đích đến. Trong trường hợp này, bạn đang nhìn thấy những kiểu tấn công nào dưới đây?

  - A. Quỷ song sinh
  - B. Người trung gian
  - C. Hủy kết nối
  - D. Nhân bản MAC.
2. Người dùng đang báo cáo rằng mạng không dây trên một phía của tòa nhà đang bị lỗi. Họ có thể kết nối nhưng không thể truy cập được Internet. Khi tiến hành điều tra, bạn nhận thấy tất cả những người dùng bị ảnh hưởng đang kết nối tới một điểm truy cập mà bạn không nhận ra được. Những người dùng này là nạn nhân của kiểu tấn công nào?

  - A. AP giả mạo
  - B. WPS
  - C. Bluejacking
  - D. Hủy kết nối.
3. Bạn đang ngồi tại sân bay khi một người bạn của bạn nhận được tin nhắn trên điện thoại của cô ấy. Trong tin nhắn là một hình

ảnh của một con vịt với từ “Pwnd” như lời chú thích. Bạn của bạn không biết ai đã gửi tin nhắn đó. Bạn của bạn đang là nạn nhân của kiểu tấn công nào?

- A. Snarfing**
  - B. Bluejacking**
  - C. Quacking**
  - D. Collision.**
4. Tất cả người dùng mạng không dây tại tầng ba của tòa nhà của bạn đang báo cáo về những sự cố với mạng. Cứ mỗi 15 phút, thiết bị của họ bị ngắt kết nối khỏi mạng. Trong 1 phút hoặc hơn, họ lại có khả năng kết nối trở lại. Kiểu tấn công nào có khả năng xảy ra nhất trong tình huống này?
- A. Quỷ song sinh**
  - B. Jamming**
  - C. Chiếm đoạt tên miền**
  - D. Hủy kết nối.**
5. Trang thương mại điện tử của bạn đang bị lỗi vì một lượng lớn lưu lượng cực kỳ cao. Khi xem xét nhật ký lưu lượng, bạn nhìn thấy 10.000 yêu cầu cho cùng một URL đến từ hàng trăm địa chỉ IP khác nhau trên toàn cầu. Bạn đang phải đổi mặt với kiểu tấn công nào?
- A. Chiếm đoạt tên miền**
  - B. DDoS**
  - C. Nhiễm độc DNS**
  - D. Chuyển hướng URL.**
6. Một người dùng muốn biết rằng nếu như mạng có đang gặp vấn đề hay không bởi vì cô không thể kết nối đến bất cứ gì. Khi khắc phục sự cố, bạn nhận thấy địa chỉ MAC của cửa ngõ mặc định của cô ấy không khớp với địa chỉ MAC của bộ định tuyến của tổ chức

của bạn. Kiểu tấn công nào đã được sử dụng để tấn công người dùng này?

- A.** Nhân bản MAC
  - B.** Nhiễm độc ARP
  - C.** Hủy kết nối
  - D.** Điểm truy cập giả mạo.
- 7.** Bạn có một phiếu hỗ trợ dịch vụ từ một hệ thống đang hoạt động một cách bất thường. Khi xem xét hệ thống từ xa, bạn nhận thấy địa chỉ sau trong bộ nhớ đệm của trình duyệt: [www.micros0ft.com/office](http://www.micros0ft.com/office). Bạn đang nhìn thấy kiểu tấn công nào:
- A.** PowerShell
  - B.** Chiếm đoạt tên miền
  - C.** Chuyển hướng URL
  - D.** Hủy kết nối.
- 8.** Bạn nhìn thấy một loạt các tập tin PDF đang tràn ngập hộp thư đến của mọi người với tiêu đề như "Tỷ suất Thuế Mới năm 2021". Véc-tơ tấn công nào có nhiều khả năng nhất đang được sử dụng?
- A.** Python
  - B.** Macro
  - C.** Người trung gian
  - D.** DDoS.
- 9.** Khi bạn cập nhật trình duyệt của mình, bạn nhận được một cảnh báo về một plugin không tương thích với phiên bản mới. Bạn không nhận ra được plugin và bạn không chắc chắn lầm về việc nó đang làm gì. Tại sao điều quan trọng là phải hiểu về các plugin? Và véc-tơ tấn công nào có thể liên quan đến các plugin?
- A.** Tấn công người trung gian
  - B.** Tấn công chiếm đoạt tên miền
  - C.** Tấn công người trong trình duyệt

**D.** Tấn công chuyển hướng URL.

- 10.** Kết quả quét mạng của bạn đang cho thấy một lượng lớn những thay đổi địa chỉ trong các bảng MAC và rất nhiều thông điệp ARP và RARP. Điều gì đang diễn ra?
- A.** Tấn công gây ngập lụt MAC
  - B.** Tấn công hủy kết nối
  - C.** Tấn công jamming
  - D.** Nhiễm độc DNS.

## Đáp án

1. **B.** Đây rất có thể là cuộc tấn công người trung gian. Phương pháp tấn công này thường được thực hiện bằng cách định tuyến tất cả các lưu lượng của nạn nhân đến máy chủ của kẻ tấn công, nơi kẻ tấn công có thể xem xét nó, điều chỉnh nó, hoặc ngăn chặn nó. Kẻ tấn công chèn chính bản thân mình vào giữa các giao tiếp mạng của nạn nhân của hắn.
2. **A.** Đây là một cuộc tấn công AP giả mạo. Những kẻ tấn công thiết lập các điểm truy cập riêng của chúng để nỗ lực khiến cho các thiết bị không dây kết nối vào AP giả mạo thay vì các điểm truy cập đã được cấp phép.
3. **B.** Đây có nhiều khả năng là một cuộc tấn công bluejacking. Nếu như điện thoại của một nạn nhân có Bluetooth được bật và đang trong chế độ có thể phát hiện được thì có khả năng là một kẻ tấn công gửi các tin nhắn, hình ảnh hoặc âm thanh không mong muốn đến điện thoại của nạn nhân.
4. **D.** Các cuộc tấn công hủy kết nối chống lại một hệ thống không dây là những cuộc tấn công được thiết kế để ngắt kết nối một máy vật chủ khỏi điểm truy cập không dây và khỏi mạng không dây. Nếu như kẻ tấn công có một danh sách các địa chỉ MAC cho các thiết bị không dây, chúng có thể giả mạo các khuôn khổ hủy xác thực, khiến cho các thiết bị không dây ngắt kết nối ra khỏi mạng.
5. **B.** Đây là một cuộc tấn công DDoS. Các cuộc tấn công DDoS (hoặc từ-chối-dịch-vụ được phân tán) cố gắng làm quá tải mục tiêu của chúng bằng lưu lượng từ rất nhiều nguồn khác nhau. Các botnet được sử dụng một cách khá phổ biến để khởi đầu các cuộc tấn công DDoS.
6. **B.** Nhiễm độc ARP là một cuộc tấn công liên quan đến việc gửi đi các phản hồi ARP hoặc RARP bị giả mạo cho một nạn nhân để cố

gắng thay thế bảng ARP trên hệ thống của nạn nhân. Nếu thành công, một cuộc tấn công nhiễm độc ARP sẽ thay thế một hoặc nhiều địa chỉ ARP trong bảng ARP của nạn nhân bằng địa chỉ mà kẻ tấn công cung cấp trong những phản hồi đã bị giả mạo của chúng.

7. **C.** Đây là [cuộc tấn công] chuyển hướng URL, vì tên gọi của Microsoft không có ký tự số 0 tại vị trí của ký tự 0.
8. **B.** Các tập tin PDF có khả năng macro và có thể thực thi các đoạn mã cơ bản khác nhau nếu được chấp thuận.
9. **C.** Các cuộc tấn công người trong trình duyệt thường được tiến hành thông qua các tiện ích mở rộng hoặc plugin của trình duyệt.
10. **A.** Đây là một cuộc tấn công gây ngập lụt MAC – một nỗ lực để gây tràn các bảng MAC trong các bộ định tuyến.

## Chương 5      Các Tác nhân, Véc-tơ và Nguồn Tình báo về Mối đe dọa

---

### Các Tác nhân, các Véc-tơ và Nguồn Tình báo về Mối đe dọa

Trong chương này, bạn sẽ

- Khám phá các kiểu khác nhau của các tác nhân đe dọa và những thuộc tính của chúng,
  - Xem xét các véc-tơ đe dọa khác nhau và có khả năng phân biệt chúng,
  - Giải nghĩa được các nguồn tình báo khác nhau và các nguồn nghiên cứu tương ứng.
- 

Các mối đe dọa là những hành động có thể mang lại rủi ro cho một hệ thống. Một tác nhân đe dọa là nguồn của mối đe dọa đối với hệ thống. Các véc-tơ là những phương pháp mà các tác nhân đe dọa sử dụng để tấn công một lỗ hổng trong một hệ thống nhằm đạt được mục tiêu của chúng. Nguồn tình báo về mối đe dọa là những kiến thức dựa trên bằng chứng cho phép bạn ngăn chặn hoặc giảm thiểu các mối đe dọa mạng.

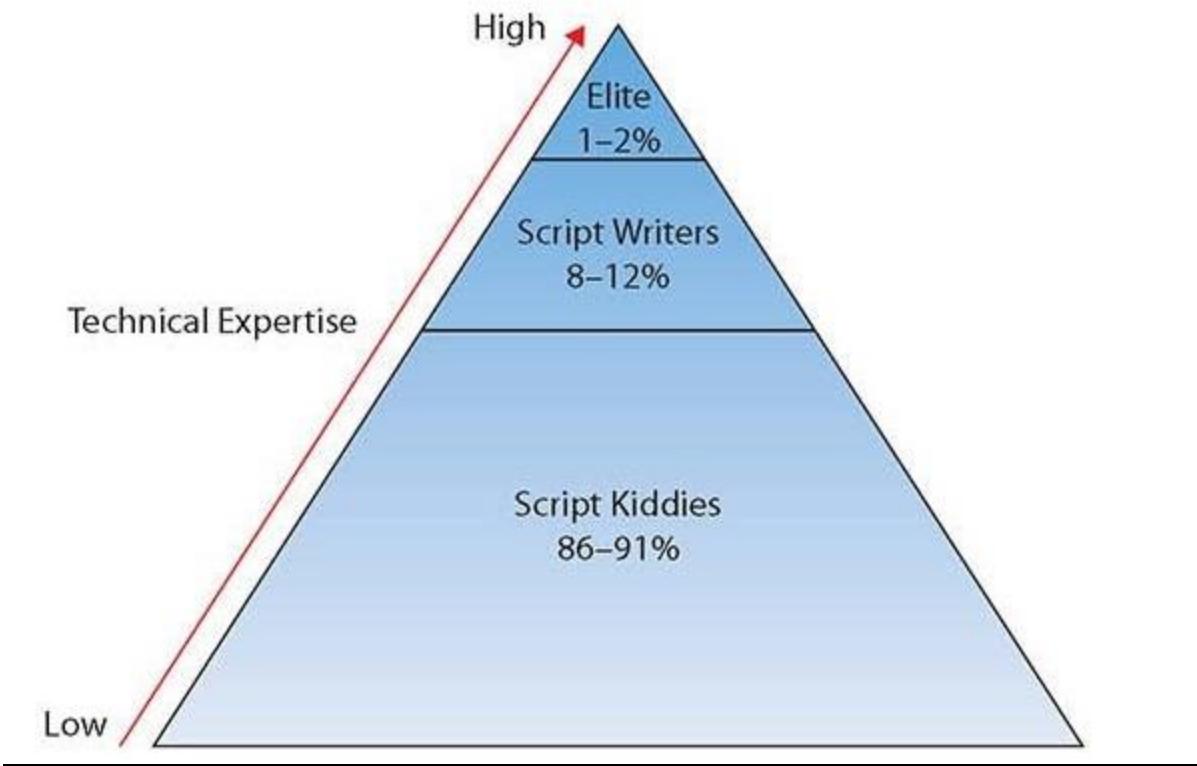
#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 1.5 của kỳ thi CompTIA Security+: Giải nghĩa sự khác biệt giữa các tác nhân, véc-tơ và nguồn tin tình báo về mối đe dọa.

## Các Tác nhân và Mối đe dọa

Hành động truy cập một cách cố ý vào hệ thống máy tính và mạng mà không được phép thường được gọi là *truy nhập trái phép* (*hacking*), với những cá nhân thực hiện hoạt động này được gọi là *tin tặc*. Thuật ngữ *hacking* cũng áp dụng cho hành vi vượt quá thẩm quyền của một người trong hệ thống. Điều này cũng sẽ bao gồm những người dùng đã được cấp phép cố gắng giành quyền truy cập vào các tập tin mà họ không được phép truy cập hoặc những người cố gắng chiếm lấy các quyền mà họ chưa được cấp. Mặc dù hành động đột nhập vào hệ thống máy tính và mạng đã được ca tụng trên các phương tiện truyền thông và phim ảnh nhưng hành động này không phù hợp với sự cường điệu của Hollywood. Những kẻ xâm nhập, nếu không có gì khác, cực kỳ kiên nhẫn, vì quá trình giành quyền truy cập vào một hệ thống đòi hỏi sự kiên trì và quyết tâm rất cao. Kẻ tấn công sẽ tiến hành nhiều hoạt động trước khi tiến hành tấn công nhằm thu thập được những thông tin cần thiết để xác định cuộc tấn công nào có khả năng thành công nhất. Thông thường, vào thời điểm một cuộc tấn công được phát động, kẻ tấn công sẽ thu thập đủ thông tin để rất tự tin rằng cuộc tấn công sẽ thành công.

Nói chung, các cuộc tấn công bởi một cá nhân hoặc thậm chí một nhóm nhỏ những kẻ tấn công thuộc thể loại *mối đe dọa không có cấu trúc*. Các cuộc tấn công ở cấp độ này nói chung thường được tiến hành trong thời gian ngắn (kéo dài nhiều nhất là vài tháng), không liên quan đến một số lượng lớn các cá nhân, ít được hỗ trợ về mặt tài chính và được thực hiện bởi những người trong cuộc hoặc những người bên ngoài không tìm kiếm sự thông đồng với những người trong cuộc. Những kẻ xâm nhập, hoặc những người đang cố gắng thực hiện một cuộc xâm nhập, chắc chắn thuộc nhiều loại khác nhau và có mức độ tinh vi khác nhau (xem [Hình 5-1](#)).



**Hình 5-1 Sự phân tán của những cấp độ kỹ năng của kẻ tấn công**



**LƯU Ý** [Hình 5-1](#) sẽ được tham chiếu trong toàn bộ chương này khi chúng ta thảo luận về các cấp độ kỹ năng khác nhau của những tin tặc.



**MÁCH NƯỚC CHO KỲ THI** Hãy chuẩn bị cho những câu hỏi yêu cầu bạn xác định những điểm khác biệt giữa các kiểu tác nhân đe dọa, bao gồm những tác nhân đã được liệt kê trong những phần sau của chương.

## Các Mối đe dọa Dai dẳng được Tăng cường (APT)

Một bước tiến lớn trong các cuộc tấn công mạng là sự phát triển của các *mối đe dọa dai dẳng được tăng cường* (APT). Một cuộc tấn công APT có đặc trưng bởi việc sử dụng các bộ công cụ để đạt được sự hiện diện trên hệ thống mạng được nhắm mục tiêu và sau đó, thay vì chỉ di chuyển để đánh cắp thông tin, chúng tập trung vào trò chơi dài hơi bằng cách duy trì sự hiện diện liên tục trên hệ thống mạng mục tiêu. Các chiến thuật, công cụ và thủ tục của các APT tập trung vào việc duy trì quyền truy cập với đặc quyền quản trị vào hệ thống mạng mục tiêu và tránh bị phát hiện. Sau đó, trong một thời gian dài, kẻ tấn công có thể xóa bỏ tài sản trí tuệ và nhiều thứ khác khỏi tổ chức mà thường không bị phát hiện.

Chiến dịch Rồng Đêm (Night Dragon) là tên gọi được đặt cho một cuộc tấn công sở hữu trí tuệ được thực hiện nhằm vào các công ty dầu, khí đốt và hóa dầu tại Hoa Kỳ vào năm 2006. Bằng cách sử dụng một tập hợp bao gồm các máy chủ trên toàn cầu, những kẻ tấn công từ Trung Quốc đã tấn công các công ty năng lượng toàn cầu để chiếm đoạt những thông tin độc quyền và có tính bảo mật cao như dữ liệu đấu thầu cho các hợp đồng thuê. Cuộc tấn công đã làm sáng tỏ những gì cấu thành nên dữ liệu tối quan trọng và các rủi ro tương ứng. Hơn nữa, như đã được chứng minh qua các cuộc tấn công của Stuxnet nhằm vào các nhà máy uranium của Iran, các cuộc tấn công mạng ở Estonia và các cuộc tấn công vào hệ thống phân phối điện ở Ukraine, nguy cơ các cuộc tấn công giữa-cá-quốc-gia là có thật. Đã có rất nhiều cáo buộc về hành vi trộm cắp tài sản trí tuệ được tài trợ bởi, và trong một số trường hợp, thậm chí được thực hiện bởi các tổ chức quốc-gia-nhà-nước. Trong một thế giới mà thông tin chi phối chính phủ, doanh nghiệp và các nền kinh tế, việc thu thập thông tin chính là chìa khóa thành công và với phần thưởng lớn, danh sách những nhân vật sẵn sàng chi tiêu những nguồn lực đáng kể sẽ rất nhiều.

## Các Mối đe dọa từ Bên trong

Các chuyên gia bảo mật nói chung thường thừa nhận rằng *những người trong nội bộ* nguy hiểm hơn ở nhiều khía cạnh so với những kẻ xâm nhập từ bên ngoài. Lý do cho điều này rất đơn giản: những người trong nội bộ có được quyền truy cập và những kiến thức cần thiết để gây ra thiệt hại ngay lập tức cho một tổ chức. Hầu hết các thành phần bảo mật được thiết kế để bảo vệ nhằm chống lại những kẻ xâm nhập từ bên ngoài và do đó nằm ở ranh giới giữa tổ chức và phần còn lại của thế giới. Những người trong nội bộ thực sự có thể đã có tất cả quyền truy cập mà họ cần để thực hiện những hoạt động tội phạm như gian lận. Ngoài khả năng truy cập chưa từng có tiền lệ, những người trong nội bộ cũng thường có kiến thức về hệ thống an ninh tại chỗ của tổ chức và có khả năng tránh bị phát hiện tốt hơn. Các cuộc tấn công bởi những người trong nội bộ thường là kết quả từ những nhân viên đã trở nên bất mãn với tổ chức của họ và đang tìm cách để phá vỡ hoạt động của tổ chức. Cũng có khả năng một "cuộc tấn công" bởi một người trong nội bộ có thể là một tai nạn và hoàn toàn không phải là một cuộc tấn công. Ví dụ về điều này có thể là việc một nhân viên xóa mất một tập tin quan trọng mà không hiểu được bản chất quan trọng của nó.



## MÁCH NƯỚC CHO KỲ THI

Một trong những mối đe dọa khó khăn nhất mà các chuyên gia bảo mật phải giải quyết là những người trong nội bộ. Vì nhân viên thực sự đã có quyền truy cập vào tổ chức và những tài sản của tổ chức, các cơ chế bổ sung cần phải được sử dụng để phát hiện ra những cuộc tấn công bởi những người trong nội bộ và làm giảm bớt khả năng thành công của những cuộc tấn công đó.

Nhân viên không phải là những người trong nội bộ duy nhất mà tổ chức cần phải quan tâm. Thông thường, một số những cá nhân khác có quyền truy cập về mặt vật lý vào những cơ sở vật chất của công ty. Các đội giám sát thường có quyền truy cập không được giám sát vào trong toàn bộ cơ sở chất, thường là khi không có ai khác ở xung quanh. Các cá nhân khác, chẳng hạn như các nhà thầu hoặc đối tác, có thể không chỉ có quyền truy cập thực tế vào các cơ sở của tổ chức mà còn có cả quyền truy cập vào hệ thống máy tính và mạng. Một nhà thầu tham gia vào lĩnh vực điện toán tình báo của Hoa Kỳ, Edward Snowden, đã bị cáo buộc tội danh gián điệp vào năm 2013 sau khi anh ta công bố một loạt dữ liệu minh chứng cho năng lực kỹ thuật của hệ thống giám sát tình báo của Hoa Kỳ. Anh ta là nội gián cuối cùng, và tên gọi của anh ta đã trở thành từ đồng nghĩa với vấn đề đe dọa nội gián.



**LƯU Ý** Một trong những cách để bảo vệ chống lại một tin tặc lành nghề là ngăn chặn bất kỳ cá nhân nào thực hiện những nhiệm vụ tối quan trọng một mình. Phương pháp để thực hiện việc này là thông qua phân tách nhiệm vụ (seperation of duties), một chính sách mà theo đó, các chức năng tối quan trọng đòi hỏi nhiều hơn một cá nhân để có tác động đến những thay đổi.

### Các Tác nhân Nhà nước

Ở phần trên cùng của dải phổ được thể hiện trong [Hình 5-1](#) là những cá nhân có kỹ thuật cao, thường được gọi là những *tin tặc ưu tú (elite hacker)*, những người không chỉ có khả năng viết các đoạn mã khai thác các lỗ hổng mà còn có khả năng phát hiện ra các lỗ hổng mới. Tuy nhiên, nhóm này là nhóm nhỏ nhất trong dải phổ và chịu trách nhiệm nhiều nhất, chỉ từ 1 đến 2% cho những hoạt động xâm nhập. Rất nhiều trong số

những tin tặc ưu tú này đã được tuyển dụng bởi các công ty an ninh mạng lớn trong những nỗ lực chống lại các hoạt động tội phạm. Những người khác được tuyển dụng bởi các quốc-gia và các tổ chức quốc tế khác, để đào tạo và điều hành các nhóm lớn tin tặc có tay nghề cao để tiến hành các cuộc tấn công quốc gia chống lại nhiều đối thủ. Tại Hoa Kỳ, các quy tắc và luật lệ của chính phủ ngăn cản việc nhân viên chính phủ tấn công các công ty vì lý do chiến tranh kinh tế. Không phải tất cả các quốc gia đều tuân theo nguyên tắc này và rất nhiều quốc gia đã thu xếp những nỗ lực lấy cắp dữ liệu nhằm thu thập thông tin từ các công ty quốc tế, đánh cắp tài sản trí tuệ với mục đích rõ ràng là thúc đẩy các công ty quốc gia của chính quốc gia của họ.



**MÁCH NƯỚC CHO KỲ THI** Các tác nhân nhà nước được sử dụng bởi các chính phủ để xâm phạm hoặc có được quyền truy cập vào dữ liệu tình báo về các chính phủ đã được nhắm mục tiêu. Chúng thường được tài trợ vốn và thường tiến hành các cuộc tấn công APT.

Khi các quốc gia ngày càng trở nên phụ thuộc hơn vào hệ thống máy tính và hệ thống mạng, khả năng các thành phần thiết yếu của xã hội có thể bị nhắm mục tiêu bởi các tổ chức hoặc các quốc gia khác đã được xác định là có ảnh hưởng xấu đến chúng đã trở thành hiện thực. Ngày nay, rất nhiều quốc gia đã phát triển, ở một mức độ nào đó, khả năng tiến hành *chiến tranh thông tin*. Có một vài định nghĩa về chiến tranh thông tin, nhưng một định nghĩa đơn giản là đây là cuộc chiến tranh được tiến hành chống lại thông tin và những thiết bị xử-lý-thông-tin được sử dụng bởi đối phương. Trên thực tế, đây là một chủ đề phức tạp hơn nhiều, bởi vì thông tin không chỉ có thể trở thành mục tiêu của kẻ thù mà còn có thể được sử dụng như một loại vũ khí. Bất kể bạn sử dụng định nghĩa

nào, chiến tranh thông tin đều thuộc loại *mối đe dọa có cấu trúc cao*. Kiểu mối đe dọa này có đặc trưng là thời gian chuẩn bị lâu hơn nhiều (hàng năm không phải là hiếm), sự hậu thuẫn tài chính to lớn và một nhóm lớn những kẻ tấn công có tổ chức. Mỗi đe dọa có thể bao gồm các nỗ lực không chỉ để lật đổ những người trong cuộc mà còn để đưa các cá nhân vào bên trong một mục tiêu tiềm năng trước một cuộc tấn công đã được lên kế hoạch.

Một khía cạnh thú vị của chiến tranh thông tin là danh sách các mục tiêu khả dĩ. Chúng ta đã quen với ý tưởng rằng, trong chiến tranh, các lực lượng quân sự sẽ nhắm mục tiêu vào các lực lượng quân sự đối lập nhưng nhìn chung sẽ cố gắng phá hủy càng ít cơ sở hạ tầng dân sự càng tốt. Trong chiến tranh thông tin, các lực lượng quân sự chắc chắn vẫn là mục tiêu hàng đầu, nhưng người ta đã viết nhiều về các mục tiêu khác, chẳng hạn như các cơ sở hạ tầng khác nhau mà một quốc gia dựa vào để tồn tại hàng ngày. Các nhà máy lọc và phân phôi nước, điện, dầu khí, tài chính và ngân hàng, viễn thông đều thuộc nhóm cơ sở hạ tầng trọng yếu của một quốc gia. Cơ sở hạ tầng trọng yếu là những cơ sở mà sự tổn thất sẽ để lại hậu quả nặng nề cho quốc gia. Cùng với việc các quốc gia đang phụ thuộc quá nhiều vào các cơ sở hạ tầng này, việc chúng (*các cơ sở hạ tầng trọng yếu – người dịch*) bị coi là mục tiêu hợp lệ trong xung đột là điều không thể tránh khỏi. Với mức độ phụ thuộc của các cơ sở hạ tầng này vào các hệ thống máy tính và mạng, cũng không thể tránh khỏi việc các hệ thống và mạng máy tính tương tự này sẽ là mục tiêu tấn công mạng trong một cuộc chiến tranh thông tin.

## **Hacktivists**

Như đã được minh họa trong [Hình 5-1](#), ở cấp độ tiếp theo bên dưới những tin tức ưu tú là những người có khả năng viết những tập lệnh kịch bản để khai thác những lỗ hổng đã biết. Những cá nhân này có năng lực kỹ

thuật hơn “script kiddies” (lớp dưới cùng của dải phổ) và chịu trách nhiệm cho 8% đến 12% của các hoạt động độc hại trên Internet. Khi tin tức hoạt động cùng nhau trong một nỗ lực tập thể, thường nhân danh một số nguyên nhân, họ được gọi là *những người theo chủ nghĩa hacktivists*. Các nhóm hacktivist có thể bao gồm các script kiddies, nhưng nói chung, các script kiddies không có đủ kỹ năng để tham gia vào theo một cách có ý nghĩa vào việc thúc đẩy một nguyên nhân hacktivist, mặc dù họ có thể được tuyển chọn như là quân đỗ bộ để làm gia tăng khối lượng cho cuộc tấn công.

### **Script Kiddies**

Ở lớp dưới cùng của dải phổ, về mặt kỹ thuật mà nói thì là những ai được gọi chung là các *script kiddies* – những cá nhân không có đủ chuyên môn kỹ thuật để phát triển các tập lệnh kịch bản hoặc khám phá ra những lỗ hổng mới trong phần mềm, mà là những ai chỉ đủ hiểu về các hệ thống máy tính để có khả năng tải về và chạy các tập lệnh kịch bản được người khác phát triển. Những cá nhân này nói chung không quan tâm đến việc tấn công các mục tiêu cụ thể mà thay vào đó chỉ đơn giản là muốn tìm kiếm bất kỳ tổ chức nào đã không vá những lỗ hổng [bảo mật] mới được khám phá để từ đó, các script kiddies đã xác định được một tập lệnh để khai thác [lỗ hổng]. Rất khó để ước tính có bao nhiêu cá nhân đang thực hiện các hành động như thăm dò mạng hoặc quét các hệ thống riêng lẻ là một phần của nhóm này, nhưng tuy nhiên, chắc chắn đây là nhóm phát triển nhanh nhất, và hầu hết các hoạt động “không thân thiện” diễn ra trên Internet là có lẽ được tiến hành bởi các cá nhân này.

### **Tổ chức Tội phạm**

Khi các doanh nghiệp trở nên phụ thuộc ngày càng nhiều hơn vào các hệ thống và mạng máy tính, và vì lượng giao dịch tài chính được tiến hành qua Internet gia tăng, điều không thể tránh khỏi là *tội phạm có tổ chức*

cuối cùng sẽ chuyển sang thế giới điện tử như một đích nhắm mục tiêu mới để khai thác. Một trong những thay đổi lớn trong vài thập kỷ qua trong lĩnh vực an ninh mạng là khả năng của tin tặc để kiếm tiền từ những nỗ lực của chúng. Một phần của điều này là sự phát triển của tiền điện tử, chẳng hạn như bitcoin, nhưng toàn bộ không gian thị trường trên web đen (dark web) tồn tại để đánh cắp danh tính, dữ liệu tài chính, và tài sản trí tuệ, tính theo đô la [Mỹ], lớn hơn cả hoạt động buôn bán ma túy quốc tế. Điều này đã dẫn đến việc hình thành nên một lớp nhân vật tội phạm có tổ chức hoàn toàn mới, những tội phạm an ninh mạng, những kẻ có thể ẩn mình trong bóng tối ẩn danh và tạo ra phần mềm độc hại và thực hiện các cuộc tấn công, tất cả đều nhắm vào mục đích kiếm tiền.

Hoạt động tội phạm trên Internet về cơ bản không khác gì hoạt động tội phạm trong thế giới thực tế. Gian lận, tống tiền, trộm cắp, biển thủ và giả mạo cũng đều diễn ra trong môi trường điện tử.

Một điểm khác biệt giữa các nhóm tội phạm và tin tặc “trung bình” là cấp độ tổ chức mà các phần tử tội phạm sử dụng trong cuộc tấn công của chúng. Các nhóm tội phạm thường có nhiều tiền hơn để chi tiêu cho việc hoàn thành các hoạt động tội phạm và sẵn sàng dành thêm thời gian để hoàn thành nhiệm vụ, miễn là mức thưởng khi kết thúc [cuộc tấn công] là đủ lớn. Với lượng tiền khổng lồ được trao đổi qua Internet hàng ngày, mức thưởng cho một vụ tấn công thành công đủ cao khiến cho các phần tử tội phạm quan tâm. Các cuộc tấn công của các tổ chức tội phạm thường thuộc loại *mối đe dọa có cấu trúc*, vốn được đặc trưng bởi thời lượng hoạch định nhiều hơn, thời gian tiến hành hoạt động dài hơn, nhiều ủng hộ tài chính hơn để hoàn thành nó, và có thể tham nhũng hoặc thông đồng với nội gián.

## Tin tặc

*Tin tặc* là một thuật ngữ rất phong phú, vì nó được nhiều người sử dụng cho những mục đích khác nhau. Cách sử dụng ban đầu của thuật ngữ liên quan đến những cá nhân đã dành thời gian để cố gắng tìm ra cách thức mà một thứ gì đó hoạt động như thế nào để họ có thể kiểm soát nó theo những cách mà nó [thứ gì đó] đã không được thiết kế. Điều này đôi khi có nghĩa là điều khiển phá hoại, dẫn đến việc sử dụng trái phép. Ngày nay, nhóm này vẫn tiếp tục tồn tại. Tuy nhiên, nhiều người cũng sử dụng thuật ngữ này để mô tả bất kỳ ai sử dụng máy tính không đúng cách, kể cả tội phạm. Điều này đã dẫn đến các bộ mô tả được cấp phép, trái phép và bán ủy quyền.

## Được cấp phép

Những cá nhân được phép, những người sử dụng các kỹ năng “hacking” máy tính của họ cho những mục đích tốt đẹp có tên gọi phổ biến là những tin tặc “mũ trắng” (white hat). Họ có thể là các chuyên gia tư vấn bảo mật theo đuổi những lỗ hổng [bảo mật] hoặc thực hiện các kiểm nghiệm xâm nhập, cũng như rất nhiều các hoạt động bảo mật khác. Sự khác biệt giữa một tin tặc mũ trắng và một ai đó đang phá vỡ luật lệ là rằng tin tặc mũ trắng sử dụng cùng các công cụ và kỹ thuật như các tác nhân đe dọa, nhưng thực hiện việc đó với những quyền hạn để từ đó một công ty có thể khám phá ra những điểm yếu của mình và khắc phục chúng.

## Trái phép

Những tin tặc mũ đen (black hat) đối ngược với những tin tặc mũ trắng. Thay vì sử dụng những kỹ năng của mình cho những mục đích tốt đẹp, chúng (tin tặc mũ đen) sử dụng các kỹ năng của mình để thực hiện các hoạt động tội phạm và hoạt động phi pháp. Các nhóm và cá nhân hoạt động theo một cách phi pháp vi phạm luật pháp và gây ra rủi ro cho các hệ thống. Có rất nhiều động cơ khác nhau đứng sau những tin tặc mũ đen, nhưng cuối cùng, chúng đang thực hiện những hoạt động phi pháp.

## Bán-Ủy-quyền

Những tin tặc mũ xám (*gray hat*) đứng trong cả hai thế giới [*hàm ý chỉ cả mũ trắng lẫn mũ đen – người dịch*]. Họ có thể sử dụng những kỹ năng của mình cho những mục đích tốt đẹp và công việc của họ cũng như những tin tặc mũ trắng, nhưng sau đó, tại những thời điểm khác, họ sử dụng cùng các kỹ năng để hoạt động một cách phi pháp như là một tin tặc mũ đen. Nhóm những tin tặc bán-Ủy-quyền này hoạt động trong cả lĩnh vực bảo mật được chấp thuận lẫn lĩnh vực hoạt động tội phạm.



## MÁCH NƯỚC CHO KỲ THI

Cần biết rằng những tin tặc mũ trắng/được cấp phép là những chuyên gia bảo vệ các hệ thống, những tin tặc mũ đen/trái phép là những tội phạm xâm nhập các thiết bị và ứng dụng để đánh cắp dữ liệu, và những tin tặc mũ xám/bán-Ủy-quyền thường vi phạm các quy tắc đạo đức và luật lệ, nhưng không phải lúc nào cũng có những ý định độc hại như các tin tặc mũ đen.



**LƯU Ý** Tại sao lại có những thuật ngữ *mũ đen* và *mũ trắng*? Đây là sự liên tưởng ngược về những bộ phim cao bồi thời xưa, khi người tốt đội mũ trắng còn kẻ phản diện đội mũ đen.

## Bóng đổ CNTT (Shadow IT)

*Bóng đổ CNTT* là một tên gọi được đặt cho những bộ phận của một tổ chức thực hiện những chức năng CNTT của riêng họ. Những nhóm này vượt ra khỏi mong muốn “hoàn thành công việc” khi trung tâm CNTT không phản hồi về những gì mà đơn vị coi là một khung thời gian hợp lý. Mặc dù nỗ lực CNTT tự tổ chức này trông có vẻ khá hữu ích vì nó nằm

ngoài tầm kiểm soát của chức năng trung tâm CNTT, các hệ thống CNTT đã được tạo ra không nằm trong cùng một lĩnh vực bảo vệ. Nếu như bạn thiết lập một điểm truy cập không dây để bạn có thể di chuyển tự do trong khu vực văn phòng của mình mà không bị ràng buộc bởi cáp mạng, câu hỏi sẽ trở thành ai sẽ là người giữ cho kết nối mạng được an toàn khỏi các mối đe dọa bên ngoài? Nếu như một ổ cứng bị lỗi trên một phần bóng đổ CNTT của cơ sở hạ tầng, nó đã được sao lưu một cách đúng đắn hay chưa? Dữ liệu sẽ được khôi phục như thế nào? Nói chung thì bóng đổ CNTT là một triệu chứng của một quy trình CNTT tập trung kém hoàn hảo và có thể dẫn đến những rủi ro gia tăng. Bóng đổ CNTT có thể trở thành một rủi ro đáng kể vì cơ sở hạ tầng của nó mang lại cho người dùng nội bộ quyền truy cập và những kết nối được tăng cường.

### **Đối thủ cạnh tranh**

*Đối thủ cạnh tranh* có thể là một mối đe dọa đối với doanh nghiệp trên thương trường: bán hàng, giảm giá, sản phẩm của đối thủ - đó là một cuộc chiến giành khách hàng trong từng ngày. Nhưng đây là kinh doanh – hợp pháp và bình thường. Tuy nhiên, những đối thủ cạnh tranh đã được biết là đã tấn công những quy trình CNTT của các công ty khác. Những phương pháp là khác nhau, từ đơn giản là đánh giá sai sản phẩm đến những yếu tố nghiêm trọng hơn như xâm nhập thực tế vào các hệ thống. Có một số trường hợp đã được ghi nhận lại về hoạt động tội phạm của một công ty chống lại công ty khác. Điều này bao gồm việc đánh cắp tài sản sở hữu trí tuệ hoặc các danh sách khách hàng cũng như các hoạt động khác chẳng hạn như các cuộc tấn công từ-chối-dịch-vụ.

### **Các thuộc tính của các Tác nhân**

Các tác nhân đe dọa có thể được chia thành các nhóm dựa trên khả năng. Có một số cách để phân biệt các tác nhân đe dọa, bao gồm: theo vị trí

(bên trong hoặc bên ngoài), mức độ tinh vi, mức độ tài nguyên, và dự định. Những thuộc tính sẽ được mô tả ngay tiếp theo đây.

## **Nội bộ/Bên ngoài**

Các tác nhân đe dọa trong nội bộ có một lợi thế đáng kể so với các tác nhân bên ngoài: họ có quyền truy cập vào hệ thống. Mặc dù quyền truy cập có thể bị hạn chế ở mức người dùng nhưng nó vẫn mang lại cho tác nhân đe dọa khả năng theo đuổi cuộc tấn công của họ. Các tác nhân bên ngoài có thêm một bước bổ sung cần phải thực hiện: thiết lập quyền truy cập vào hệ thống mục tiêu.

## **Mức độ Tinh vi/Năng lực**

Như đã được minh họa trước đây trong [Hình 5-1](#), kỹ năng và mức độ tinh vi của kẻ tấn công có thể được chia thành một vài thể loại. Tuy nhiên, trong phạm vi một nhóm các tác nhân đe dọa, mức độ kỹ năng của cá nhân các thành viên của nhóm có thể được kết hợp, với một vài cá nhân có kỹ năng cao đóng vai trò thúc đẩy một lượng lớn những người tham gia có ít kỹ năng hơn. Mức độ kỹ năng càng cao thì một cá nhân sẽ càng được kỳ vọng dẫn dắt và thiết kế nên các cuộc tấn công. Khi đề cập đến mức độ tinh vi của bản thân cuộc tấn công, có một khuynh hướng đáng chú ý là rằng khi mức độ kỹ năng tăng lên thì việc sử dụng các phương pháp tối thiểu cũng vậy. Dù cho các cuộc tấn công Zero-day đã được đề cập một cách rộng rãi trên các bản tin, những lỗ hổng zero-day thực sự vẫn hiếm khi được sử dụng, chúng được để dành cho một số ít trường hợp khi không còn sự lựa chọn nào khác, bởi vì khi những lỗ hổng này bị khai thác, chúng sẽ được vá lại. Thậm chí ngay cả với những nhóm quốc gia có mức độ tinh vi cao đang sử dụng các phương pháp APT, một số cuộc tấn công ngạc nhiên thay lại là những hình thức tấn công cũ, khai thác những lỗ hổng cũ, và sử dụng các phương pháp đơn giản để tận dụng “những mục tiêu dễ đạt được – low-hanging fruit”. Điều này

không có nghĩa là những phương pháp mới hơn, tiên tiến hơn không bao giờ được sử dụng, mà thay vào đó, có một cơ chế kinh tế trong bản thân các cuộc tấn công, chỉ sử dụng những gì cần thiết tại từng thời điểm. Cũng có rất nhiều dữ liệu bị thiếu trong kịch bản này, vì chúng ta thường không biết về các phương pháp đã được sử dụng một cách thành công nếu như tác nhân đe dọa vẫn không bị phát hiện.

### **Tài nguyên/Nguồn vốn**

Như đã được đề cập trước đây, các tổ chức tội phạm và các quốc gia có nguồn ngân sách dồi dào, có các nhóm lớn và khả năng theo đuổi các chiến dịch trong những khoảng thời gian dài. An ninh mạng là một thách thức cho cả những kẻ tấn công lẫn những người phòng thủ, và có những khoản chi tiêu nhất định tương xứng với việc duy trì các nhóm và các công cụ được sử dụng bởi các tác nhân đe dọa để chống lại một hệ thống. Các APT, cùng với thiên hướng của chúng đối với các cuộc tấn công dài hạn, một số thậm chí kéo dài hàng năm, đòi hỏi những nguồn lực đáng kể để dàn xếp kiểu hoạt động này, từ đó, có một nhu cầu đối với những nguồn lực dài hạn mà chỉ có những tổ chức lớn hoặc những chính phủ có thể đáp ứng được theo thời gian.

### **Mục đích/Động cơ**

Về bản chất, mục đích hoặc động cơ đứng sau một cuộc tấn công có thể rất đơn giản hoặc đa dạng. Một script kiddies chỉ đang cố gắng làm cho một kỹ thuật hoạt động. Một tác nhân đe dọa có kỹ năng cao hơn thường theo đuổi một mục tiêu cụ thể, chẳng hạn như cố gắng tạo ra quan điểm như một kẻ hacktivist. Ở đỉnh trên cùng của kim tự tháp ý định là tác nhân đe dọa APT, có ý định hoặc động cơ ít nhất gấp ba lần: Đầu tiên là động lực duy trì quyền truy cập liên tục. Thứ hai là động lực về việc vẫn không bị phát hiện. Trong hầu hết các APT được phát hiện, thời gian xâm nhập đều lớn hơn một năm và trong nhiều trường hợp, việc xác định ngày

lây nhiễm ban đầu là không thể, vì nó bị giới hạn bởi độ dài của các bản ghi nhật ký. Thứ ba là mục tiêu đánh cắp thứ gì đó có giá trị trên hệ thống mạng. APT không gây ra tất cả những rắc rối trong việc duy trì quyền truy cập và vẫn vô hình chỉ để làm hư hỏng hoặc buộc xây dựng lại một hệ thống.

---



**MÁCH NƯỚC CHO KỲ THI** Kỳ thi Security+ sẽ mô tả các tác nhân đe dọa về mặt các thuộc tính: nguồn lực, mức độ tinh vi, vị trí, và động cơ. Hãy chắc chắn hiểu được cách mà những khác biệt này có ý nghĩa như thế nào liên quan đến kiểu của cuộc tấn công.

### Các Véc-tơ

Các mối đe dọa được duy trì bởi các tác nhân đe dọa và chúng sử dụng các véc-tơ khác nhau để khai thác các lỗ hổng trong hệ thống, cấp cho chúng quyền truy cập trái phép. Các *véc-tơ* là thuật ngữ chỉ các phương thức khác nhau mà kẻ tấn công có thể sử dụng để xâm nhập - cho dù đó là truy cập trực tiếp qua các kênh kết nối mạng không dây hoặc qua email, phương tiện truyền thông xã hội, chuỗi cung ứng, nguồn dữ liệu bên ngoài như phương tiện di động hoặc đám mây. Điểm mấu chốt là nếu như có một cách nào đó để di chuyển dữ liệu vào trong hệ thống của bạn thì đây có thể là một véc-tơ tiềm năng cho những kẻ tấn công sử dụng, do đó, bạn phải thực hiện các biện pháp bảo vệ thích hợp.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy chuẩn bị cho những câu hỏi yêu cầu bạn xác định sự khác biệt giữa các kiểu véc-tơ mối đe dọa.

## Truy cập Trực tiếp

*Truy cập trực tiếp* chỉ đơn giản là: kẻ tấn công trực tiếp truy cập vào hệ thống. Đây có thể là một cuộc tấn công từ bên trong, hoặc có lẽ là do người bên ngoài được cung cấp khả năng tương tác một cách trực tiếp với các hệ thống, chẳng hạn như các máy chủ web. Truy cập trực tiếp là lý do vì sao chúng ta cần áp dụng nguyên tắc đặc quyền ít nhất, chỉ cấp những quyền hạn cần thiết và chặn những đặc quyền khác. Trong trường hợp một người bên ngoài được cấp những quyền hạn sử dụng một hệ thống (có nghĩa là, tạo ra các trang trên một trang web), điều bắt buộc là tất cả mọi đầu vào từ bên ngoài phải được coi là nguy hiểm cho đến khi chứng minh được điều ngược lại.

## Mạng không dây

Các mạng không dây khiến cho việc kết nối mạng trở nên đơn giản hơn. Tuy nhiên, sự kết nối dễ dàng các máy móc này đi kèm theo một loạt các vấn đề về bảo mật. Để biết thêm chi tiết về các vấn đề bảo mật không dây tổng thể, hãy đọc [Chương 20](#). Liên quan đến các véc-tơ tấn công, truy cập *không dây* đem đến một loạt những cơ hội mới. Kẻ tấn công không cần phải truy cập vật lý trực tiếp vào hệ thống mạng – một tín hiệu không dây có thể giúp cho kẻ tấn công truy cập, người có thể chỉ cần ngồi trong bãi đỗ xe để thực hiện cuộc tấn công của mình.

## Email

*Email* là một trong những véc-tơ được yêu thích của các cuộc tấn công kỹ thuật xã hội. Việc gửi đi một email bao gồm các đường liên kết hoặc các tập tin đính kèm là một cách tương tác với người dùng. Nếu như kèm theo một thông điệp thuyết phục, người dùng có thể sẽ nhấp chuột vào các đường liên kết hoặc mở tập tin đính kèm, và véc-tơ đã hoàn thành công việc của nó – phân phối tải trọng.

## Chuỗi Cung Ứng

Một véc-tơ *chuỗi cung ứng* liên quan đến việc sử dụng chuỗi cung ứng của một công ty như là một tác nhân không chủ ý trong một cuộc tấn công. Có rất nhiều hình thức tấn công có thể được thực hiện theo cách này, và một vài hình thức được đề cập trong [Chương 1](#) và [Chương 33](#). Khái niệm là tương đối đơn giản: một kẻ tấn công tìm kiếm một phương tiện mà theo đó, chúng có thể đưa đoạn mã tấn công vào trong chuỗi cung ứng của một sản phẩm hoặc một bản cập nhật – ví dụ, việc tấn công một nhà cung cấp và để lại một đoạn mã trong một chương trình được sử dụng để kiểm nghiệm phần cứng lưu trữ, từ đó, để lại một đoạn mã xấu trên thiết bị lưu trữ mới, hoặc tấn công cơ chế cập nhật bằng cách nhiễm độc một trong số các tập tin cập nhật được phân phối qua trang web. Các công ty có khuynh hướng tin tưởng vào các nhà cung cấp của họ và có thể bỏ qua các kiểm tra an ninh chằng hạn như xác thực các bản tải về bằng các hàm băm. Đây là một lĩnh vực mà Microsoft đã thực hiện rất xuất sắc: quy trình cập nhật của họ có rất nhiều lần kiểm tra bảo mật nên hầu như không thể làm nhiễm độc một trong các bản cập nhật của công ty.

Vào tháng 12 năm 2020, một gói phần mềm quản lý tập trung phổ biến, Solar Winds Orion, được phát hiện là đã bị một tổ chức cấp quốc-gia-nhà-nước xâm phạm. Sự xâm phạm này vào chuỗi sản phẩm đã không được chú ý trong 9 tháng, lan rộng ra khắp các tập đoàn hàng đầu và các cơ quan chính phủ. Danh sách các công ty vi phạm sẽ không được công bố cho đến khoảng năm 2021, nhưng những tên tuổi lớn nhất trong ngành công nghệ, Microsoft, Cisco, FireEye và các cơ quan chính phủ lớn của Hoa Kỳ, đã phải bắt đầu xử lý thiệt hại. Cuộc tấn công, sử dụng chuỗi cung ứng của một bộ công cụ được sử dụng một cách phổ biến, rất tinh vi và tiên tiến một cách đáng kể, vẫn nằm trong bóng tối trong suốt nhiều

tháng. Các cuộc tấn công vào chuỗi cung ứng là một mối đe dọa thực sự và không thể bị ngăn chặn chỉ bằng chính sách và các hợp đồng.

## Mạng Xã hội

*Mạng xã hội* có thể trở thành một véc-tơ cho các cuộc tấn công kỹ thuật xã hội vì nó kết nối trực tiếp một kẻ tấn công với một người dùng, và rất nhiều kiểm tra bảo mật đã cho thấy không hiện diện với email và các kênh truyền thông doanh nghiệp khác. Bằng cách gửi đi một URL được rút gọn, kẻ tấn công có thể thường khiến mọi người nhấp vào nó, và sau đó với thủ đoạn chuyển hướng, những điều tồi tệ có thể xảy ra trước khi [tập tin] GIF được mong muốn xuất hiện, và người dùng không bao giờ thông minh hơn tải trọng đã được phân phối. Những cuộc tấn công kỹ thuật xã hội dựa-trên-phương-tiện-truyền-thông được đề cập trong [Chương 1](#).

## Phương tiện Di động

*Phương tiện di động* thường dưới dạng các thẻ nhớ USB, đại diện cho một mối đe dọa rõ ràng. Loại thiết bị lưu trữ này khá nhỏ gọn, phổ biến, và không đòi hỏi bất kỳ kỹ năng gì để có thể gắn vào một máy tính. Việc nó trở thành một mối đe dọa như thế nào được thúc đẩy bởi kỹ thuật xã hội. Một kẻ tấn công lấy một thiết bị lưu trữ USB và đưa mô-đun tấn công vào trong nó để từ đó nó thể được thực thi. Sau đó, mánh lới là khiến cho một ai đó tương tác với tập tin đó. Việc đặt thiết bị USB ở một vị trí dễ được phát hiện sẽ dẫn đến một cuộc tấn công được gọi là “tấn công thả rơi USB” (xem [Chương 2](#)). Như với tất cả các cuộc tấn công mang tính hành vi, chúng ta cần phải giáo dục người dùng (trong trường hợp này, người dùng nên được dạy rằng không chạm vào các ổ USB “bị bỏ rơi”). Họ nên coi các thiết bị lưu trữ USB là “đống phân chó (dog poop)” và tránh việc nhặt chúng lên và sử dụng chúng. Bạn cũng có thể sử dụng chương trình chặn USB và tắt Tự động phát [AutoPlay] (có thể được bật

theo mặc định) đối với USB và phương tiện di động. Các biện pháp bảo vệ ở cấp-hệ-thống này có thể có ý nghĩa đối với những máy móc cụ thể như ki-ốt hoặc những máy tiếp xúc với công chúng.

## **Đám mây**

*Đám mây* là một véc-tơ tấn công khác. Nếu như bạn đã được kết nối tới đám mây, nó sẽ được dành cho mục đích kinh doanh, và do đó, bạn sẽ có một số hình thức tin tưởng vào nó. Tuy nhiên, nếu bạn xem xét đám mây, và đặc biệt là đám mây lưu trữ, cũng như với một máy tính của ai đó, bạn có thể nhìn thấy véc-tơ [tấn công]. Nếu như thỏa thuận [dịch vụ] đám mây của bạn không bao gồm sự bảo vệ chống vi-rút trên các tập tin thì nó thực sự không khác gì so với bất kỳ nguồn được kết-nối-Internet nào khác.

## **Nguồn Tình báo về Mối đe dọa**

An ninh mạng là một trò chơi về quản lý tài nguyên. Không có một công ty nào có đủ nguồn lực để bảo vệ mọi thứ chống lại mọi mối đe dọa, và thậm chí việc cố gắng làm như vậy sẽ làm gia tăng thêm sự phức tạp dẫn đến việc mở ra các con đường đe dọa khác. Một trong những quyết định quan trọng cần được đưa ra là nơi để áp dụng các nguồn lực của một ai đó trong bối cảnh phức tạp về bảo vệ an ninh mạng. Thông tin tình báo về mối đe dọa là việc thu thập thông tin từ nhiều nguồn khác nhau, bao gồm cả các nguồn không công khai, để cho phép một thực thể tập trung một cách đúng đắn các biện pháp phòng thủ của mình để chống lại các tác nhân có khả năng xảy ra mối đe dọa cao nhất. Các *nguồn thông tin tình báo về mối đe dọa* là những nơi mà người ta có thể lấy được thông tin này, và có rất nhiều nguồn trong số đó - từ nguồn mở, đến độc quyền, cho đến các nguồn chuyên biệt. Những điều này sẽ được đề cập trong các phần tiếp theo sau.



**MÁCH NƯỚC CHO KỲ THI** Hãy chuẩn bị cho những câu hỏi yêu cầu bạn xác định sự khác biệt giữa các loại nguồn tin tình báo về mối đe dọa.

### **Thông tin tình báo Nguồn Mở (Open Source Intelligence – OSINT)**

*Thông tin tình báo nguồn mở*, đôi khi còn được gọi là *thông tin tình báo về mối đe dọa nguồn mở*, đề cập đến thông tin tình báo được thu thập từ những nguồn công khai. Có một loạt những nguồn thông tin công khai liên quan đến hoạt động an ninh mạng hiện hành. Từ các bài báo mới đến các blog, đến các báo cáo của chính phủ, dường như có một luồng tin tức không-bao-giờ-ngừng quan tâm đến những gì đang xảy ra, đối với ai, và như thế nào. Thách thức nằm ở việc sắp xếp thông tin thành một định dạng hữu dụng, vốn đó là một nhu cầu mà thông tin tình báo nguồn mở đáp ứng.

Có rất nhiều nguồn cấp dữ liệu nguồn mở, và mỗi nguồn đều có thể bổ sung thêm giá trị, nhưng câu hỏi quan trọng cho từng nguồn cấp dữ liệu là những thông tin đó đến từ đâu, thông tin được kiểm duyệt như thế nào, và thông tin cập nhật như thế nào. Dưới đây là một danh sách về một vài nguồn và những đáp án cơ bản cho những câu hỏi đó.

- **Bộ An ninh Nội địa Hoa Kỳ (DHS).** Chia sẻ Chỉ báo Tự động hóa là tập hợp của những thông tin như địa chỉ email độc hại, địa chỉ IP và các tài liệu xấu khác được các công ty tư nhân báo cáo cho DHS thông qua cổng thông tin Chia sẻ Chỉ báo Tự động hóa (AIS). Danh sách này được sắp xếp và phụ thuộc vào việc đóng góp của các công ty để giữ cho nó được cập nhật và toàn diện.
- **Cục Điều tra Liên bang Hoa Kỳ (FBI)** Cổng InfraGard là một tập hợp truy cập đã được kiểm duyệt thông tin bảo mật được báo cáo cho FBI. Nó có xu hướng tập trung vào cơ sở hạ tầng quan trọng và

có thể có thời gian trễ đáng kể, do FBI nắm giữ thông tin liên quan đến các cuộc điều tra.

- **SANS** Internet Storm Center (ISC) là một mạng cảm biến phân tán xử lý hơn 20 triệu mục nhập nhật ký phát hiện xâm nhập mỗi ngày và tạo ra các cảnh báo liên quan đến các mối đe dọa bảo mật.
- **VirusTotal** Hiện đang được vận hành bởi Google, VirusTotal sử dụng nguồn cấp dữ liệu từ vô số trình quét chống vi-rút để duy trì một cơ sở dữ liệu đặc trưng về phần mềm độc hại và những thông tin có liên quan.
- **Cisco** Nhóm Talos Intelligence của Cisco giới thiệu một nguồn cấp thông tin cho các khách hàng của Cisco (một phiên bản miễn phí cũng sẵn có). Độ rộng của bộ sưu tập của Cisco và đội ngũ nghiên cứu chuyên sâu của họ khiến cho đây là một nguồn cấp thông tin quan trọng về các mối nguy hiểm mới và đang nổi lên.

### **Đóng/Độc quyền**

Thị trường thông tin tình báo về mối đe dọa được lấp đầy bằng các công ty bảo mật đang cung cấp các sản phẩm thông tin tình báo về các mối đe dọa. Một trong số các sản phẩm chủ yếu của họ là quyền truy cập đến cơ sở dữ liệu thông tin tình báo về mối đe dọa *đóng* hoặc *độc quyền*. Để đánh giá những sản phẩm này, một trong số các yếu tố then chốt là số lượng và sự đa dạng của nguồn cung cấp dữ liệu. Nguồn dữ liệu của họ là gì và những đặc trưng liên quan đến dữ liệu trong cơ sở dữ liệu của họ là gì? Hầu hết các công ty sẽ cung cấp một định dạng tập tin có thể tự động hóa có nguồn từ cấu trúc dữ liệu của họ để cung cấp thông tin cho các công cụ bảo mật từ dữ liệu của họ. Những định dạng phổ biến bao gồm CSV, XML, JSON, và STIX. STIX (định dạng Structured Threat Information Expression) đặc biệt được đề cập sau trong chương này. Một yếu tố quan trọng khác bao gồm những điều chẳng hạn như bao lâu thì dữ liệu được cập nhật và ngành nào đang là trọng tâm của dữ liệu. Thắc

mắc về ngành là quan trọng bởi vì ở tại một cấp độ, mọi hệ thống CNTT đều đối mặt với cùng một loạt các lỗ hổng, các tác nhân đe dọa có những hình mẫu và chúng có khuynh hướng hoạt động theo ngành, khiến cho mức độ phơi nhiễm khác nhau theo từng ngành.

### Các Cơ sở dữ liệu về Lỗ hổng

Các lỗ hổng là những điểm yếu trong phần mềm cho phép một kẻ tấn công một phương tiện để truy nhập [vào phần mềm và/hoặc hệ thống]. Bạn cần phải biết lỗ hổng là gì và hoặc là vá lỗ hổng lại hoặc cung cấp một giải pháp phòng thủ để ngăn chặn lỗ hổng khỏi bị khai thác bởi một kẻ tấn công. Việc biết được những lỗ hổng nào đang tồn tại trong phần mềm là một thách thức. Bởi vì có rất nhiều mảnh của phần mềm và rất nhiều lỗ hổng, đây là một vấn đề dữ liệu và cần phải có một cơ sở dữ liệu để lập danh mục và duy trì. Do đó, có những *cơ sở dữ liệu về lỗ hổng* – và không chỉ có một và có đến vài cơ sở dữ liệu. Ví dụ, Cơ sở dữ liệu về Lỗ hổng Quốc gia Hoa Kỳ (NVD) được lưu trữ tại nvd.nist.gov là một kho lưu trữ về các lỗ hổng và thông tin có liên quan chẳng hạn như các tham chiếu danh mục kiểm tra bảo mật, các khiếm khuyết phần mềm liên-quan-đến-bảo-mật, những cấu hình sai, tên sản phẩm, và các chỉ số tác động.

Đã có những nỗ lực khác trong việc tạo ra những cơ sở dữ liệu về lỗ hổng bảo mật, bao gồm Cơ sở dữ liệu về Lỗ hổng Bảo mật Nguồn Mở (Open Source Vulnerability Database - OSVDB) lâu dài, đã hoạt động từ năm 2004 đến năm 2016, khi nó đã trở thành một mô hình đăng ký thuê bao. Hầu hết các cơ sở dữ liệu về lỗ hổng do các công ty bảo mật tung ra thị trường đều được sửa đổi từ NVD. Một ngoại lệ chính là cơ sở dữ liệu về lỗ hổng Metasploit, vốn là một kho lưu trữ được biên tập chỉnh sửa của các hoạt động khai thác đã được kiểm duyệt đối với các lỗ hổng được sử dụng trong khuôn khổ Metasploit.

## Trung tâm Chia sẻ Thông tin Công khai/Riêng tư

Trong địa hạt các trung tâm chia sẻ thông tin công khai/riêng tư là các Trung tâm Phân tích và Chia sẻ Thông tin (Information Sharing and Analysis Centers - ISAC) và các Tổ chức Phân tích và Chia sẻ Thông tin (Information Sharing and Analysis Organizations - ISAO). Các ISAO rất khác nhau về năng lực nhưng về cơ bản, bao gồm bất kỳ tổ chức nào, cho dù là lĩnh vực công nghiệp hay khu vực địa lý, đang chia sẻ thông tin liên-quan-đến-mạng nhằm mục đích nâng cao vị thế an ninh mạng của các thành viên của họ. Các ISAC là một hạng mục đặc biệt của ISAO bao gồm an ninh mạng dựa-thao-ngành do tư nhân điều hành nhưng được chính phủ phê duyệt. ISAC có thể được coi là trung tâm tổng hợp, nơi thông tin thời-gian-thực có thể được chia sẻ giữa các thành viên. Các ISAO và ISAC hoạt động trên một tiền đề rất đơn giản: chia sẻ những gì đang xảy ra với bạn và cùng nhau tìm hiểu những gì đang xảy ra trong ngành của bạn. Việc chia sẻ được ẩn danh, quá trình phân tích được thực hiện bởi các nhân viên có tay nghề cao trong trung tâm vận hành bảo mật và thông tin về kết quả được cung cấp lại cho các thành viên gần với thời gian thực nhất có thể. Chi phí cho các nhà phân tích có kỹ năng cao rất đắt đỏ và cơ chế này chia sẻ chi phí cho tất cả các tổ chức thành viên.

Một chương trình của chính phủ Hoa Kỳ, InfraGard, được điều hành bởi FBI và cũng hoạt động như một phương tiện chia sẻ, mặc dù tính kịp thời và mức độ phân tích không bằng ISAC, nhưng giá cả phù hợp (miễn phí).

## Web Tối

*Web tối (dark web)* là một tập hợp con của nội dung toàn cầu trên Internet bị hạn chế quyền truy cập thông qua các phương pháp giải mã cụ thể. Các trang web đen là các trang yêu cầu Tor — một phần mềm mã nguồn mở và miễn phí cho phép giao tiếp ẩn danh. Bởi vì dark web chỉ

tồn tại trong lĩnh vực định tuyến củ hành (onion routing), các trang dark web kết thúc bằng .onion, trái ngược với .com, .net, v.v... Khi một trình duyệt ở trên dark web, do giao thức định tuyến củ hành, quyền truy cập là ẩn danh. Điều này đã khiến cho dark web trở thành thiên đường của hoạt động tội phạm và người ta có thể tìm thấy rất nhiều mặt hàng bất hợp pháp ở đó - từ thông tin bị đánh cắp cho đến các chất bất hợp pháp.

---



**LƯU Ý** Có một khu vực trên Internet được gọi là deep web, vốn là một phần của Internet không được đánh chỉ mục bởi các công cụ tìm kiếm. Một ví dụ về deep web là một tài liệu đòi hỏi bạn phải đăng nhập vào một tài khoản trước khi nó được hiển thị. Vâng, deep web thực tế là có thể truy cập được từ trình duyệt, nhưng chỉ với những thông tin cụ thể, chẳng hạn như một phiên đăng nhập để truy cập vào đó. Đây là điểm khác biệt so với dark web. Do đó, mặc dù một số có thể sử dụng các thuật ngữ thay thế cho nhau nhưng vẫn có sự khác biệt giữa deep web và dark web.

### **Chỉ báo Xâm phạm**

Các chỉ báo xâm phạm (IoCs) đúng như tên gọi của nó: các chỉ báo chỉ ra rằng một hệ thống đã bị xâm phạm bởi hoạt động trái phép. Khi một tác nhân đe dọa thay đổi một hệ thống, hoặc bởi hành động trực tiếp, phần mềm mã độc, hoặc hình thức khai thác khác, những chứng cứ điều tra pháp y vẫn tồn tại đằng sau hệ thống. IoC đóng vai trò như đường dẫn dấu vết cho các nhà điều tra, cung cấp những manh mối nhỏ có thể giúp xác định sự hiện diện của một cuộc tấn công vào một hệ thống. Thách thức ở đây là việc tìm kiếm, thu thập và phân tích các bit thông tin này và sau đó xác định ý nghĩa của chúng đối với một hệ thống nhất định. Đây là một trong những nhiệm vụ chính của người ứng phó sự cố:

thu thập và xử lý các phần dữ liệu khác nhau này và tạo ra một bức tranh có ý nghĩa về trạng thái hiện tại của hệ thống.

May mắn thay, chúng ta có những bộ công cụ hỗ trợ cho điều tra viên trong nhiệm vụ này. Các công cụ như YARA có thể lấy một tập hợp các chữ ký (còn được gọi là IoC) và sau đó quét hệ thống để tìm chúng, xác định xem có đáp ứng một ngưỡng cụ thể hay không chỉ ra một sự lây nhiễm cụ thể. Mặc dù danh sách cụ thể sẽ khác nhau dựa trên hệ thống và mối đe dọa cụ thể mà người ta đang tìm kiếm, một tập hợp IoC chung mà các công ty nên giám sát bao gồm những điều sau:

- Lưu lượng mạng đi ra bất thường,
- Sự bất thường trong hoạt động của tài khoản của người dùng đặc quyền,
- Sự bất thường về vị trí địa lý trong lưu lượng mạng,
- Các cờ đỏ đăng nhập tài khoản,
- Sự gia tăng khối lượng đọc cơ sở dữ liệu,
- Kích thước phản hồi HTML,
- Số lượng lớn các yêu cầu cho cùng một tập tin,
- Lưu lượng ứng-dụng-cổng (port-application) không khớp, bao gồm cả lưu lượng được mã hóa trên cổng đơn giản,
- Thay đổi tập tin hệ thống hoặc registry đáng ngờ,
- Yêu cầu DNS bất thường,
- Bản vá lỗi đột xuất của hệ thống,
- Thay đổi biên dạng thiết bị di động,
- Nhóm dữ liệu ở sai vị trí,
- Lưu lượng truy cập web với hành vi không phải của con người,
- Dấu hiệu của hoạt động DDoS, ngay cả khi tạm thời.

Không có sự xâm phạm nào sẽ thể hiện tất cả mọi thứ trong danh sách này, nhưng việc giám sát các mục này sẽ có xu hướng nắm bắt hầu hết các xâm phạm, bởi vì tại một số thời điểm trong vòng đời của sự xâm phạm, mọi xâm phạm sẽ thể hiện một hoặc nhiều hành vi trước đó. Sau đó, một khi sự xâm phạm được phát hiện, người ứng phó có thể tập trung vào thông tin và ghi nhận lại đầy đủ bản chất và phạm vi của vấn đề.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy lưu ý rằng các chỉ báo điển hình về sự xâm phạm có thể bao gồm các chữ ký nhận dạng vi-rút, các tên miền hoặc URL của máy chủ botnet, và các hàm băm MD5 của phần mềm độc hại.

### **Chia sẻ Chỉ báo Tự động hóa (AIS)**

Được tạo ra bởi Bộ An ninh Nội địa Hoa Kỳ, *Chia sẻ Chỉ báo Tự động hóa (AIS)* là một phương pháp chỉ báo về các mối đe-dọa-mạng hai chiều được tự động hóa được sử dụng cho mục đích báo cáo. Một yếu tố then chốt của AIS là rằng nó hoạt động ở tốc độ của máy móc, cho phép báo cáo và phản hồi gần-như-thời-gian-thực. Các công ty phải đăng ký để tham gia vào nỗ lực này, và một khi họ thống nhất chia sẻ thông tin được ẩn danh, kết nối của họ được thiết lập. Mục tiêu của chương trình AIS là để chuyển hóa thành hàng hóa việc thu thập thông tin tình báo về mối đe dọa để cho phép mọi người tiếp cận để cung cấp các mối đe dọa về mạng. Hệ thống AIS sử dụng những đặc tả kỹ thuật Structured Threat Information Expression (STIX) và Trusted Automated Exchange of Intelligence Information (TAXII) để cho phép kết nối máy-máy ở tốc độ của máy móc. Những người tham gia vào AIS phải có khả năng sản xuất và tiêu dùng những giao thức này.

## Điễn đạt Thông tin về Mối đe dọa có Cấu trúc (STIX)/Trao đổi Thông tin Tình báo Tự động hóa Đáng tin cậy (TAXII)

Để truyền đạt những thông tin về các-mối-đe-dọa-mạng ở tốc độ máy móc, Bộ An ninh Nội địa Hoa Kỳ đã khởi đầu chương trình STIX/TAXII (Structured Threat Information Expression/Trusted Automated Exchange of Intelligence Information) vào năm 2012. Giờ đây được điều hành bởi cơ quan đồng thuận quốc tế OASIS, cả STIX lẫn TAXII đều cung cấp một bộ các tiêu chuẩn hướng-cộng-đồng để cho phép tự động hóa việc trao đổi thông tin tương ứng với các mối đe dọa mạng, các biện pháp phòng thủ mạng, và phân tích về các mối đe dọa. STIX là một ngôn ngữ có cấu trúc được tiêu chuẩn hóa, có-thể-đọc-bằng-máy (và cả con người) để trình bày những thông tin về các mối-đe-dọa-mạng. TAXII định nghĩa một bộ các dịch vụ và thông điệp trao đổi để cho phép tự động hóa việc chia sẻ những thông tin về các mối-đe-dọa-mạng có thể hành động được qua các ranh giới tổ chức, dòng sản phẩm và dịch vụ. TAXII giới thiệu các phương pháp truyền tải, và STIX trình bày thông điệp.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng STIX trình bày về những thông tin về các mối-đe-dọa-mạng (nguồn tin về mối đe dọa) trong khi TAXII định nghĩa cách thức thông tin được trao đổi. Bạn có thể nghĩa về TAXII như là “làm thế nào để đến đó”.

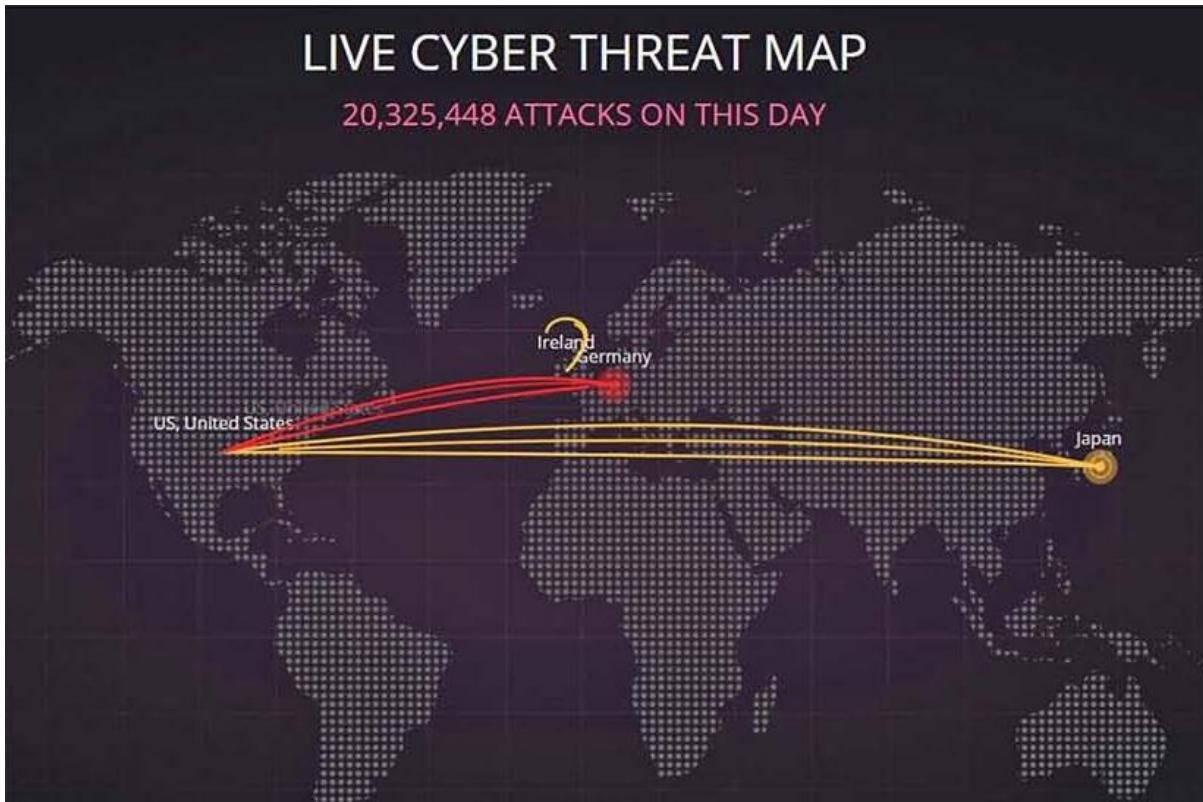
### Phân tích Dự báo

*Phân tích dự báo* là việc sử dụng thông tin tình báo về mối đe dọa để dự báo sự dịch chuyển tiếp theo của một mối đe dọa. Thông thường, việc này được hoàn thành bằng cách tiến hành tổ chức sắp xếp một lượng lớn dữ liệu từ rất nhiều nguồn và chọn lọc giữa vô số dữ liệu này để tìm kiếm những mẫu thông tin quan trọng cần thiết để cùng đưa ra giả thuyết về những mối đe dọa tiềm ẩn và xác định cách thức làm thế nào để tìm ra

chúng trong doanh nghiệp của bạn. Vì mỗi ngành có các tác nhân đe dọa khác nhau, và mỗi tập hợp tác nhân đe dọa có khuynh hướng sử dụng các phương pháp cụ thể, nỗ lực này hoạt động tốt nhất khi được điều chỉnh phù hợp với các yếu tố cụ thể của một ngành. Nó cũng có thể rất hữu ích khi kiểm tra những mối đe dọa mới nổi vì một số yếu tố cụ thể, chẳng hạn như thông tin báo chí tiêu cực xoay quanh công ty của bạn, khiến cho công ty của bạn trở thành đích nhắm mục tiêu của những kẻ theo chủ nghĩa hacktivists.

### **Bản đồ Mối đe dọa**

*Bản đồ mối đe dọa* là dạng trình bày các cuộc tấn công theo khu vực địa lý cho thấy các gói tin đến từ đâu và đi đến đâu, như được minh họa trong [Hình 5-2](#). Những thứ này thu hút được rất nhiều sự chú ý của giới truyền thông và rất dễ nhìn, nhưng mọi người phải tiếp cận chúng một cách thận trọng. Sự quy kết là rất khó và chỉ vì một cuộc tấn công đến từ một IP ở một thành phố nhất định không có nghĩa là cuộc tấn công thực sự bắt nguồn từ đó. Cỗ máy đang tấn công bạn cũng có thể là nạn nhân, với việc kẻ tấn công đang hoạt động từ một nơi khác để làm cho việc điều tra xuyên biên giới trở nên khó khăn và tốn kém hơn.



**Hình 5-2 Ví dụ về bản đồ mối đe dọa**

### Kho lưu trữ Tập tin/Mã nguồn

Một trong những lĩnh vực tăng trưởng chính trong phát triển phần mềm trong vài thập kỷ qua là các *kho lưu trữ tập tin/mã nguồn*. Các kho lưu trữ chặng hạn như GitHub đóng vai trò như các vị trí nơi mọi người có thể hoạt động cùng nhau trên các dự án và phát triển phần mềm. Những kho lưu trữ này có thể đóng hai vai trò riêng biệt trong nguồn tin tình báo về mối đe dọa. Trước tiên, chúng có thể cung cấp một nguồn thông tin các đối thủ về cách thức phần mềm được xây dựng, mang lại cho họ một cơ hội để kiểm tra phần mềm để tìm kiếm những lỗ hổng. Nếu tổ chức của bạn sử dụng mã phần mềm từ một kho lưu trữ và bạn phổ biến nó cho thế giới (thường là vì một trong số các nhân viên của bạn là một người đóng góp), sau đó thì bạn đang cung cấp cho các đối thủ những

thông tin về cơ sở hạ tầng của bạn có thể được sử dụng để chống lại bạn. Thứ hai, bạn có thể sử dụng các nguồn giống nhau để kiểm tra năng lực của một vài trong số các công cụ mà các đối thủ của bạn sẽ sử dụng để chống lại bạn. Do đó, các kho lưu trữ mã phần mềm là không tốt không xấu khi liên quan đến nguồn tin tình báo về mối đe dọa: thay vào đó, chúng là một nguồn cân bằng cho cả hai phía.

---



**LƯU Ý** Khi bạn phát triển phần mềm trong nội bộ, việc duy trì một kho lưu trữ về nguồn gốc của mọi mô-đun, bao gồm cả các phiên bản, là điều quan trọng để truy tìm các vấn đề. Đây được gọi là định mức nguyên liệu phần mềm (software Bill Of Materials – BOM) và là điều rất quan trọng khi bạn tìm hiểu về các lỗ hổng trong mã phần mềm mà bạn đang sử dụng.

### Các Nguồn Nghiên cứu

Khi một ai đó muốn nghiên cứu về một chủ đề, một trong những thách thức là tìm kiếm những nguồn thông tin đã được kiểm duyệt về tính chân thực. Nguồn thông tin tình báo về mối đe dọa cũng vậy. Có rất nhiều nguồn thông tin, từ các nhà thầu cho đến các nhóm ngành cục bộ, từ nguồn cung cấp những lỗ hổng cho đến nguồn cung cấp mối đe dọa, từ các cuộc hội nghị cho đến các tạp chí học thuật đến các mục nhập yêu cầu bình luận (requests for comment – RFC). Những nguồn này và các nguồn khác nữa sẽ được xem xét trong phần này, nhưng hãy lưu ý rằng mỗi nguồn đều có những điểm mạnh và điểm yếu riêng, vốn có thể là điều tối quan trọng, do đó, việc sử dụng sự kết hợp thích hợp giữa các nguồn là điều quan trọng.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy chuẩn bị cho các câu hỏi yêu cầu bạn xác định sự khác biệt giữa các kiểu nguồn nghiên cứu về mối đe dọa.

### Trang Web của Nhà thầu

Mỗi nhà thầu đều muốn trở thành một đối tác có giá trị trong các vấn đề bảo mật của bạn và được chia sẻ ngân sách của bạn. Để đạt được điều đó, họ có các nhóm tiếp thị để phát triển các trang web đẹp mắt. *Những trang web của nhà thầu* này thường như chứa đầy thông tin – những thông tin được thiết kế để khiến cho bạn muốn trở thành đối tác với họ. Nhưng hãy nhớ rằng, đây chỉ là hoạt động tiếp thị - bạn cần phải tìm kiếm nguồn của họ là gì, cách thức các nguồn được quản lý như thế nào, và những tiêu chuẩn nào mà họ đang sử dụng. Điều này không có nghĩa là những tài liệu đó là xấu, chỉ là câu ngạn ngữ cổ *hãy để người mua chọn lựa* được áp dụng.

### Nguồn cung cấp Lỗi hỏng

Như đã được đề cập trong phần trước đó, chất lượng của nguồn cung cấp lỗi hỏng có thể khác nhau rất nhiều giữa các nguồn. Để đảm bảo rằng bạn có được những nguồn tốt, điều quan trọng là phải kiểm duyệt những nguồn cung cấp của bạn về một loạt các vấn đề, bao gồm nguồn của dữ liệu đó là gì, và những đặc trưng cụ thể nào được thể hiện như một phần của nguồn cấp tin. Ngoài ra, nhiều nguồn cấp tin gần như là bắt buộc đối với tin tức được đưa ra, nhưng điều đó cũng có nghĩa là bạn cần phải so sánh các mục giữa các nguồn cung cấp tin tức bởi vì hai bộ nguồn cấp dữ liệu với cùng một nguồn chung duy nhất (giả sử là NVD) thực tế không mang lại nhiều giá trị. Sử dụng nhiều nguồn cấp dữ liệu, với các nguồn và đặc điểm khác nhau, được hợp nhất thành một cơ sở dữ liệu duy nhất là con đường dẫn đến phạm vi bao phủ tốt hơn.

## Các cuộc hội nghị

Giới học thuật tiến hành việc nghiên cứu, và khi nghiên cứu có yếu tố thời hạn thì việc chờ đợi một bài báo trên tạp chí (được đề cập trong phần tiếp theo) là một vấn đề. Giải pháp cho vấn đề này là xuất bản tài liệu và trình bày nó tại một cuộc hội nghị. Điều này có hai ưu điểm: Thứ nhất, các mốc thời gian cho các bài gửi đến cuộc hội nghị ngắn hơn nhiều so với các tạp chí. Thứ hai, việc trình bày tài liệu tại hội nghị là một cách rất tốt để có được nhiều quan điểm dưới dạng phản hồi một cách nhanh chóng hơn. Nhược điểm là trừ khi phản hồi này được xem xét và được hiệu đính, hầu hết các báo cáo hội nghị đều ít được đánh giá nghiêm túc từ đồng nghiệp, vì vậy chúng cần được xử lý với một cái nhìn cởi mở về độ chính xác và khả năng áp dụng.

Một nguồn khác là các hội nghị trong ngành, tạo ra cơ hội cho mọi người từ các công ty khác nhau đến với nhau để chia sẻ thông tin về một loạt các chủ đề có liên quan. Đôi khi được tài trợ bởi chính phủ hoặc các nhóm thương mại công nghiệp, lợi thế chủ yếu của việc tham dự các hội nghị này không phải là các phiên họp, vì nội dung thường có sẵn ở nơi khác sau đó, mà là kết nối trực tiếp. Ba hội nghị an ninh lớn được tổ chức mỗi năm: hội nghị RSA ở San Francisco và hội nghị Black Hat USA và DEF CON ở Las Vegas. Mặc dù mỗi nơi có số lượng khán giả hơi khác nhau, nhưng tất cả đều lên đến hàng chục nghìn người tham dự. Lý do chính mà các chuyên gia tham dự các buổi trình diễn này là để kết nối với các chuyên gia khác và học hỏi các phương pháp mới và hữu ích mà họ có thể áp dụng sau sự kiện.

## Các Tạp chí học thuật

Một thành phần chính của học thuật là tiến hành những nghiên cứu mới - nghiên cứu đã được bình duyệt và được xuất bản trên *các tạp chí học thuật*. Tuy nhiên, các tạp chí học thuật có hai vấn đề: tính hợp thời và

khả năng ứng dụng. Việc xuất bản một bài báo trên một tạp chí học thuật có thể mất tối thiểu từ một năm đến mười tám tháng – *sau khi công việc đã hoàn thành*. Sự chậm trễ này là do sự đánh giá và chỉnh sửa của đồng nghiệp. Trong rất nhiều trường hợp, điều này có nghĩa là các nghiên cứu hàn lâm trên các tạp chí đã lỗi thời vào thời điểm nó được in ra. Hơn nữa, các học giả hiếm khi là chuyên gia trong việc ứng dụng các công nghệ mà họ nghiên cứu. Họ nhìn mọi thứ như những vấn đề lý thuyết và bỏ qua rất nhiều khía cạnh ứng dụng. Một học giả sẽ xem xét những điều như phòng thủ có chiều sâu để bảo mật một hệ thống giải quyết lỗ hổng XYZ, dựa trên lý thuyết, chứ không phải thứ có thể được thực hiện theo nghĩa thực tế. Các nhà học thuật phân giải cấu trúc một vấn đề thành các thành phần cơ bản của nó để tìm ra câu trả lời, nhưng liệu câu trả lời đó có áp dụng được trong thực tế hay không lại là một vấn đề hoàn toàn khác.

### Các Yêu cầu Bình luận

*Các Yêu cầu bình luận (RFC)* là những tập hợp các tiêu chuẩn được sử dụng để xác định cách thức mà Internet và các giao thức liên quan đến World Wide Web được thiết lập và quản lý như thế nào. Chúng miễn phí và mở công khai, và không giống như một số hạng mục liên tục phát triển như wiki, chúng được cố định về thời gian khi được viết ra. Những thay đổi đối với những tài liệu này là chính thức và được lưu ý, và nếu như một tiêu chuẩn Internet đòi hỏi sự cập nhật, một RFC mới được phác thảo và phê duyệt. Đây là những nguồn tài liệu rất hữu ích vì chúng liệt kê ra những chi tiết mà theo đó các giao thức vận hành, bao gồm cả những phương pháp có sẵn nhưng không được sử dụng một cách rộng rãi.

### Các Nhóm Ngành Cục bộ

*Các nhóm ngành cục bộ* là nguồn vô giá từ nhiều quan điểm. Đầu tiên, chúng là một nguồn thông tin thực tế rất tốt liên quan đến các mối đe

dọa, các tác nhân gây ra mối đe dọa và những gì có thể được thực hiện để bảo vệ hệ thống mạng. Thứ hai, chúng là một nguồn thông tin mạng vững chắc cho phép một người có được câu trả lời cho những câu hỏi đã được kiểm duyệt bởi những người khác cũng ở vị trí tương tự. Phần lớn an ninh mạng xoay quanh việc chia sẻ thông tin giữa các bên đáng tin cậy và việc tham gia và hoạt động tích cực trong các nhóm ngành cục bộ là một cách thích hợp để xây dựng các mối quan hệ đáng tin cậy này. Thời điểm để xây dựng những mối quan hệ này là trước khi bạn cần chúng chứ không phải khi bạn cần câu trả lời hoặc sự giúp đỡ.

### **Mạng Xã hội**

Ngày nay *Phương tiện truyền thông xã hội* đã trở nên phổ biến, với nhiều nền tảng khác nhau nhằm mục tiêu đến các phân khúc thị trường khác nhau. Vào cuối mỗi ngày, từng nền tảng này được thiết kế để người dùng có thể chia sẻ ý tưởng với những người cùng chí hướng. Ví dụ: Facebook hoặc Instagram có thể không phải là nơi tốt nhất để có các cuộc thảo luận có ý nghĩa liên quan đến thông tin về mối đe dọa, nhưng giao tiếp với các địa chỉ liên hệ trên một trang web định hướng doanh nghiệp như LinkedIn có thể sẽ phù hợp hơn. Như với tất cả các nguồn, điều quan trọng là kiểm duyệt các nguồn thông tin. Do đó, nếu các đồng nghiệp đáng tin cậy của bạn đã chọn một trong những nền tảng truyền thông xã hội và thường xuyên đi đến đó thì đó có thể là nơi bạn sẽ tìm thấy câu trả lời cho mình. Tuy nhiên, cũng như với nhiều nguồn thông tin, hãy nhớ rằng ngạn ngữ cổ *hãy để người mua chọn lựa* vẫn được áp dụng.

### **Các Nguồn cung cấp Mối đe dọa**

*Các nguồn cung cấp mối đe dọa* rất giống với các nguồn cung cấp về lỗ hổng khi bạn đánh giá chúng về mặt tiện ích như một nguồn nghiên cứu. Việc hiểu được thông tin đến từ đâu, nó đã được kiểm duyệt như thế nào, và cách nó được áp dụng cho ngành của bạn là những yếu tố rất quan

trọng. Tương tự, cần phải tồn tại nhiều nguồn cung cấp không trùng lặp vì không có một nguồn đơn lẻ nào đáp ứng được tất cả các nhu cầu.

### **Chiến thuật, Kỹ thuật và Thủ tục của Kẻ địch (TTPs)**

Từ viết tắt *TTP* được sử dụng để mô tả cách thức các tác nhân đe dọa tổ chức và điều phối những nỗ lực của chúng như thế nào. Giống như bất kỳ tổ chức nào khác, các tin tức cũng tiến hóa để sử dụng những phương pháp có thể lặp lại để có hiệu quả. Những phương pháp đó có thể được lập thành danh mục và được tìm hiểu như các hình mẫu tấn công, cho phép các biện pháp phòng thủ chuẩn bị trước được các kịch bản ứng phó. Các *TTP*, hoặc các hình mẫu được sử dụng bởi những kẻ địch là một yếu tố then chốt của một chương trình thông tin tình báo về mối đe dọa. Những nguồn thông tin khác nhau tương ứng với các *TTP* tồn tại, và điều quan trọng là tìm được một nguồn vững chắc dựa trên các nguồn có thể tìm hiểu được và phù hợp với ngành của bạn.

## Tóm tắt Chương

Chương này đề cập đến 5 chủ đề chính: các tác nhân và các mối đe dọa, các thuộc tính của các tác nhân, các véc-tơ, các nguồn thông tin tình báo về mối đe dọa và các nguồn nghiên cứu. Trong phần nói về các tác nhân và mối đe dọa, các chủ đề về APTs, mối đe dọa nội gián và các tác nhân cấp quốc-gia-nhà-nước được đề cập trước tiên, tiếp theo là những kẻ theo chủ nghĩa hacktivists, script kiddies, tổ chức tội phạm và tin tặc (bao gồm cả tin tặc mũ trắng, mũ đen và mũ xám). Phần này kết thúc với một cuộc thảo luận về CNTT bóng tối và các đối thủ cạnh tranh. Phần nói về các thuộc tính của các tác nhân đe dọa bao gồm các mối đe dọa bên trong và bên ngoài, mức độ phức tạp/khả năng, nguồn lực/kinh phí và ý định/động cơ.

Chương này sau đó chuyển sang chủ đề về véc-tơ, hoặc các lô tuyển tấn công. Phần này bao gồm các chủ đề về truy cập trực tiếp, không dây, email và các phương pháp xâm nhập chuỗi cung ứng. Phần này kết thúc với phương tiện truyền thông xã hội, phương tiện di động và véc-tơ đám mây.

Chương này đã kết thúc với các phần trình bày về các nguồn thông tin tình báo về mối đe dọa và các nguồn nghiên cứu. Phần về nguồn thông tin tình báo về mối đe dọa được mở đầu với chủ đề về thông tin tình báo nguồn mở và nguồn đóng/độc quyền, sau đó là cuộc thảo luận về cơ sở dữ liệu lỗ hổng, các trung tâm chia sẻ thông tin công khai/riêng tư và web đen như là các nguồn. Những phương pháp chỉ báo về sự xâm phạm, Chia sẻ Chỉ báo Tự động hóa và Diễn đạt Thông tin về Mỗi đe dọa có Cấu trúc/Trao đổi Thông tin tình báo Tự động hóa Đáng tin cậy cũng được trình bày. Phần nguồn thông tin tình báo về mối đe dọa đã kết thúc với phân tích dự đoán, bản đồ mối đe dọa và kho lưu trữ tập tin/mã nguồn. Phần cuối cùng của chương là kiểm tra các nguồn nghiên cứu. Chúng bao

gồm các trang web của nhà cung cấp, nguồn cung cấp lỗ hổng bảo mật, các cuộc hội nghị, tạp chí học thuật và các yêu cầu bình luận. Các yếu tố cuối cùng được trình bày là các nhóm ngành cụt bộ, phương tiện truyền thông xã hội, nguồn cấp dữ liệu về mối đe dọa và các chiến thuật, kỹ thuật và quy trình của kẻ địch.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Những nhân viên tài chính cấp cao của bạn đã bị tấn công bằng một đoạn phần mềm độc hại nhằm mục tiêu đến các báo cáo tài chính. Căn cứ vào cuộc thảo luận với một trong số những giám đốc điều hành, giờ đây bạn biết rằng đây là một cuộc tấn công kiểu spear phishing. Phần nào dưới đây là véc-tơ có khả năng được sử dụng nhất?

  - A. Đám mây
  - B. Không dây
  - C. Truy cập trực tiếp
  - D. Phương tiện di động.
2. Bạn là một người mới đối với công việc, với ngành và với thành phố. Những nguồn nào sau đây sẽ là tốt nhất để kết nối bạn với những đồng nghiệp của bạn về thông tin tình báo về mối đe dọa?

  - A. Nhà thầu
  - B. Phương tiện xã hội
  - C. Các nhóm ngành cục bộ
  - D. Nguồn cung cấp về lỗ hổng hoặc mối đe dọa.
3. Công ty của bạn gặp những tin tức xấu liên quan đến sự hỗ trợ của họ (hoặc thiếu hỗ trợ) cho một vấn đề xã hội địa phương. Loại tin tức nào sẽ có khả năng là mối đe dọa tấn công hoặc phá hoại trang web của bạn liên quan đến vấn đề này?

  - A. Tác nhân nhà nước
  - B. Hacktivist
  - C. Mũ đen

**D. Đối thủ.**

4. Việc sử dụng phân tách nhiệm vụ đúng đắn liên quan đến những người dùng có đặc quyền trên các hệ thống của bạn là một biện pháp phòng thủ chống lại kiểu tin tặc nào?
  - A. Tác nhân quốc-gia-nhà-nước
  - B. Nội gián
  - C. Tổ chức tội phạm
  - D. Tất cả những điều trên.
5. Bạn đã đọc được về một mối đe dọa mới chống lại phần mềm dễ bị tấn công. Lỗ hổng bảo mật nằm trong một thư viện Python và công ty của bạn đang sử dụng Python để phát triển rất nhiều dự án nội bộ. Đâu là nguồn thông tin tốt nhất liên quan đến mối đe dọa này?
  - A. Các kho lưu trữ tập tin/mã phần mềm
  - B. Cơ sở dữ liệu về lỗ hổng
  - C. Nguồn tin tình báo nguồn mở
  - D. Các chỉ báo xâm phạm.
6. Nhà cung cấp thông tin tình báo về mối đe dọa của bạn đang gửi ra những thông điệp khẩn cấp đề cập đến một hình thức mã phần mềm độc hại lưu-trú-trong-bộ-nhỏ mới. Mục nào có khả năng sẽ được họ chia sẻ với bạn?
  - A. Cơ sở dữ liệu về lỗ hổng
  - B. Chỉ báo xâm phạm
  - C. Web tối
  - D. Trao đổi Nguồn tình báo Thông tin Tự động hóa Đáng tin cậy (TAXII).
7. Bạn sử dụng một “đĩa vàng” để cung cấp các máy mới từ nhà cung cấp của bạn. Như một phần của quy trình ứng phó sự cố,

bạn đã khám phá ra rằng nguồn của phần mềm độc hại mà bạn nhìn thấy đến từ đĩa vàng này. Đây là một ví dụ của véc-tơ nào?

- A. Nội gián**
  - B. Truy cập trực tiếp**
  - C. Phương tiện di động**
  - D. Chuỗi cung ứng.**
- 8.** Việc hiểu được cách thức mà một kẻ tấn công hoạt động để từ đó bạn có thể phát triển một thế trận phòng thủ được hoàn thành thông qua việc sử dụng những điều nào dưới đây?
- A. Phân tích dự báo**
  - B. TTPs**
  - C. Bản đồ mối đe dọa**
  - D. Chia sẻ Chỉ báo Tự động hóa.**
- 9.** Những mục nào dưới đây mà bạn, với tư cách là người phòng thủ, phải kiểm soát liên quan đến việc sử dụng nguồn tin tình báo về mối đe dọa để bảo vệ các hệ thống của bạn?
- A. Các véc-tơ**
  - B. Các tác nhân**
  - C. Các nguồn tin tình báo về mối đe dọa**
  - D. Các thuộc tính của các tác nhân.**
- 10.** Bạn muốn có được những thông tin cụ thể về một mối đe dọa cụ thể mà bạn đã đọc được trên trình tin tức trực tuyến từ điện thoại của bạn. Những mục nào dưới đây là nguồn tốt nhất để có thông tin chi tiết?
- A. Cơ sở dữ liệu về lỗ hổng**
  - B. Nguồn tin tình báo nguồn mở**
  - C. Web tối**
  - D. Phân tích dự báo.**

## Đáp án

1. **D.** Phương tiện di động được liên kết một cách phổ biến với các cuộc tấn công kỹ thuật xã hội chẳng hạn như spear phishing.
2. **C.** Việc kết nối với các đồng nghiệp là một thuộc tính hữu ích của các nhóm ngành cục bộ.
3. **B.** Hacktivists là những tin tặc đang theo đuổi một sứ mệnh tương ứng với một nguyên nhân.
4. **D.** Phân tách nhiệm vụ được thiết kế để cung cấp những biện pháp phòng thủ chống lại những kẻ nội gián độc hại. Tuy nhiên các tác nhân quốc-gia-nhà-nước và các tổ chức tội phạm có những nguồn lực và khả năng để xâm nhập các tài khoản và chiếm được quyền truy cập bên trong. Không có các tài khoản bên ngoài, do đó khi đã có một tin tặc được cấp nguồn-lực-tốt, họ sẽ có những quyền hạn tương xứng với một kẻ nội gián.
5. **A.** Các kho lưu trữ tập tin/mã phần mềm là một đáp án chính xác bởi vì mã phần mềm mà bạn đề cập đến là được phát triển trong nội bộ, do đó, nó sẽ không xuất hiện trong các cơ sở dữ liệu thương mại hoặc các nguồn khác.
6. **B.** Một chỉ báo xâm phạm (IoC) cung cấp những chi tiết liên quan đến cách thức một người có thể tìm được phần mềm độc hại đang hoạt động trên một hệ thống.
7. **D.** Đây là một véc-tơ chuỗi cung ứng. Mặc dù công việc được thực hiện trong nội bộ nhưng chuỗi cung ứng trải dài từ từng bộ phận đến hệ thống đang hoạt động và bạn đã bổ sung thêm phần mềm cuối cùng để tạo ra hệ thống đang hoạt động, vì vậy nhóm của bạn là một phần của chuỗi cung ứng.
8. **B.** Các chiến thuật, kỹ thuật và quy trình (TTP) của địch thủ cung cấp thông tin chi tiết về cách thức hoạt động của địch thủ.

- 9. A.** Các véc-tơ là câu trả lời đúng vì đây là mục duy nhất bạn có quyền kiểm soát trực tiếp. Các mục khác là vẫn đề thực sự, chỉ không phải là vẫn đề mà bạn có bất kỳ biện pháp kiểm soát trực tiếp nào.
- 10. B.** Thông tin tình báo nguồn mở là câu trả lời tốt nhất. Bởi vì bạn đang tìm kiếm thông tin về mối đe dọa và điều này sẽ loại bỏ thông tin về lỗ hổng bảo mật như một câu trả lời. Web tối có thể có hoặc có thể không có thông tin, và bạn sẽ phải tìm nó, và phân tích dự đoán cần những thông tin bạn tìm kiếm để hoạt động.

## Chương 6      Các Lỗ hổng

---

### Các Lỗ hổng

Trong chương này, bạn sẽ:

- Tìm hiểu về những mối quan tâm về bảo mật khác nhau tương ứng với các lỗ hổng,
  - Tìm hiểu về một loạt các lỗ hổng hệ thống.
- 

Các hệ thống của doanh nghiệp được cấu thành từ rất nhiều bộ phận khác nhau, cùng với rất nhiều công nghệ và những phần tử đa dạng có thể kém hoàn hảo. Hầu như bất cứ thứ gì được thiết kế và xây dựng đều sẽ có những điểm yếu và những lỗ hổng. Việc hiểu được nơi mà những điểm yếu và lỗ hổng này tồn tại, và cách để quản lý bảo mật của doanh nghiệp bất chấp chúng là gì, là một yếu tố cực kỳ quan trọng của một chương trình bảo mật. Chương này xem xét các loại và ảnh hưởng của các lỗ hổng khác nhau trong một doanh nghiệp.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 1.6 của kỳ thi CompTIA Security+: Giải nghĩa những mối quan tâm về bảo mật tương ứng với các kiểu lỗ hổng khác nhau.

## Các Lỗ hổng Dựa-trên-Đám-mây so với Tại-Cơ-sở

Điện toán đám mây đã được các chuyên gia mô tả là điện toán trên máy tính của một ai đó khác, và ở một mức độ nào đó, tuyên bố này là đúng. Vì các lỗ hổng tồn tại trong mọi hệ thống, do đó bất kể một hệ thống là *trên đám mây* hay *tại chỗ*, nó vẫn sẽ luôn có những lỗ hổng tiềm ẩn. Với những lỗ hổng của các hệ thống tại-chỗ, doanh nghiệp có quyền truy cập không bị giới hạn vào các phần tử cơ sở hạ tầng, khiến cho việc khám phá và khắc phục các lỗ hổng trở thành một vấn đề được xác định bởi phạm vi và nguồn lực. Với [điện toán] đám mây, tính kinh tế của quy mô và các môi trường được tiêu chuẩn hóa mang lại cho các nhà cung cấp đám mây một lợi thế về mặt phạm vi và nguồn lực của phương trình. Điều còn thiếu sót trong quản lý lỗ hổng từ quan điểm của doanh nghiệp là tính minh bạch trong chính bản thân yếu tố cơ sở hạ tầng, vì điều này nằm bên dưới tầm quan sát của nhà cung cấp đám mây.



## MÁCH NƯỚC CHO KỲ THI

Dữ liệu có thể được lưu trữ tại chỗ một cách cục bộ hoặc từ xa trên đám mây. Điều quan trọng cần nhớ là bất kể dữ liệu được lưu trữ ở đâu, vẫn luôn luôn tồn tại những lỗ hổng tiềm ẩn.

## Zero Day

*Zero day* là một thuật ngữ được sử dụng để xác định những lỗ hổng chỉ mới được khám phá và vẫn chưa được giải quyết bởi một bản vá lỗi. Hầu hết các lỗ hổng đều tồn tại ở một trạng thái không xác định cho đến khi được phát hiện bởi một nhà nghiên cứu hoặc nhà phát triển. Nếu một nhà nghiên cứu hoặc nhà phát triển phát hiện ra lỗ hổng bảo mật nhưng không chia sẻ thông tin thì lỗ hổng này có thể bị khai thác mà nhà cung cấp không có khả năng sửa chữa nó vì đối mọi kiến thức thực tế, vẫn đề là không xác định ngoại trừ người tìm thấy nó. Tính từ thời điểm được phát

hiện cho đến khi có bản sửa lỗi hoặc bản vá lỗi, lỗ hổng bảo mật được gọi là “zero day”, chỉ ra cho thấy rằng nó vẫn chưa được giải quyết. Điều đáng sợ nhất của mối đe dọa zero day là yếu tố không xác định - khả năng và ảnh hưởng của nó đối với rủi ro là không xác định vì nó chưa Pudd được biết đến. Mặc dù không có các bản vá lỗi cho các lỗ hổng zero-day nhưng bạn vẫn có thể sử dụng các biện pháp kiểm soát bù đắp để giảm thiểu rủi ro. Các biện pháp kiểm soát bảo mật được đề cập sâu trong Chương 31, “Các biện pháp kiểm soát bảo mật”.



**MÁCH NƯỚC CHO KỲ THI** Những mối đe dọa zero-day đã trở thành một chủ đề rất phổ biến trên các bản tin và có khả năng là mục tiêu cho các câu hỏi trong đề thi. Hãy lưu ý rằng các biện pháp phòng thủ vẫn tồn tại, chẳng hạn như các biện pháp kiểm soát bù trừ, vốn là các biện pháp kiểm soát làm giảm nhẹ rủi ro một cách gián tiếp, ví dụ, một biện pháp kiểm soát bù trừ có thể ngăn chặn lộ tuyến của lỗ hổng thay vì trực tiếp giải quyết lỗ hổng đó.

### **Thiết lập cấu hình Kém**

Hầu hết các hệ thống đều có những tùy chọn cấu hình quan trọng mà các quản trị viên có thể điều chỉnh để cho phép hoặc vô hiệu hóa chức năng tùy thuộc và việc sử dụng. Khi một hệ thống bị định cấu hình sai hoặc *cấu hình yếu*, nó có thể không đạt được toàn bộ hiệu suất hoặc các mục tiêu bảo mật được mong muốn. Việc thiết lập cấu hình máy chủ cơ sở dữ liệu để xây dựng một bản sao hoàn chỉnh của tất cả các hành động như một hệ thống sao lưu có thể dẫn đến hệ thống bị sa lầy và không có khả năng phản hồi thích hợp khi mức sử dụng cao. Một cách tương tự, các tùy chọn cũ, chẳng hạn như hỗ trợ các giao thức kế thừa cũng có thể dẫn đến các lỗ hổng. Việc định cấu hình sai cũng có thể do thiếu sót, chẳng

hạn như khi quản trị viên không thay đổi thông tin xác thực mặc định, tương đương với việc hoàn toàn không có thông tin xác thực nào, do đó khiến cho hệ thống trở nên dễ bị tấn công. Dạng lỗ hổng này cung cấp một phương tiện để kẻ tấn công xâm nhập hoặc nâng cao cấp đặc quyền của chúng và bởi vì điều này có thể xảy ra trên các thành phần có phạm vi kiểm soát rất rộng, chẳng hạn như bộ định tuyến và thiết bị chuyển mạch, trong một số trường hợp, kẻ tấn công có thể giành được toàn bộ quyền sở hữu của một doanh nghiệp.

### **Quyền Mở**

*Quyền* là một thuật ngữ được sử dụng để mô tả phạm vi của các hoạt động được chấp thuận đối với một đối tượng theo một tác nhân trong một hệ thống. Việc có được những quyền hạn được cấu hình một cách đúng đắn là một trong những biện pháp phòng thủ có thể được sử dụng trong doanh nghiệp. Việc quản lý các quyền có thể là một công việc tẻ nhạt, và khi quy mô của doanh nghiệp tăng trưởng, quy mô của các quyền đòi hỏi phải được tự động hóa để quản lý. Khi các quyền không được thiết lập một cách đúng đắn, điều kiện *quyền mở* sẽ tồn tại. Rủi ro tương ứng với một quyền mở là độc lập với bối cảnh, vì đối với một số mục, quyền truy cập trái phép dẫn tới ít hoặc không có rủi ro, trong khi đối với các hệ thống khác, điều đó có thể trở thành một thảm họa. Lỗ hổng quyền mở tương đương với việc không có quyền kiểm soát truy cập đối với một hạng mục, và điều này cần phải được giám sát một cách thích hợp với rủi ro tương đối của phần tử đó trong doanh nghiệp.

### **Tài khoản Root Không bảo mật**

*Tài khoản root không bảo mật* giống như việc bỏ lại chìa khóa chính của doanh nghiệp bên ngoài phạm vi kiểm soát. Các tài khoản root có quyền truy cập tới mọi thứ và có khả năng thực hiện hầu như bất kỳ hành động nào trên một hệ thống mạng. Mọi tài khoản root nên được giám sát, và

mọi quyền truy cập phải được xác minh là chính xác. Một phương pháp bảo vệ các tài khoản có giá trị cao chẳng hạn như các tài khoản root là thông qua các vòm kiểm soát truy cập, nơi mà mọi thông tin đăng nhập được kiểm tra trước khi sử dụng. Điều này ngăn chặn hoạt động trái phép thông qua việc sử dụng những tài khoản này.

---



**MÁCH NƯỚC CHO KỲ THI** Những cấu hình mạnh mẽ bao gồm các tài khoản root (Linux) và Administrator (Windows) được bảo mật. Nếu không bảo mật những tài khoản này, bất cứ gì mà chúng kết nối đến, bao gồm các tiến trình và các dịch vụ, sẽ bị phát lộ những lỗ hổng.

### Các lỗi

Các *lỗi* là tình trạng mà một điều gì đó đã bị sai. Mọi hệ thống đều sẽ gặp lỗi và chìa khóa để quản lý tình trạng này là thiết lập bẫy lỗi và biện pháp ứng phó lỗi. Cách thức một hệ thống xử lý lỗi là tất cả, bởi vì các lỗi chưa được xử lý cuối cùng cũng sẽ được xử lý ở một số cấp độ nào đó, và hệ thống càng lên cao thì lỗi càng ít có khả năng được xử lý một cách chính xác. Một trong những điểm yếu lớn nhất bị khai thác bởi những kẻ tấn công là xác nhận đầu vào không đúng cách. Cho dù là chổng lại một đầu vào chương trình, API hay bất kỳ giao diện nào khác, việc chèn những thông tin xấu gây ra lỗi và buộc chương trình ở một trạng thái hoạt động không bình thường có thể dẫn đến lỗ hổng có thể bị khai thác. Việc bẫy và xử lý lỗi có thể làm giảm xác suất lỗi trở nên có thể khai thác được.

Các lỗi nên được bẫy bởi chương trình và các tập tin nhật ký thích hợp đã được tạo ra. Ví dụ: nhật ký máy chủ web bao gồm các nhật ký lỗi phổ biến, nhật ký tùy chỉnh và nhật ký W3C. Nhật ký W3C là nhật ký máy chủ web tập trung vào việc ghi lại các sự kiện liên quan đến web cụ thể. Nhật

ký Hệ thống Windows ghi lại các thông báo lỗi hệ điều hành. Windows có thể được cấu hình để ghi lại các bản ghi thành công và thất bại của các lần đăng nhập và các sự kiện đã được kiểm tra khác. Nhật ký ứng dụng Windows ghi lại các sự kiện liên quan đến các ứng dụng hệ thống cục bộ trên từng máy tính.

## Mã hóa Kém

Các lỗi mã hóa xuất phát từ một số nguyên nhân phổ biến. Một sai lầm điển hình là việc chọn phát triển thuật toán mật mã của riêng bạn. Việc phát triển một thuật toán mã hóa an toàn không hề là một nhiệm vụ dễ dàng và ngay cả khi nó được các chuyên gia cỗ gắng, các điểm yếu vẫn có thể bị phát hiện khiếu cho thuật toán trở nên không thể sử dụng được. Các thuật toán mã hóa chỉ trở nên đáng tin cậy sau nhiều năm giám sát và đẩy lùi các cuộc tấn công, vì vậy bất kỳ thuật toán mới nào cũng sẽ phải mất rất nhiều năm để tham gia vào tập hợp đáng tin cậy. Thay vào đó, nếu bạn quyết định dựa vào các thuật toán bí mật, hãy cảnh giác rằng các thuật toán bí mật hoặc độc quyền chưa bao giờ cung cấp được mức độ bảo vệ mong muốn. Một sai lầm tương tự khi cỗ gắng phát triển thuật toán mã hóa của riêng bạn là cỗ gắng viết về cách triển khai của riêng bạn về một thuật toán mã hóa đã biết. Các lỗi trong việc triển khai mã hóa là phổ biến và dẫn đến việc triển khai yếu kém các thuật toán bảo mật dễ bị bỏ qua. Để tránh rơi vào tình trạng tạo ra một bản triển khai kém cỏi, thay vào đó, hãy sử dụng một thư viện mật mã đã được kiểm chứng và kiểm duyệt.

Nguyên nhân chính thứ hai của sự yếu kém về mã hóa, hoặc *mã hóa yếu*, là việc sử dụng các thuật toán mã hóa yếu hoặc không còn được sử dụng nữa. Bộ mã hóa yếu là những bộ [mã hóa] mà trước đây đã từng được coi là bảo mật nhưng giờ đây không còn được coi là bảo mật nữa. Vì khả năng sử dụng phần cứng nhanh hơn bao giờ hết đã cho phép những kẻ

tấn công đánh bại một số phương pháp mã hóa, các phương pháp cũ hơn và yếu hơn đã được thay thế bằng các phương pháp mới hơn và mạnh hơn. Việc không sử dụng các phương pháp mới hơn và mạnh hơn có thể dẫn đến điểm yếu. Một ví dụ phổ biến về điều này là SSL, tất cả các phiên bản của SSL hiện được coi là không được sử dụng nữa và không nên được sử dụng. Mọi người nên chuyển hệ thống của họ sang các giải pháp dựa trên TLS.

Tác động của các lỗi mã hóa khá dễ hiểu: bất kỳ biện pháp bảo vệ nào đã được cung cấp sẽ không còn ở đó nữa, ngay cả khi nó cần thiết cho sự bảo mật của hệ thống.

### **Các Giao thức không Bảo mật**

Một cấu hình kém quan trọng khác cần đề phòng trong doanh nghiệp là *các giao thức không bảo mật*. Một trong những giao thức phổ biến nhất đã được sử dụng, HTTP, về bản chất của nó là không bảo mật. Việc bổ sung TLS cho HTTP, sử dụng HTTPS, là một thay đổi cấu hình đơn giản nên được thực thi ở mọi nơi. Những còn mọi ngăn xếp giao thức khác đã được tích hợp sẵn trong Hệ điều hành và chỉ đang đợi để trở thành một lỗ hổng, chẳng hạn như FTP, Telnet, và SNMP thì sao? Các giao thức và dịch vụ truyền thông được bảo mật không đúng cách và thông tin đăng nhập không an toàn làm tăng nguy cơ truy cập trái phép vào doanh nghiệp. Các thiết bị cơ sở hạ tầng mạng có thể bao gồm bộ định tuyến, bộ chuyển mạch, điểm truy cập, cửa ngõ, proxy và tường lửa. Khi hệ thống cơ sở hạ tầng đã được triển khai, các thiết bị này vẫn tiếp tục trực tuyến trong nhiều năm và nhiều thiết bị trong số đó hiếm khi được khởi động lại, được vá lỗi hoặc nâng cấp.

### **Các Thiết lập Mặc định**

Các thiết lập mặc định có thể là một rủi ro bảo mật trừ khi chúng được tạo ra với sự lưu tâm về bảo mật. Các Hệ điều hành cũ hơn được sử dụng

với tất cả mọi thứ được kích hoạt theo mặc định. Những phiên bản cũ hơn của một số hệ thống có các tài khoản quản trị viên được ẩn giấu, và Máy chủ SQL của Microsoft theo mặc định có mật khẩu cho tài khoản quản trị viên được để trống. Ngày nay, hầu hết các nhà cung cấp đã loại bỏ những vấn đề này, thiết lập các giá trị cài đặt mặc định với sự lưu tâm về bảo mật. Tuy nhiên, khi bạn khởi tạo một thứ gì đó trong doanh nghiệp của mình, thì nó sẽ thuộc về bạn. Do đó, bạn chỉ nên thiết lập cài đặt cho những gì bạn cần và chỉ những gì bạn cần, và bạn nên tạo những cài đặt này làm đường cơ sở cấu hình mặc định. Bằng cách này, các cài đặt và hàm ý bảo mật của chúng được hiểu rõ. Việc không thực hiện các bước này để lại quá nhiều ẩn số trong một doanh nghiệp.

### Các Cổng và Dịch vụ Mở

Đối với một dịch vụ, để phản hồi lại một yêu cầu, một cổng của nó phải được mở ra để giao tiếp. Việc có một *cổng mở* giống như việc có những cánh cửa trong tòa nhà. Ngay cả hầm ngân hàng cũng có một cánh cửa. Việc có quá nhiều *dịch vụ mở* chỉ dẫn đến những đường dẫn đi vào các hệ thống của bạn cần phải được bảo vệ. Việc vô hiệu hóa các dịch vụ không cần thiết, đóng các cổng, và sử dụng tường lửa để ngăn chặn những giao tiếp ngoại trừ trên các kênh đã được phê duyệt sẽ tạo ra những rào cản để truy nhập bởi những người trái phép. Rất nhiều dịch vụ chạy với các đặc quyền được nâng cao theo mặc định, và phần mềm độc hại đã lợi dụng điều này. Các chuyên gia bảo mật nên thực hiện mọi nỗ lực để kiểm tra các dịch vụ và vô hiệu hóa bất kỳ thứ gì không cần thiết.



### MÁCH NƯỚC CHO KỲ THI

Những thiết lập cấu hình kém làm gia tăng một cách đáng kể khả năng tấn công và xâm nhập thành công. Hãy

thực hiện mọi nỗ lực để loại bỏ các ứng dụng không cần thiết, vô hiệu hóa bất kỳ dịch vụ nào không cần thiết, thay đổi các tên người dùng và mật khẩu tài khoản mặc định, và đóng hoặc bảo mật các cổng không cần thiết.

### **Những Rủi ro Bên-thứ-ba**

Môi trường điện toán doanh nghiệp toàn bộ có liên quan đến các bên-thứ-ba, và những rủi ro của họ cũng trở thành rủi ro của doanh nghiệp. Những *rủi ro bên-thứ-ba* phổ biến thường bị xem nhẹ là những vấn đề về quản lý nhà thầu, tích hợp hệ thống, và thiếu sự hỗ trợ của nhà thầu. Tất cả những điều này đều liên quan đến thực tế là khi bạn chọn một nhà thầu như một phần của giải pháp của doanh nghiệp của bạn thì điều đó hoàn toàn hợp lý. Nhưng theo thời gian, doanh nghiệp thay đổi, nhà cung cấp thay đổi, năng lực và nhu cầu thay đổi, và những gì đã từng là phù hợp có thể không còn phù hợp trong tương lai nữa. Việc giữ cho các hệ thống được tối ưu hóa không phải là một nhiệm vụ đơn giản và nhiều khi các điều kiện sau này sẽ dẫn đến các quyết định khác nhau có liên quan đến các bên-thứ-ba và rủi ro của họ.

Các chuỗi cung ứng hiếm khi dừng lại ở bước tiếp theo, và trong công nghệ, các chuỗi đó có thể rất dài và phức tạp. Với những chuỗi cung ứng này, rủi ro đến từ các yếu tố như phát triển mã phần mềm được thuê ngoài, bảo trì hệ thống và, trong thế giới của các hệ thống đám mây, lưu trữ dữ liệu trên máy tính của bên khác.

Đối với phần mềm của bên-thứ-ba đang hoạt động trong doanh nghiệp, điều quan trọng là phải có một bản kiểm kê rằng phần mềm đó là gì, theo phiên bản và nơi mà nó được sử dụng. Điều này hỗ trợ cho nhóm bảo mật trong việc giám sát các nguồn lỗ hổng thông qua các nguồn như cơ sở dữ liệu Các Lỗ hổng Phổ biến và Mức độ phơi nhiễm (CVE). Danh sách này

cũng sẽ hỗ trợ cho việc xác định mức độ rủi ro khi phần mềm hết tuổi thọ hoặc kết thúc vòng đời sử dụng.

Các vấn đề bổ sung liên-quan-đến-chính-sách tương ứng với quản lý rủi ro bên-thứ-ba được đề cập chi tiết ở phần sau trong Chương 33, "Các Chính sách Tổ chức".



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng những mối quan tâm về chuỗi cung ứng và sự hỗ trợ của nhà cung cấp là những mối quan tâm liên quan trực tiếp đến những rủi ro và quản lý bên-thứ-ba.

### Quản lý Nhà thầu

Một nhà thầu hoặc nhà cung cấp là một công ty có một mối quan hệ kinh doanh với doanh nghiệp. Trong hầu hết các trường hợp, mối quan hệ này trong doanh nghiệp là một mối quan hệ của rất nhiều khách hàng. Mặc dù tiếng nói từ khách hàng là rất quan trọng nhưng tiếng nói của một khách hàng đơn lẻ hầu như chưa bao giờ được lắng nghe. Thách thức của *quản lý nhà thầu* là một trong những thách thức trong việc xác định nhu cầu của riêng một ai đó và sau đó tìm kiếm các nhà cung cấp để đề xuất giải pháp giá trị tốt nhất cho những nhu cầu đó. Đây không chỉ đơn giản là lựa chọn và mua một sản phẩm cho hầu hết các thành phần trong doanh nghiệp, các vấn đề về hỗ trợ, vòng đời hệ thống và sự bảo trì đều đóng một vai trò trong giá trị lâu dài của một nhà cung cấp và các sản phẩm của họ. Việc lập bản đồ các nhu cầu và quản lý vấn đề đa chiều của việc xác định mối quan hệ phù hợp nhất và sau đó duy trì mối quan hệ đó theo thời gian là điều thiết yếu trong môi trường doanh nghiệp luôn luôn thay đổi ngày nay.

## Tích hợp hệ thống

Các doanh nghiệp được cấu thành từ rất nhiều các thành phần khác nhau hoạt động cùng nhau để xử lý những thông tin chảy qua doanh nghiệp. Các thành phần khác nhau có những chức năng khác nhau, nhưng cuối cùng thì chúng hoạt động cùng với nhau. Việc *tích hợp hệ thống* là sự kết nối những thành phần này, mỗi thành phần đại diện cho một phần của một hệ thống, thành một đơn vị chức năng hoàn chỉnh. Tích hợp hệ thống là một lĩnh vực nơi mà những lỗ hổng có thể tồn tại, vì các phần có thể có những khoảng cách trong sự tích hợp hoặc năng lực của chúng không biểu thị như đặc tả kỹ thuật được mong muốn. Tích hợp hệ thống được kết hợp với quản lý cấu hình vì các cấu hình của các phần riêng lẻ có thể tác động đến cách thức toàn bộ hệ thống hoạt động. Bất kỳ sai lệch nào so với đặc tả kỹ thuật thiết kế đều thể hiện cho một cơ hội đối với rủi ro.

## Thiếu Hỗ trợ của Nhà cung cấp

*Thiếu hỗ trợ của nhà cung cấp* có thể trở thành một vấn đề ở vài cấp độ khác nhau. Kịch bản được quan sát thấy nhiều nhất là khi nhà sản xuất ban đầu của một hạng mục, có thể là phần cứng hoặc phần mềm, không còn cung cấp sự hỗ trợ nữa. Khi một hạng mục hết thời gian sử dụng (EOL) từ quan điểm của nhà sản xuất ban đầu, điều này biểu thị cho tuổi thọ cuối cùng của hạng mục đó trong hầu hết mọi trường hợp. Sau khi nhà sản xuất ngừng hỗ trợ cho một hạng mục, các tùy chọn để giữ cho nó được cập nhật cùng với các bản vá và sửa lỗi cũng hiếm khi tiếp tục tồn tại. Tại thời điểm này, một tổ chức đang tiếp tục sử dụng sản phẩm sẽ gánh chịu tất cả những rủi ro tương ứng với những vấn đề được khám phá ra sau khi sản phẩm đã ở trạng thái EOL, và các phương án để giải quyết những rủi ro này bị giới hạn ở những biện pháp kiểm soát bù trừ.



**MÁCH NƯỚC CHO KỲ THI** Đừng nhầm lẫn! *Hết hạn sử dụng (End of life – EOL)* là thuật ngữ được sử dụng để chứng tỏ rằng một thứ gì đó đã đến hạn của “vòng đời sử dụng” của nó. *Kết thúc vòng đời dịch vụ (End of service life – EOSL)* hoặc *hết hạn hỗ trợ* là khi nhà sản xuất ngừng bán một mặt hàng nào đó. Trong hầu hết trường hợp, nhà sản xuất không còn cung cấp các dịch vụ bảo trì hoặc các bản cập nhật nữa.

Một kịch bản khác mà theo đó, sự thiếu hỗ trợ của nhà cung cấp phát sinh là khi hệ thống đang đề cập được triển khai bởi một nhà thầu bên-thứ-ba và nhà thầu đó hoặc là không còn hỗ trợ cho cấu hình hoặc không còn kinh doanh nữa. Công nghệ nền tảng cơ bản có thể vẫn được các nhà sản xuất ban đầu hỗ trợ, nhưng việc thiếu hỗ trợ cho phần mềm trung gian do nhà triển khai bên-thứ-ba cung cấp đặt ra câu hỏi rằng liệu các sản phẩm cơ bản có thể được cập nhật hoặc được vá lỗi hay không. Điều này đặt gánh nặng kiểm tra lên người dùng cuối và trong nhiều trường hợp, người dùng cuối không có đủ kiến thức hoặc kỹ năng cần thiết để tiến hành kiểm tra hồi quy một cách kỹ lưỡng.



**MÁCH NƯỚC CHO KỲ THI** Một hệ thống có thể có nhiều lỗ hổng liên quan đến tuổi đời của nó. Dù cho hệ thống được cấu thành từ các bộ phận cũ, hoặc trong một hệ thống được nhúng, hoặc trở thành một hệ thống kế thừa hết-hạn-sử-dụng, việc thiếu hỗ trợ của nhà cung cấp có thể dẫn đến việc chủ sở hữu không đủ khả năng để giải quyết rất nhiều vấn đề mới được khám phá sau này.

## **Chuỗi Cung ứng**

Rủi ro *Chuỗi cung ứng* là do các lỗ hổng nằm trong phạm vi chuỗi cung ứng. Bất kể những lỗ hổng đó là trong bản thân chuỗi cung ứng thực tế hoặc trong một sản phẩm từ một bên-thứ-ba, kết quả là như nhau – một mức độ rủi ro được gia tăng. Như chúng ta đã thấy trong năm 2020 do kết quả của một dịch bệnh, các chuỗi cung ứng toàn cầu có thể bị phá vỡ bởi các sự kiện bên ngoài mà sau đó đã gây ra các vấn đề cho các công ty phụ thuộc hoàn toàn vào chức năng chuỗi cung ứng. Việc trì hoãn sự ra mắt sản phẩm, các bản cập nhật và các cột mốc thời gian quan trọng tất cả đều có thể diễn ra khi các bộ phận, thành phần hoặc phần tử cấu thành phần mềm không được cung cấp đúng hạn.



### **MÁCH NƯỚC CHO KỲ THI**

Một cuộc tấn công vào chuỗi cung ứng thường diễn ra tại liên kết bảo mật yếu nhất trong chuỗi cung ứng, và đây là điều phổ biến trong tiến trình sản xuất hoặc thậm chí trong giai đoạn bàn giao sản phẩm.

### **Phát triển Mã nguồn được Thuê ngoài**

Mã nguồn phần mềm có thể là một trong những nguồn lỗ hổng và rủi ro lớn nhất trong một doanh nghiệp. Mã phần mềm được nhúng vào rất nhiều khía cạnh của doanh nghiệp — từ thiết bị đến các quy trình kinh doanh, từ các ứng dụng giúp mọi thứ vận hành đến cơ sở hạ tầng mà tất cả đều hoạt động trên đó. Mã phần mềm là chất keo kết dính tất cả lại với nhau. Tuy nhiên, khi mã bị chôn vùi trong các quy trình và mã đó được phát triển bởi một bên-thứ-ba, thường sử dụng các đoạn mã nguồn của bên-thứ-ba, thì chuỗi rủi ro sẽ trở nên dài và rất khó quản lý. Rủi ro không chỉ nằm ở thực tế là mã phần mềm được thuê ngoài, mà còn ở thực tế là tính minh bạch và kiểm soát đối với những rủi ro này trở nên khó quản lý hơn với mỗi bước rời khỏi nguồn.

Việc tạo ra mã phần mềm có thể bảo trì và an toàn không phải là một nhiệm vụ đơn giản. Điều quan trọng là phải có các điều kiện trong hợp đồng đòi hỏi áp dụng các biện pháp phát triển thích hợp cho mã nguồn của bên-thứ-ba, bao gồm quyền kiểm tra và xác minh chức năng bảo mật. Các mục như cổng hậu, dù cho là được đặt một cách cẩn thận hoặc bị bỏ qua trong quá trình kiểm nghiệm, thường yêu cầu quyền truy cập vào mã nguồn để tìm và xóa. Việc đảm bảo rằng các nhà phát triển bên-thứ-ba có được các phương pháp thực tiễn lập trình an toàn phù hợp và việc mã của họ được xem xét bởi những người kiểm tra độc lập và đặt trong giao kèo để lưu giữ an toàn được coi là những thực tiễn tốt nhất.

### **Lưu trữ Dữ liệu**

*Lưu trữ dữ liệu* là một khía cạnh quan trọng của mọi doanh nghiệp, và nó thường bị phân tán trong toàn bộ doanh nghiệp với các dung lượng và cấu hình khác nhau. Nếu tất cả dữ liệu đều ở một vị trí duy nhất thì việc quản lý lưu trữ dữ liệu, bao gồm các chức năng sao lưu và phục hồi, sẽ rất dễ quản lý. Do việc lưu trữ dữ liệu được phân tán trong toàn bộ doanh nghiệp thành nhiều phân vùng với các yêu cầu và mức độ quan trọng khác nhau, việc quản lý lưu trữ dữ liệu trở nên khó khăn hơn nhiều. Việc đảm bảo các biện pháp kiểm soát truy cập chính xác và các biện pháp bảo vệ bảo mật, chẳng hạn như sao lưu, là điều quan trọng đối với tất cả các kho lưu trữ dữ liệu và khi các lỗ hổng trong những biện pháp kiểm soát này xuất hiện, điều này sẽ tạo ra các lỗ hổng bảo mật. Nếu kẻ tấn công có thể thao túng kho dữ liệu thì chúng có thể tác động đến hoạt động của doanh nghiệp. Để đảm bảo tất cả dữ liệu được bảo vệ để không trở thành lỗ hổng bảo mật đối với hệ thống, việc có được một chính sách lưu trữ dữ liệu được tiêu chuẩn hóa và danh sách kiểm tra là một thông lệ tốt trong doanh nghiệp. Các phần tử có thể thay đổi dựa trên mức độ quan trọng của kho dữ liệu, nhưng việc tuân theo một quy trình tiêu

chuẩn sẽ làm giảm thiểu nguy cơ tồn tại các lỗ hổng do giám sát hoặc sai sót.

### **Quản lý Bản vá Kém hoặc Không thích hợp**

Mỗi hệ thống đều cần những bản vá lỗi định kỳ vì các lỗi và lỗ hổng được phát hiện và các nhà cung cấp phát hành các bản sửa lỗi phần mềm cho các lỗ hổng này. Một trong những điểm thực tế quan trọng khi tiến hành vá lỗi là một khi nhà cung cấp vá lỗi phần mềm của họ, tin tức có thể thiết kế ngược lại lỗ hổng bảo mật từ bản vá. Do đó, một khi bản vá lỗi được phát hành, những kẻ tấn công tìm hiểu nơi để tấn công. Để quản lý những rủi ro liên quan đến các lỗ hổng quản lý bản vá lỗi, điều quan trọng là phải thiết lập nên một chương trình quản lý bản vá lỗi mạnh mẽ bao gồm tất cả các hệ thống và tất cả phần mềm. Tài liệu về các lỗi bảo mật có đầy đủ các ví dụ trong đó việc bỏ sót một hoặc hai hệ thống là tất cả những gì một kẻ tấn công cần để xâm nhập vào hệ thống. Việc có một hệ thống *quản lý bản vá không phù hợp yếu kém* là một lời mời mở để khai thác các lỗ hổng. Điều này khiến cho việc quản lý bản vá trở thành một trong những biện pháp kiểm soát bảo mật thiết yếu và là một trong những nơi không có lý do gì để giải thích tại sao nó đã không được triển khai.

Để giảm thiểu những rủi ro liên quan đến việc áp dụng các bản vá cho các hệ thống sản xuất, chúng tôi khuyến cáo rằng quy trình kiểm soát thay đổi của doanh nghiệp nên được sử dụng. Bởi vì các bản vá có thể nhạy cảm về mặt thời gian nên điều quan trọng là phải xác định được khoảng thời gian khi các bản vá phải được cài đặt cũng như một phương tiện được tự động hóa để xác định những bản vá nào cần thiết, chúng được cần đến ở đâu và trạng thái của mức bản vá hiện tại theo vị trí mục tiêu.

## Firmware

*Firmware* chỉ là một hình thức khác của phần mềm với một sự khác biệt đáng chú ý: nó được lưu trữ trong phần cứng để có mặt khi hệ thống khởi động. Tuy nhiên, nó vẫn là phần mềm, với tất cả các quan niệm trước đây về phần mềm – các lỗi, lỗ hổng bảo mật, yêu cầu vá lỗi, cập nhật, v.v... Với firmware là một phần của chính bản thân hệ thống, luôn hiện diện, nên thường bị bỏ sót khi xem xét cách thức giữ cho phần mềm được cập nhật. Điều này cũng xảy ra đối với các nhà sản xuất. Nếu bạn đang xem xét một hệ thống có firmware, các câu hỏi hợp lý cần phải được đặt ra trong quá trình nghiên cứu của bạn trước khi lựa chọn bao gồm: Firmware đã được cập nhật như thế nào? Tần suất như thế nào? Và các bản cập nhật được phân phối như thế nào? Vòng đời, các lỗ hổng và các vấn đề bảo trì liên quan đến firmware phản ánh những vấn đề của phần mềm. Việc vá lỗi firmware là một vấn đề thường-bị-bỏ-quá và điều này có thể dẫn đến các lỗ hổng bảo mật, đặc biệt là do tuổi thọ điển hình của một số thiết bị.



## MÁCH NƯỚC CHO KỲ THI

Các bản cập nhật và vá lỗi được sử dụng để đảm bảo phần mềm và firmware được cập nhật và được bảo vệ. Các nhà sản xuất phần cứng thường cung cấp các bản cập nhật dành cho firmware, và trách nhiệm của tổ chức là đảm bảo các bản cập nhật firmware được áp dụng.

## Hệ điều hành (OS)

Quản lý vá lỗi *Hệ điều hành (OS)* đã từng là một việc lặt vặt cách đây vài năm, với các bản vá được cập nhật một cách liên tục theo thời gian, mỗi bản vá đều cần đến sự can thiệp thủ công. Ngày nay, các hệ điều hành

lớn có thể tự mình vá lỗi, và với một chút tự động hóa, việc theo dõi và quản lý các bản vá đã trở nên rất dễ dàng. Chỉ có một số bước để thực hiện đúng điều này. Đầu tiên, hãy có một chính sách quản lý bản vá và làm cho nó vá mọi thứ và theo dõi tất cả các bản vá. Thứ hai, tuân theo chính sách đó. Có nhiều lý do cho việc không thể vá lỗi vì nhiều lý do, nhưng một chiến lược quản lý bản vá được thực thi một cách đúng đắn sẽ khắc phục được tất cả những rủi ro đó. Lo lắng về một bản vá phá vỡ một hệ thống quan trọng? Nếu nó là một hệ thống tối quan trọng, bạn sẽ có nhiều hơn một, phải không (*hàm ý chỉ nếu là hệ thống tối quan trọng thì thường sẽ có thêm một hệ thống dự phòng cho hệ thống này – người dịch*)? Hãy vá một hệ thống, kiểm tra xem nó có hoạt động hay không, sau đó vá phần còn lại.

Danh sách các doanh nghiệp đã bỏ lỡ một bản vá sau đó mà trở thành con đường cho kẻ tấn công rất dài. Những kẻ tấn công dễ dàng kiểm tra xem bạn đã vá lỗi hay chưa — chúng cố gắng khai thác lỗ hổng đã biết và nếu nó vẫn còn hoạt động, chúng biết bạn chưa vá và chúng đã có quyền truy cập.

## Ứng dụng

*Ứng dụng* là các chương trình bao gồm khía cạnh chức năng của doanh nghiệp. Từ các thành phần dựa-trên-máy-chủ như máy chủ web và máy chủ cơ sở dữ liệu, đến các ứng dụng máy tính để bàn như Microsoft Office, các ứng dụng là những công cụ xử lý dữ liệu và bổ sung thêm giá trị cho hệ thống. Các ứng dụng, giống như tất cả phần mềm, đòi hỏi phải được cập nhật và vá lỗi để sửa chữa các lỗ hổng và lỗi. Thách thức với việc vá lỗi ứng dụng trong một doanh nghiệp nằm ở việc theo dõi tất cả các ứng dụng được sử dụng, bao gồm cả những chương trình nhỏ dường như vô nghĩa được cài đặt trên máy tính để bàn. Doanh nghiệp không chỉ phải theo dõi tất cả các ứng dụng mà doanh nghiệp đang có mà còn phải

xác định xem những ứng dụng nào có bản cập nhật và vào thời điểm nào. Một số nhà cung cấp phần mềm lớn thực hiện quá trình này một cách dễ dàng, nhưng vô số nhà cung cấp bổ sung khiến cho nhiệm vụ tìm hiểu những gì cần cập nhật, khi nào và ở đâu là một thách thức thực sự. Có những ứng dụng được thiết kế riêng để quản lý khía cạnh này, và chúng tôi khuyến cáo các doanh nghiệp nên sử dụng phần mềm theo-dõi-bản-vá-lỗi để có thể xác định khi nào có bản vá và cài đặt chúng.

---



**MÁCH NƯỚC CHO KỲ THI** Một phần trong trách nhiệm của chuyên gia bảo mật là cập nhật Lỗ hổng và Phơi nhiễm Phổ biến (Common Vulnerabilities and Exposures – CVE) và tiến hành cập nhật hoặc vá lỗi hệ thống để giữ cho môi trường doanh nghiệp được an toàn. Điều này được áp dụng cho firmware, hệ điều hành, ứng dụng, máy ảo, và các thiết bị.

### Các Nền tảng Kế thừa

Các *nền tảng kế thừa* là thuật ngữ được sử dụng để mô tả các hệ thống không còn có mặt trên thị trường hoặc không được hỗ trợ nữa. Chúng cũng được xem là [nền tảng] cũ, vốn trong thuật ngữ CNTT có thể chỉ là vài năm. Các hệ thống kế thừa đại diện cho một lỗ hổng thú vị vì do nằm trong danh mục kế thừa nên chúng không còn được hỗ trợ nữa, do đó nếu những vấn đề mới được khám phá thì cách khắc phục duy nhất là biện pháp kiểm soát bù trừ. Việc có các hệ thống không thể vá lỗi là một rủi ro, nhưng cũng giống như mọi rủi ro, nó phải được đo lường và cân nhắc dựa trên chi phí thay đổi. Trong một môi trường bảo mật được cấu trúc đúng cách, rủi ro của các lỗ hổng kế thừa được bao hàm một phần bởi các biện pháp kiểm soát bù trừ để khiến cho việc thực thi các lỗ hổng đó trở nên cực kỳ khó khăn, nếu không muốn nói là không khả thi.

## Tác động

*Tác động* là những hậu quả khi rủi ro được hiện thực hóa. Tác động là các hạng mục mà một tổ chức đang cố gắng để tránh khi xảy ra một sự cố bảo mật. Các tác động có thể được phân thành một số nhóm khác nhau, và chúng được mô tả trong những phần tiếp theo. Hàm ý của tác động trong quản lý rủi ro được đề cập chi tiết trong Chương 34, "Quản lý Rủi ro". Để biết thêm chi tiết về rủi ro và tác động, tài liệu trong chương đó sẽ kết hợp với nhau cùng với các mục sau đây.

## Mất Dữ liệu

*Mất dữ liệu* là khi một tổ chức thực sự bị mất thông tin. Các tập tin có thể bị xóa, bị ghi đè, hoặc thậm chí đặt sai vị trí. Ransomware là hình thức mất dữ liệu nguy hiểm nhất với vì nó được thúc đẩy bởi các lực lượng bên ngoài và bản chất của nó là khiến cho dữ liệu trở nên không sẵn sàng đổi với doanh nghiệp cho đến khi tiền chuộc được trả. Lỗi phần cứng là một nguồn mất dữ liệu khác. Biện pháp phòng thủ chính đối với mất dữ liệu chính là một chương trình sao lưu vững chắc để có thể khôi phục lại dữ liệu bị mất.

## Xâm phạm Dữ liệu

*Xâm phạm dữ liệu* là công bố dữ liệu cho các bên khác không được phép. Những kẻ tấn công xâm nhập vào hệ thống thường tìm cách đánh cắp những thông tin như thông tin nhận dạng cá nhân (personally identifiable information - PII), dữ liệu tài chính, dữ liệu của công ty có giá trị trên thị trường mở và tài sản trí tuệ. Việc vi phạm dữ liệu có thể là một vấn đề pháp lý, vấn đề tài chính, vấn đề danh tiếng hoặc bất kỳ sự kết hợp nào của những vấn đề này, tùy thuộc vào loại và phạm vi của sự vi phạm. Các biện pháp kiểm soát truy cập mạnh mẽ, mã hóa dữ liệu ở phần còn lại và các yếu tố ngăn chặn mất dữ liệu (DLP) có thể làm giảm bớt tác động. Mã hóa là biện pháp kiểm soát mạnh nhất vì vi phạm dữ liệu đã được mã hóa mà không có khóa thực sự không phải là vi phạm.

## Sàng lọc Dữ liệu

Dữ liệu là một tài sản độc đáo theo nhiều nghĩa. Một trong những cách có liên quan hơn đến sự độc đáo là nó có thể được sao chép và sau đó bị đánh cắp mà không ảnh hưởng đến dữ liệu gốc. Việc đánh cắp dữ liệu trở thành một bài tập trong việc lọc dữ liệu hoặc lấy bản sao ra khỏi doanh nghiệp. Cũng giống như khi kẻ trộm lấy cắp bất cứ thứ gì, vụ trộm thực sự chỉ xảy ra khi chúng trốn thoát cùng với món đồ đó. *Lọc dữ liệu* là việc trích xuất dữ liệu bị đánh cắp từ một doanh nghiệp. Tác động của việc lọc dữ liệu có liên quan đến việc dữ liệu bị đánh cắp. Nếu đó là tài sản trí tuệ thì tác động có thể trực tiếp đến lợi nhuận. Việc mất quyền sở hữu trí tuệ có thể dẫn đến mất doanh số bán hàng trong tương lai.

Việc mất dữ liệu khách hàng có thể ảnh hưởng đến danh tiếng cũng như ảnh hưởng trực tiếp đến tài chính thông qua các hình phạt theo quy định. Các vụ vi phạm dữ liệu lớn đã khiến các công ty phải trả hàng trăm triệu đô la tiền phạt, tiền bồi thường và các thỏa thuận của tòa án.

## Đánh cắp Danh tính

*Đánh cắp danh tính* là một tội phạm khi một ai đó sử dụng thông tin của một bên khác để mạo danh họ. Đây là một tác động thứ cấp khi dữ liệu bị trích xuất. Mất mát dữ liệu có thể đến từ các hệ thống thương mại và thậm chí các hệ thống tại nhà, và kết quả là như nhau: mọi người có thể mất tiền, tài sản, và thời gian để giải quyết đơn kiện về việc trộm cắp danh tính. Tác động của việc lọc dữ liệu bao gồm cả thông tin nhận dạng cá nhân (PII) có thể sẽ đáng kể về mặt chi phí quản lý. Các vi phạm lớn gần đây đã bị phạt rất nhiều theo quy định và các chi phí pháp lý liên quan đến việc đánh mất PII. Loại hồ sơ đắt giá nhất bị mất là các hồ sơ PII của khách hàng, liên quan đến khoảng 80% vi phạm trong báo cáo vi phạm của Verizon. Đây không chỉ là vấn đề tài chính nghiêm trọng của một công ty. Với chi phí trung bình cho mỗi hồ sơ bị mất cắp là khoảng

150 đô la, nó khiến cho việc vi phạm 1,000 hồ sơ dù là nhỏ cũng trở thành một vấn đề tiềm ẩn đối với các doanh nghiệp nhỏ hơn.

## Tài chính

Tại thời điểm cuối ngày, rủi ro được đo lường về mặt *tài chính*, và tác động từ các lỗ hổng cũng có thể được diễn giải theo khía cạnh tài chính. Mặc dù đôi khi sẽ rất khó để theo dõi trực tiếp từng vấn đề một với một con số tài chính, nhưng vẫn có một loạt các ví dụ khác nhau nơi mà những kết quả được liên kết một cách dễ dàng với tài chính. Một nhà máy thép của Đức đã bị phá hủy bởi những kẻ tấn công, Sony đã mất một bản phát hành phim vào tay tin tặc Triều Tiên, Equifax đã phải trả gần 2 tỷ đô la để ứng phó với vụ vi phạm năm 2017 - tất cả đều là những chi phí dễ dàng được cho là do tác động trực tiếp của một cuộc tấn công mạng.

Dưới đây là danh sách các hạng mục có thể đóng góp vào chi phí tài chính của một cuộc tấn công mạng:

- Chi phí liên quan đến việc điều tra và khắc phục các hệ thống doanh nghiệp,
- Đơn đặt hàng/doanh thu bị mất do thời gian ngừng hoạt động của hệ thống,
- Tiền phạt do không tuân thủ quy định về luật quyền riêng tư,
- Chi phí cho luật sư từ các vụ kiện,
- Thanh toán tiền chuộc được trả cho ransomware,
- Tổn thất do tài sản trí tuệ bị đánh cắp,
- Giá cổ phiếu giảm và mất vốn hóa thị trường.

Hầu hết các con số tài chính được thấy trên báo chí đều bị nghiêng lệch bởi các khoản thanh toán lớn của các công ty lớn với khoản thua lỗ lớn, nhưng ảnh hưởng đối với các doanh nghiệp vừa và nhỏ thậm chí còn đáng kể hơn nữa. Một tổn thất an ninh mạng trung bình có thể khiến một doanh

nghiệp vừa và nhỏ thiệt hại 400,000 đô la. Đối với nhiều doanh nghiệp, con số này đủ lớn để tiêu diệt họ.

### Danh tiếng

Tác động đến *danh tiếng* như là kết quả của một cuộc tấn công vào hệ thống mạng có hai hình thức chính: mất lòng tin của khách hàng và, trong những trường hợp có liên quan đến lực lượng lao động lành nghề, tổn thất nhân viên chủ chốt trong những lĩnh vực cạnh tranh. Nếu như khách hàng của bạn thắc mắc về năng lực của bạn để hoàn thành các đơn đặt hàng và quản lý những thông tin của họ, hoặc chỉ là mất lòng tin nói chung vào sự quản lý của công ty, sau đó khách hàng có thể chuyển sang một đối thủ cạnh tranh. Điều này đặc biệt đúng về những doanh nghiệp có cơ sở khách hàng là những người tiêu dùng cũng như những doanh nghiệp có khách hàng là doanh nghiệp.

Các công ty có lực lượng lao động tay nghề cao đang thiếu hụt cũng phải quan tâm đến danh tiếng của họ trong mắt nhân viên. Rốt cuộc, ai sẽ muốn làm việc cho một công ty khiến họ bối rối vì những tin bài về những thất bại trong quản lý dẫn đến tổn thất an ninh mạng? Mọi nhân viên công nghệ đều muốn có tên của Google hoặc Apple trong sơ yếu lý lịch của họ, nhưng không ai trong lĩnh vực an ninh mạng muốn nói về việc làm việc cho một công ty như Equifax, nơi mà việc quản lý kém các tài nguyên CNTT đã gây ra một trong những vụ vi phạm tốn kém nhất trong lịch sử. Việc để nhân viên ra đi chỉ vì họ không tin tưởng vào công ty của mình và tìm người thay thế nhân sự có kỹ năng cao khi công ty đang gặp khủng hoảng về danh tiếng không phải là điều mà vị trí quản lý muốn tham gia.

### Mất Tính khả dụng

Bộ ba CIA là tính bảo mật, tính toàn vẹn và tính khả dụng (confidentiality, integrity, availability). Tính khả dụng được định nghĩa là các tài nguyên

sẵn sàng cho người dùng được ủy quyền khi chúng được cho là đang sẵn sàng. Khi tác động của một cuộc tấn công mạng ảnh hưởng đến các yếu tố cơ sở hạ tầng, hoặc do hư hỏng hệ thống, mất dữ liệu hoặc tổn thất hệ thống trong nỗ lực khôi phục, hậu quả là dẫn đến mất khả năng của hệ thống. Nếu khả năng tổn thất này đủ cao, hệ thống sẽ ngừng xử lý các hồ sơ. Đối với một số công ty, việc này có thể tồn tại trong một khoảng thời gian tương đối ngắn. Đối với những công ty khác, thời gian ngừng hoạt động sẽ chuyển trực tiếp thành doanh thu bị mất và trong một số trường hợp, là chi phí liên quan đến các thỏa thuận mức dịch vụ (SLA) bị phá vỡ. Việc mất tính sẵn sàng đối với một phần của bất kỳ hệ thống nào sẽ có tác động đến doanh nghiệp, nếu không, tại sao lại có hệ thống? Việc xác định quy mô thực tế của tổn thất tính khả dụng là đơn giản trong một số hệ thống giao dịch và phức tạp hơn ở những hệ thống khác, nhưng cuối cùng, một công ty đang đầu tư nguồn lực doanh nghiệp vào hệ thống CNTT của mình để tạo điều kiện thuận lợi cho hoạt động kinh doanh chứ không phải làm gián đoạn chúng.



**MÁCH NƯỚC CHO KỲ THI** Những lỗ hổng chưa được kiểm tra do cấu hình yếu kém, rủi ro bên-thứ-ba, quản lý bản vá không đúng/yếu kém, và các hệ thống kẽ thưa có thể dẫn đến những tác động nghiêm trọng, bao gồm mất mát dữ liệu, xâm phạm, lọc dữ liệu và mất cắp danh tính, cũng như tổn thất về tài chính, danh tiếng và tính khả dụng.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các mối quan tâm về bảo mật liên quan đến các loại lỗ hổng bảo mật khác nhau. Chương này mở đầu bằng một cuộc thảo luận về các lỗ hổng dựa-trên-đám-mây so với tại-chỗ và các lỗ hổng zero-day. Phần chính đầu tiên đề cập đến các thiết lập cấu hình yếu kém. Trong phần này, các chủ đề về quyền mở, tài khoản root không được bảo mật, lỗi, mã hóa yếu, giao thức không bảo mật, các thiết lập cài đặt mặc định cũng như các cổng và dịch vụ đang mở đã được đề cập đến.

Phần chính tiếp theo là nói về rủi ro của bên-thứ-ba. Trong phần này, các chủ đề phụ về quản lý nhà cung cấp, tích hợp hệ thống, thiếu hỗ trợ từ nhà cung cấp, chuỗi cung ứng, phát triển mã phần mềm được thuê ngoài và lưu trữ dữ liệu đã được đề cập. Tiếp theo là một cuộc thảo luận về quản lý bản vá không phù hợp hoặc yếu kém. Trong phần này, firmware, hệ điều hành và ứng dụng đã được nói đến. Phần tiếp theo đề cập đến các hệ thống kế thừa.

Chương này khép lại với phần thảo luận về tác động của một lỗ hổng bảo mật đã bị khai thác. Trong phần này, chúng tôi đã đề cập đến việc mất dữ liệu, xâm phạm dữ liệu, đánh cắp dữ liệu, mất cắp danh tính và tổn thất về tài chính, danh tiếng và tính khả dụng.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Rủi ro bên-thứ-ba trực tiếp bao gồm những điều nào dưới đây (Hãy chọn mọi đáp án phù hợp)?

  - A. Tích hợp hệ thống
  - B. Chuỗi cung ứng
  - C. Quản lý tài chính
  - D. Quản lý nhà cung cấp.
2. Các nguồn phổ biến của các vấn đề về lỗ hổng đối với các hệ thống bao gồm những điều nào dưới đây (Hãy chọn mọi đáp án phù hợp)?

  - A. Quản lý bản vá yếu kém
  - B. Mất dữ liệu
  - C. Mất cắp danh tính
  - D. Thiết lập cấu hình kém.
3. Những thiết lập cấu hình kém có thể bao gồm những điều nào dưới đây (Hãy chọn mọi đáp án phù hợp)?

  - A. Các cổng mở
  - B. Thiếu hỗ trợ từ nhà cung cấp
  - C. Firmware
  - D. Sử dụng các giao thức không bảo mật.
4. Một quy trình quản lý bản vá nên bao gồm những điều nào dưới đây (Hãy chọn mọi đáp án phù hợp)?

  - A. Quản lý tự động các tài sản phần mềm
  - B. Xác minh tự động các mức vá lỗi hiện hành

- C.** Một khoảng thời gian được chỉ định mà theo đó hệ thống nên được vá lỗi
- D.** Kết nối của quy trình quản lý bản vá với quy trình kiểm soát thay đổi.
- 5.** Những rủi ro tài chính tương ứng với các lỗ hổng có thể bao gồm những điều nào dưới đây (Hãy chọn mọi đáp án phù hợp)?
- A.** Các hình phạt và tiền phạt theo quy định
- B.** Mất danh tiếng của doanh nghiệp
- C.** Mất doanh thu do bị ngừng hoạt động
- D.** Mất dữ liệu.
- 6.** Kiểu mối đe dọa nào khai thác những lỗ hổng của hệ thống và ứng dụng mà các nhà phát triển phần mềm và thậm chí các nhà sản xuất phần mềm chống phần mềm độc hại vẫn chưa biết đến?
- A.** Một cuộc tấn công [vào hệ thống] tại-chỗ
- B.** Một cuộc tấn công zero-day
- C.** Một cuộc tấn công vào [hệ thống] dựa-trên-đám-mây
- D.** Một cuộc tấn công vào nền tảng kẽ th逵a.
- 7.** Là một chuyên gia bảo mật, bạn nên làm gì để xác định các thiết lập cấu hình kém có thể gây ra những rủi ro bảo mật cho tổ chức của bạn (Hãy chọn mọi đáp án phù hợp)?
- A.** Thay đổi tên người dùng và mật khẩu mặc định
- B.** Loại bỏ các ứng dụng không cần thiết
- C.** Vô hiệu hóa các dịch vụ không cần thiết
- D.** Mở tất cả các cổng để từ đó mọi thứ có thể được quét.
- 8.** Mệnh đề nào là sai liên quan đến thực tiễn mã hóa và mã hóa kém?
- A.** Phát triển thuật toán mã hóa của riêng bạn được xem là thực tiễn không bảo mật

- B.** Các thuật toán bảo mật chỉ được tin tưởng sau nhiều năm giám sát và đẩy lùi các cuộc tấn công
- C.** Khả năng sử dụng phần cứng nhanh hơn đã cho phép những kẻ tấn công đánh bại một số phương pháp mã hóa
- D.** Vì TLS không được sử dụng nữa nên thay vào đó, SSL nên được sử dụng.
- 9.** Ai phải gánh chịu những rủi ro tương ứng với một hệ thống hoặc một sản phẩm sau khi nó chuyển sang trạng thái EOL?
- A.** Nhà sản xuất ban đầu
- B.** Nhà cung cấp
- C.** Tổ chức
- D.** Nhà quản lý chuỗi cung ứng.
- 10.** Điều nào dưới đây mô tả đúng nhất về việc xuất dữ liệu bị đánh cắp từ một doanh nghiệp?
- 1.** Mất dữ liệu
- 2.** Xâm phạm dữ liệu
- 3.** Lọc dữ liệu
- 4.** Mất cắp danh tính.

## Đáp án

1. **A, B và D.** Tích hợp hệ thống, chuỗi cung ứng và quản lý nhà cung cấp là những nguồn rủi ro bên-thứ-ba. Quản lý tài chính liên quan đến những tác động, không phải là rủi ro bên-thứ-ba chính.
2. **A và D.** Quản lý bản vá không phù hợp hoặc yếu kém và các thiết lập cấu hình kém được xác định là những nguồn phổ biến của các lỗ hổng.
3. **A và D.** Việc có các cổng mở và sử dụng các giao thức không bảo mật có thể cung cấp các lối vào cho những kẻ tấn công xâm nhập vào hệ thống. Thiếu hỗ trợ từ nhà cung cấp là một rủi ro bên-thứ-ba, và firmware có một cấu hình cố định.
4. **A, B, C và D.** Một quy trình quản lý bản vá tốt nên bao gồm quản lý tự động các tài sản phần mềm, xác minh tự động các mức vá lỗ hiện hành, một khoảng thời gian được chỉ định mà theo đó hệ thống nên được vá lỗ và kết nối của quy trình quản lý bản vá với quy trình kiểm soát thay đổi.
5. **A và C.** Những hình phạt và khoản phạt theo quy định cũng như mất doanh thu do ngừng hoạt động là những tác động tài chính trực tiếp của các vấn đề an ninh mạng. Danh tiếng của doanh nghiệp có thể dẫn tới việc mất khách hàng, nhưng đây không phải là một liên kết trực tiếp. Mất dữ liệu có thể hoặc không có một tác động tài chính, tùy thuộc vào dữ liệu và liên kết của nó với doanh thu.
6. **B.** Một cuộc tấn công zero-day khai thác những lỗ hổng hệ thống và ứng dụng vẫn chưa được những người khác biết đến ngoại trừ những người tìm ra nó. Các đáp án lựa chọn khác không phải là các kiểu tấn công. Những lỗ hổng có thể tồn tại trong các hệ thống tại chỗ hoặc dựa trên đám mây, và các nền tảng kẽ thưa

là thuật ngữ được sử dụng để mô tả các hệ thống không còn được bán ra thị trường hoặc không còn được hỗ trợ nữa.

7. **A, B và C.** Mọi nỗ lực nên được thực hiện để loại bỏ các ứng dụng không cần thiết, vô hiệu hóa những dịch vụ không cần thiết, và thay đổi tên người dùng và mật khẩu mặc định. Việc mở tất cả các cổng là một công thức để xảy ra thảm họa. Các cổng không cần thiết hoặc không sử dụng nên được đóng hoặc được bảo vệ.
8. **D.** Tất cả các phiên bản của SSL giờ đây được xem là không còn sử dụng nữa và không nên được sử dụng. Mọi người nên chuyển các hệ thống của họ sang các giải pháp dựa-trên-TLS. Tất cả các mệnh đề khác đều đúng.
9. **C.** Một tổ chức tiếp tục sử dụng một hệ thống hoặc một sản phẩm phải gánh chịu những rủi ro tương ứng với các vấn đề được khám phá sau khi sản phẩm chuyển sang trạng thái hết-thời-hạn-sử-dụng (EOL). Nhà sản xuất trên thực tế thường là nhà cung cấp, và từ quan điểm của họ, sản phẩm đến hạn sử dụng khi họ ngừng hỗ trợ cho nó. Nhà quản lý chuỗi cung ứng là một lựa chọn đáp án sai.
10. **C.** Lọc dữ liệu là việc trích xuất những dữ liệu bị đánh cắp từ một doanh nghiệp. Mất dữ liệu là khi một tổ chức thực sự mất những thông tin của mình. Vi phạm dữ liệu là việc phát hành dữ liệu cho các bên khác không được phép. Mất cắp danh tính là một tội phạm khi một ai đó sử dụng thông tin của một bên khác để mạo danh họ.

## Chương 7      Đánh giá Bảo mật

---

### Đánh giá bảo mật

Trong chương này bạn sẽ

- Tìm hiểu về việc săn lùng mối đe dọa,
  - Xem xét những chi tiết của quá trình quét lỗ hổng,
  - Khám phá các kỹ thuật syslog/SIEM/SOAR.
- 

Đánh giá là việc kiểm tra một điều gì đó so với một tiêu chuẩn, để xem xét cách thức nó được đo lường như thế nào. Trong lĩnh vực bảo mật, tiêu chuẩn chính nên là bộ các chính sách bảo mật của bạn – và chúng nên liên kết với bất kỳ yêu cầu bên ngoài nào. Vậy, làm thế nào để bạn kiểm tra các hệ thống của bạn để xem liệu mọi thứ có đang hoạt động thực tế theo cách mà bạn mong muốn hay không? Chương này sẽ khám phá một vài khía cạnh về việc thực hiện quá trình đánh giá. Một trong những phương pháp chính để thực hiện đánh giá bảo mật là thông qua sử dụng các kiểm nghiệm xâm nhập, và những kiểm nghiệm này được đề cập đến trong Chương 8, "Kiểm nghiệm Xâm nhập".

**Mục tiêu Chứng nhận:** Chương này đề cập đến mục tiêu 1.7 của kỳ thi CompTIA Security+: Tóm tắt những kỹ thuật được sử dụng trong đánh giá bảo mật.

## Săn tìm Mối đe dọa

*Săn lùng mối đe dọa* là thực hiện việc tìm kiếm một cách chủ động những mối đe dọa đến hệ thống mạng nằm trong một mạng, và vẫn chưa được phát hiện. Săn lùng mối đe dọa hệ thống mạng sử dụng các công cụ, kỹ thuật và thủ tục (TTP) để khám phá những tác nhân trái phép trong hệ thống mạng của bạn nhưng vẫn chưa được phát hiện bởi hệ thống phòng thủ của bạn. Hầu hết các yếu tố phòng thủ đều hướng ra bên ngoài và nằm trên hoặc gần với ranh giới chu vi mạng, vì đây là nơi bạn có nhiều khả năng nhất bắt gặp những người dùng trái phép. Nhưng nếu như kẻ tấn công có thể vượt qua hàng rào phòng thủ đó thì chúng có thể ẩn náu trong một hệ thống mạng hàng tháng, nếu không muốn nói là hàng năm. Trong thời gian này, chúng có thể âm thầm thu thập dữ liệu, tìm kiếm tài liệu bí mật hoặc lấy cắp thông tin đăng nhập khi những thông tin này di chuyển ngang qua môi trường. Những kẻ tấn công có thể sử dụng tài nguyên hệ thống để tiếp tục sự hiện diện của chúng, một kỹ thuật được gọi là “sống nhờ đất” (living off the land).

Việc săn lùng các mối đe dọa sử dụng những công cụ và kỹ thuật để đặc biệt phát hiện kiểu người dùng này - các công cụ như nguồn dữ liệu thông tin tình báo về mối đe dọa chiến thuật và nguồn cấp dữ liệu về mối đe dọa mô tả các hoạt động của tin tặc, cũng như các công cụ như chỉ báo tấn công (indicators of attacks - IOA) và chỉ báo xâm phạm (indicators of compromise - IOC). Các chỉ báo tấn công bao gồm một loạt các hành động mà kẻ tấn công phải hoàn thành để thực hiện một cuộc tấn công. Việc này bao gồm các hoạt động như tạo tài khoản, kết nối với máy chủ điều-khiển-và-kiểm-soát cũng như di chuyển dữ liệu ra khỏi mạng theo một luồng được mã hóa. Đây là những hành động được thực hiện bởi một tác nhân đe dọa như là một phần của quy trình làm việc của họ nhằm xâm phạm hệ thống. Việc tìm kiếm những hoạt động này là một phần của việc săn tìm mối đe dọa. Các chỉ báo xâm phạm là những hiện vật do các

hoạt động của kẻ tấn công để lại. Các chuỗi cụ thể trong bộ nhớ từ phần mềm độc hại, hiện vật pháp y như các tập tin liên kết và các tập tin có thể thực thi giả mạo - đây là tất cả các chỉ báo về hoạt động độc hại, nhưng cũng là những hoạt động trong quá khứ. Những người săn lùng mối đe dọa sử dụng những manh mối này để tập trung vào nơi kẻ tấn công đã từng ở đó, những gì chúng đã thực hiện và nơi chúng có khả năng sẽ đi đến tiếp theo khi kẻ tấn công theo dõi phiên bản Cyber Kill Chain của chúng.

### **Nguồn tình báo Hợp nhất**

Nguồn tin tình báo về mối đe dọa là những kiến thức ẩn giấu sau năng lực, cơ sở hạ tầng, động cơ, mục tiêu và nguồn lực của một mối đe dọa. *Nguồn tin tình báo hợp nhất* về mối đe dọa cho phép một người phòng thủ xác định và đặt bối cảnh thích hợp cho những mối đe dọa mà họ đang phải đối mặt trong môi trường, sử dụng những thông tin từ nguồn tình báo về mối đe dọa trong Mô hình Kim cương về Phân tích Xâm nhập (Diamond Model of Intrusion Analysis), như được minh họa trong Chương 27, "Các Chính sách, Quy trình và Thủ tục Ứng phó Sự cố". Khi bạn hiểu được địch thủ của bạn, bạn có thể thực hiện hành động dứt khoát để bảo vệ tổ chức của bạn tốt hơn.



**MÁCH NƯỚC CHO KỲ THI** Nguồn tình báo hợp nhất là một quy trình liên quan đến việc thu thập và phân tích các nguồn cung cấp tin tức về mối đe dọa từ cả các nguồn từ bên trong lẫn bên ngoài trên quy mô lớn.

### **Nguồn cung cấp dữ liệu về Mối đe dọa**

*Nguồn cung cấp dữ liệu về mối đe dọa* là những nguồn thông tin liên quan đến đối thủ. Nguồn cung cấp dữ liệu về đe dọa có thể đến từ các nguồn

nội bộ và bên ngoài. Bằng cách tận dụng dữ liệu về mối đe dọa từ mạng lưới của riêng bạn dựa trên dữ liệu ứng phó sự cố (nghĩa là tập tin nhật ký, cảnh báo và kết quả ứng phó sự cố), bạn có khả năng tìm được các vị trí khác có cùng mối đe dọa trong môi trường của bạn. Các nguồn thông tin về mối đe dọa từ bên ngoài đến từ nhiều thực thể bên ngoài khác nhau và kết quả là chúng có thể liên kết hoặc không liên kết với môi trường cụ thể của bạn. Những nguồn cung cấp dữ liệu từ bên ngoài cần nhiều công sức quản lý hơn để điều chỉnh thông tin thành những dạng hữu ích trong doanh nghiệp của bạn, nhưng các phương pháp trao đổi được tự động hóa, chẳng hạn như Biểu thị Thông tin về Mỗi đe dọa có Cấu trúc (STIX), hỗ trợ cho việc di chuyển thông tin quan trọng này giữa các công ty. Cuối cùng, việc xác định mức độ liên quan của nguồn cung cấp dữ liệu bên ngoài phụ thuộc vào nhóm bảo mật của bạn với những kiến thức cụ thể của họ về môi trường và toàn cảnh mối đe dọa của tổ chức bạn.

### **Nguồn Tư vấn và các Bản tin**

*Nguồn tư vấn và các bản tin* là những tập hợp thông tin được công bố từ các đối tác, chẳng hạn như nhà cung cấp bảo mật, các nhóm trong ngành, chính phủ, các nhóm chia-sẻ-thông-tin, và các nhóm khác có thông tin “đáng tin cậy”. Đây là những nguồn cung cấp dữ liệu về mối đe dọa từ bên ngoài này và cần phải được xử lý bởi nhân viên bảo mật để xác định khả năng ứng dụng của chúng và cách thức sử dụng chúng để cải thiện những biện pháp phòng thủ của doanh nghiệp.

### **Cơ động**

*Cơ động* đề cập đến khả năng di chuyển trong một mạng lưới, một chiến thuật được sử dụng một cách phổ biến bởi những đối thủ được tăng cường khi họ tiến đến phía mục tiêu của mình. Việc săn lùng mối đe dọa có thể chống lại sự cơ động của kẻ tấn công thông qua một số cơ chế. Đầu tiên,

người săn lùng mối đe dọa có thể theo dõi lưu lượng truy cập tại các điểm chướng ngại vật (nghĩa là các điểm mà thực thể trái phép bắt buộc phải đi qua). Thứ hai, người săn lùng mối đe dọa có thể phân tích cơ sở hạ tầng mạng của chính công ty, thông qua con mắt của kẻ tấn công và cung cấp thông tin chi tiết về cách mạng có thể được kết nối để cung cấp khả năng phòng thủ tốt hơn chống lại sự di chuyển sang phía bên kia, cả về mặt kết nối lẫn việc ghi nhật ký. Những nỗ lực này khiến việc điều động không bị phát hiện trở thành thách thức lớn hơn nhiều đối với những kẻ tấn công, và bởi vì phần lớn các biện pháp phòng thủ có thể được thực hiện một cách thụ động đối với những gì kẻ tấn công nhìn thấy, nó thậm chí còn có hiệu quả hơn.



**MÁCH NƯỚC CHO KỲ THI** Cơ động cũng là một biện pháp phòng thủ chiến thuật được sử dụng bởi các chuyên gia bảo mật để cắt đứt hoặc ngăn chặn một kẻ tấn công khỏi việc di chuyển sang phía bên kia như một phần của chuỗi tấn công.

### Quét Lỗ hổng

*Quét lỗ hổng* là tiến trình kiểm tra các dịch vụ trên các hệ thống máy tính để phát hiện các lỗ hổng đã biết trong phần mềm. Về cơ bản, đây là một tiến trình đơn giản về việc xác định các phiên bản cụ thể của một chương trình phần mềm và sau đó tìm kiếm những lỗ hổng đã biết. Cơ sở dữ liệu Lỗ hổng và Sự phơi nhiễm Phổ biến (CVE) có thể được sử dụng như một kho lưu trữ, và nó ghi nhận hơn 145,000 lỗ hổng cụ thể. Điều này khiến cho tác vụ không chỉ làm một nhiệm vụ thủ công, một số các chương trình phần mềm khác nhau có thể được sử dụng để thực hiện chức năng này.

## Dương tính Giả

Bất kỳ hệ thống nào sử dụng một phép đo một số thuộc tính để phát hiện một số điều kiện khác đều có thể có lỗi. Khi một phép đo được sử dụng như một phần của quy trình ra quyết định, các yếu tố bên ngoài có thể gây ra sai số. Đến lượt mình, những sai số này có thể ảnh hưởng đến một phép đo với một điều kiện nào đó tạo ra một sai số trong con số cuối cùng. Khi một phép đo được sử dụng trong một quy trình ra quyết định, xác suất của sai sót và ảnh hưởng của chúng phải là một phần của quy trình ra quyết định. Ví dụ, khi một nhà hàng chế biến món bít-tết ở nhiệt độ trung bình, cách thức dễ nhất để xác định xem liệu món bít-tết đã được chế biến một cách đúng đắn hay chưa sẽ là cắt nó ra và xem xét. Nhưng việc này có thể được thực hiện trong bếp, vì vậy các điều kiện khác cũng được sử dụng, chẳng hạn như thời gian, nhiệt độ, v.v... Khi khách hàng cắt miếng bít-tết chính là thời điểm của sự thật, bởi vì lúc đó, tình trạng thực tế mới được phát lộ.



### MÁCH NƯỚC CHO KỲ THI

Dương tính giả và âm tính giả phụ thuộc vào kết quả của kiểm nghiệm và kết quả chính xác. Nếu bạn kiểm tra một điều gì đó và có một chỉ báo dương tính, nhưng chỉ báo đó là sai thì đó là dương tính giả. Nếu bạn kiểm tra một điều gì đó, không nhận được chỉ báo nhưng kết quả đáng lẽ ra phải đúng thì đó là âm tính giả.

Hai loại lỗi có liên quan: dương tính giả và âm tính giả. Việc lựa chọn các thuật ngữ *dương tính* và *âm tính* liên quan đến kết quả của thử nghiệm. Nếu bạn đang sử dụng Nmap như một công cụ để kiểm tra hệ điều hành, nó sẽ báo cáo hệ điều hành là một loại cụ thể (giả sử như Windows 10). Nếu kết quả này không chính xác, thì đây là lỗi *dương tính giả* nếu bạn đã tính kết quả là đúng.



**MÁCH NƯỚC CHO KỲ THI** Đây là một hạng mục đã được kiểm nghiệm kỹ. Một kết quả dương tính giả xảy ra khi hành vi được kỳ vọng hoặc hành vi bình thường được xác định sai là [hành vi] độc hại. Việc phát hiện một lần đăng nhập sai tiếp theo là một lần đăng nhập thành công đang được gán nhãn là độc hại, khi một hành động của người dùng tạo ra một lỗi sau một lần thay đổi mật khẩu của họ gần đây, là một ví dụ về một dương tính giả.

### Âm tính Giả

Những kết quả *âm tính giả* đối ngược với những kết quả dương tính giả. Nếu bạn kiểm tra một điều gì đó và kết quả trả lại là âm tính, nhưng trong thực tế lại là dương tính thì kết quả đó là âm tính giả. Ví dụ, nếu như bạn quét các cổng để tìm kiếm bất kỳ cổng nào đang được mở và bạn bỏ lỡ một cổng đang mở vì chương trình quét không thể phát hiện ra nó đang mở, và bạn không chạy một kiểm nghiệm bởi vì kết quả sai này, bạn đang mắc một lỗi âm tính giả.



**MÁCH NƯỚC CHO KỲ THI** Khi một hệ thống phát hiện xâm nhập (IDS) không tạo ra một cảnh báo từ một cuộc tấn công phần mềm độc hại thì đây là một kết quả âm tính giả.

### Xem xét Nhật ký

Một hệ thống nhật ký được thiết lập cấu hình một cách đúng đắn có thể cung cấp những thông tin sâu sắc về những gì đã xảy ra trên một hệ thống máy tính. Điều then chốt nằm ở cấu hình thích hợp để bạn nắm bắt được những sự kiện mà bạn muốn nhưng không cần thêm những dữ liệu không liên quan. Điều này có nghĩa là một hệ thống nhật ký là một kho

tàng tiêm năng chứa những thông tin hữu ích cho một ai đó đang tiến hành tấn công vào một hệ thống. Nó sẽ chứa những thông tin về các hệ thống, các tên tài khoản, những gì đã hoạt động để truy cập [vào hệ thống], và những gì không. *Xem xét nhật ký* có thể cung cấp những thông tin về các sự cố bảo mật, vi phạm chính sách (hoặc cố gắng vi phạm chính sách), và những tình huống bất thường khác đòi hỏi sự phân tích thêm.

### **Được Chứng thực so với Không được Chứng thực**

Quá trình quét lỗ hổng có thể được thực hiện có và không có thông tin chứng thực. Việc thực hiện một quá trình quét [lỗ hổng] mà không có thông tin xác thực có thể cung cấp thêm một số thông tin về trạng thái của dịch vụ và liệu nó có dễ bị tổn thương hay không. Đây là góc nhìn của một người ngoài cuộc thực sự trên hệ thống mạng. Nó có thể được thực hiện một cách nhanh chóng, theo cách được tự động hóa trên các phân đoạn lớn của hệ thống mạng. Tuy nhiên, nếu không có thông tin đăng nhập, sẽ không thể xem chi tiết mà thông tin đăng nhập cung cấp. *Quét lỗ hổng bảo mật được chứng thực [có thông tin đăng nhập]* có thể xem xét sâu hơn một máy chủ lưu trữ và trả về những thông tin rủi ro quan trọng và chính xác hơn. Thường thì những quá trình quét này được sử dụng cùng nhau. Đầu tiên, một *quá trình quét không xác thực* được thực hiện trên các phân đoạn mạng lớn bằng các công cụ được tự động hóa. Sau đó, dựa trên những kết quả sơ bộ này, những quá trình quét có thông tin xác thực chi tiết hơn sẽ được chạy trên các máy có nhiều hứa hẹn nhất về các lỗ hổng.



### **MÁCH NƯỚC CHO KỲ THI**

Những quá trình quét có thông tin xác thực có liên quan nhiều hơn, đòi hỏi những thông tin xác thực và các bước bổ sung để đăng nhập vào một hệ thống, trong khi những quá trình

quét không được xác thực có thể được thực hiện một cách nhanh chóng hơn trên toàn bộ các máy bằng cách sử dụng tự động hóa.

Những quá trình quét có thông tin xác thực có thể tiết lộ thêm nhiều thông tin bổ sung hơn những quá trình quét không có thông tin xác thực.

### **Xâm nhập so với Không xâm nhập**

Những quá trình quét lỗ hổng có thể là xâm nhập hoặc không xâm nhập đối với hệ thống đang được quét. Một quá trình quét *không xâm nhập* thường là một quá trình quét đơn giản các cổng và dịch vụ đang mở, trong khi quá trình quét *xâm nhập* cố gắng lợi dụng những lỗ hổng tiềm năng thông qua việc khai thác để chứng minh các lỗ hổng. Sự xâm nhập (intrusion) này có thể dẫn đến sự cố hệ thống và do đó được gọi là sự xâm nhập (intrusive).

### **Ứng dụng**

Các *ứng dụng* là những chương trình phần mềm thực hiện việc xử lý dữ liệu trên những thông tin trong một hệ thống. Là phần tử hoạt động liên quan đến dữ liệu, cũng như phương tiện điển hình để tương tác giữa người dùng và dữ liệu, các ứng dụng là những đích nhắm mục tiêu phổ biến cho những kẻ tấn công. Những quá trình quét lỗ hổng đánh giá sức mạnh của một ứng dụng đã được triển khai so với hiệu suất mong muốn của hệ thống khi bị tấn công. Những lỗ hổng ứng dụng đại diện cho một số những vấn đề rủi ro trong doanh nghiệp bởi vì các ứng dụng là cần thiết, và càng có một số ít các phương pháp để xử lý thông tin dữ liệu sai lệch khi càng đi lên cao hơn trong ngăn xếp.

### **Ứng dụng Web**

Các *ứng dụng web* chỉ là những ứng dụng có thể truy cập được từ web. Phương pháp truy cập này đem đến sự tiện lợi và sự tiếp xúc tiềm ẩn lớn hơn nữa với những hoạt động trái phép. Mọi chi tiết về các ứng dụng tiêu

chuẩn vẫn được áp dụng, tuy nhiên việc đặt một hệ thống trên web bổ sung thêm những gánh nặng cho hệ thống để ngăn chặn việc truy cập trái phép và giữ quyền kiểm soát đối với những rủi ro dựa-trên-nền-web. Từ quan điểm quét lỗ hổng bảo mật, một ứng dụng web giống như một lời mời khám phá cách nó được bảo vệ đến mức nào. Rủi ro lớn nhất là những ứng dụng web dạng cây nhà lá vườn vì chúng hiếm khi có được mức bảo vệ đầu vào cần thiết cho một môi trường web thù địch.

## Mạng

*Hệ thống mạng* là một thành phần kết nối tất cả hệ thống điện toán lại với nhau, truyền tải dữ liệu giữa các hệ thống và người dùng. Hệ thống mạng cũng có thể được sử dụng trong quét lỗ hổng để truy cập vào các hệ thống đã được kết nối. Những quá trình quét lỗ hổng phổ biến nhất được thực hiện trên toàn bộ hệ thống mạng trong đó mọi hệ thống đều bị quét, lập bản đồ, và liệt kê danh sách theo các cổng và các dịch vụ. Thông tin này sau đó có thể được sử dụng để quét thêm nhằm vào mục tiêu cụ thể vào các hệ thống riêng lẻ theo cách chi-tiết-di-chuyển (*move-detailed – đoạn này không rõ lỗi chính tả không – người dịch*), sử dụng những thông tin đăng nhập và các hoạt động xâm nhập tiềm ẩn.

## Các Lỗ hổng và Phơi nhiễm Phổ biến (CVE)/Hệ thống Chấm điểm Lỗ hổng Phổ biến (CVSS)

Bảng liệt kê *Các Lỗ hổng và Phơi nhiễm Phổ biến (CVE)* là một danh sách các lỗ hổng đã biết trong các hệ thống phần mềm. Từng lỗ hổng trong danh sách có một mã số định danh, mô tả, và tài liệu tham chiếu. Danh sách này là cơ sở cho hầu hết các hệ thống quét lỗ hổng bảo mật, vì bộ quét xác định phiên bản phần mềm và tra cứu các lỗ hổng đã biết hoặc đã được báo cáo. *Hệ thống Chấm điểm Lỗ hổng Phổ biến (CVSS)* là một hệ thống chấm điểm để xác định mức độ rủi ro của một lỗ hổng bảo mật đối với một hệ thống. Điểm CVSS nằm trong khoảng từ 0 đến 10. Khi điểm

số CVSS tăng lên, mức độ nghiêm trọng của rủi ro do lỗ hổng bảo mật gây ra cũng tăng theo. Mặc dù CVSS không thể xem xét vị trí của lỗ hổng bảo mật trong doanh nghiệp nhưng nó có thể giúp xác định mức độ nghiêm trọng bằng cách sử dụng các chỉ số như liệu nó có dễ bị khai thác hay không, liệu nó có đòi hỏi sự can thiệp của người dùng hay không, mức độ đặc quyền cần thiết, v.v... Cùng với nhau, hai bộ thông tin này có thể cung cấp một loạt thông tin về những rủi ro tiềm ẩn liên quan đến một hệ thống phần mềm cụ thể.

Điểm số CVSS và mức độ nghiêm trọng của rủi ro tương ứng của chúng được thể hiện như dưới đây:

Xếp hạng Rủi ro	Điểm CVSS
Thấp	0.1 – 3.9
Trung bình	4.0 – 6.9
Cao	7.0 – 8.9
Nghiêm trọng	9.0 - 10



**MÁCH NƯỚC CHO KỲ THI** Hãy nhận biết rằng Lỗ hổng và Sự phơi nhiễm Phổ biến (CVE) là một danh sách các lỗ hổng đã biết, từng lỗ hổng có một mã số định danh, mô tả và tài liệu tham chiếu. Hệ thống Chấm điểm Lỗ hổng Phổ biến (CVSS) xác định mức rủi ro mà một lỗ hổng đối với một hệ thống. Điểm số CVSS có phạm vi từ 0 đến 10. Khi điểm số này gia tăng, mức độ nghiêm trọng của rủi ro từ lỗ hổng cũng gia tăng.

## Xem xét Cấu hình

Cấu hình hệ thống đóng một vai trò đáng kể trong bảo mật hệ thống. Việc cấu hình sai lệch sẽ đặt một hệ thống vào trạng thái dễ tổn thương hơn, thậm chí thỉnh thoảng khiến cho các biện pháp kiểm soát bảo mật hoàn toàn bị bỏ qua. Xác minh cấu hình hệ thống là một hạng mục kiểm tra lỗ hổng bảo mật quan trọng, nếu như bạn phát hiện một cấu hình sai lệch, cơ hội tiếp xúc với một lỗ hổng bảo mật sẽ trở nên cao hơn. *Xem xét cấu hình* đủ quan trọng để chúng nên được tự động hóa và thực hiện trên cơ sở định kỳ thường xuyên. Có nhiều giao thức và tiêu chuẩn để đo lường và xác thực các cấu hình. Các hướng dẫn Bảng liệt kê Cấu hình Phổ biến (CCE) và Bảng liệt kê Nền tảng Phổ biến (CPE), là một phần của Cơ sở dữ liệu Lỗ hổng Quốc gia Hoa Kỳ (NVD) được duy trì bởi NIST, là nơi để bắt đầu để có thêm chi tiết.

## Quản lý Sự kiện và Thông tin Bảo mật/Nhật ký hệ thống (SIEM)

*Syslog* (*nhật ký hệ thống*) là viết tắt của Giao thức Ghi nhật ký Hệ thống (System Logging Protocol) và là một giao thức tiêu chuẩn được sử dụng trong các hệ thống Linux để gửi nhật ký hệ thống hoặc những thông điệp sự kiện đến một máy chủ cụ thể, được gọi là máy chủ nhật ký hệ thống. Một loạt các thiết bị khác nhau, chẳng hạn như máy in, thiết bị mạng, và các hệ thống trên rất nhiều nền tảng, đều sử dụng tiêu chuẩn syslog. Giá trị của syslog là sự tách biệt một hệ thống khỏi các báo cáo lỗi, cho phép cả các chức năng bảo mật của việc ghi nhật ký hệ thống được tách biệt khỏi hệ thống đang được giám sát lẫn việc tổng hợp nhiều luồng nhật ký trên một máy chủ chung. Một máy chủ syslog lắng nghe trên cả cổng UDP 514 và TCP 6514. Syslog còn nhiều hơn chỉ là các lỗi, nó là tiêu chuẩn dành cho ghi nhật ký từ xa trên các hệ thống Linux. Ubuntu lưu trữ hoạt động toàn cầu và các thông điệp khởi động trong /var/log/syslog. Các ứng dụng cũng có thể sử dụng nó.

Thông tin trong một máy chủ syslog chỉ là các bảng biểu chứa dữ liệu thô. Để khiến cho dữ liệu này dễ sử dụng hơn, một hệ thống được gọi là *quản lý sự kiện và thông tin bảo mật (SIEM)* được sử dụng để thu thập, tổng hợp, và áp dụng hình mẫu khớp với khối lượng dữ liệu. Việc này chuyển các bảng dữ liệu thành những thông tin hợp lý hữu ích dựa trên các quy tắc đã được thiết lập bởi một tổ chức. Bước đầu tiên của việc xử lý trong một SIEM là thu thập dữ liệu thành một loạt các bảng biểu có cấu trúc. Điều này cho phép nhiều nguồn dữ liệu khác nhau với các phần tử dữ liệu khác nhau có khả năng hoạt động cùng nhau. Các bảng biểu dữ liệu này sau đó được làm giàu bằng cách sử dụng các chức năng tra cứu và kết hợp khác để cung cấp bối cảnh lớn hơn cho dữ liệu đã được thu thập. Sau đó hệ thống có thể kiểm tra những dữ liệu liên-quan-đến-thời-gian này đối với những sự kiện tương quan có thể được sử dụng để kích hoạt các hành động ứng phó sự cố.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng syslog có thể được sử dụng để tổng hợp nhật ký từ các thiết bị mạng và hệ điều hành Linux. Một máy chủ syslog lắng nghe và ghi nhật ký các thông điệp từ các máy khách syslog. Các hệ thống SIEM thu thập, tổng hợp, và áp dụng hình mẫu khớp với khối lượng dữ liệu để tạo ra những thông tin mà con-người-có-thể-đọc-được.

### Xem xét các Báo cáo

Phương tiện chủ yếu để cung cấp kết quả đầu ra từ một SIEM là một cảnh báo hoặc một báo cáo. Đây là những điều kiện được xác định trước để kích hoạt một kết quả đầu ra cụ thể về những thông tin dựa trên các quy tắc trong hệ thống. Những báo cáo này sau đó có thể được xem xét để

xác định xem liệu một sự cố có đang tồn tại hay không hay đây chỉ là một báo động giả.

## Bắt Gói tin

*Bắt gói tin* đã từng là một công việc quan trọng của các kỹ sư mạng miễn là các hệ thống mạng còn tồn tại. Việc chẩn đoán và tìm hiểu các vấn đề giao tiếp mạng trở nên dễ dàng hơn khi người ta quan sát cách thức các gói tin truyền qua mạng như thế nào. Gần đây, khái niệm bắt gói tin liên tục để giám sát một phân đoạn của hệ thống mạng đã trở thành một công cụ trong hộp công cụ của chuyên gia bảo mật. Phần lớn các cảnh báo bảo mật đều diễn ra sau thực tế. Một điều gì đó diễn ra, một quy tắc được kích hoạt, và dữ liệu được thu thập, dẫn đến một cuộc điều tra về quy tắc đó. Mặc dù điều này có thể được thực hiện một cách nhanh chóng với sự tự động hóa nhưng các gói tin liên quan đã biến mất từ lâu. Gói tin liên tục đi vào được bắt lại. Trong những khu vực mạng chủ yếu, nơi có khả năng phát lại lưu lượng mạng từ một khoảng thời gian trước đó là điều quan trọng, việc thu thập liên tục các gói tin có thể cung cấp cơ hội đó. Điều này thường sẽ làm tiêu tốn đáng kể dung lượng lưu trữ, do đó, vị trí và thời lượng thu thập có thể sẽ rất quan trọng.

Bằng cách sử dụng một SIEM, được kết hợp với những thiết bị thông minh như các tường lửa thế-hệ-kế-tiếp, khi một quy tắc được kích hoạt, thiết bị bắt lưu lượng mạng có thể tự động thu thập và gửi đi một lượng lưu lượng được xác định trước để phân tích sau này. Với chi phí tương đối thấp của các thiết bị lưu trữ và vị trí thích hợp, phương pháp thu thập dữ liệu này có thể được thực hiện bằng phần cứng hàng hóa thương mại.

## Dữ liệu Đầu vào

*Dữ liệu đầu vào* cho một SIEM cũng đa dạng như những hệ thống mà chúng được sử dụng để bảo vệ. Trong khi một hệ thống mạng hiện đại có thể tạo ra một lượng lớn dữ liệu nhật ký, điều quan trọng là một SIEM

xác định những thông tin nào là cần thiết để hỗ trợ cho những quyết định nào. Một SIEM có thể thu thập mọi thứ, nhưng điều này làm phát sinh nhiều chi phí và tạo ra rất nhiều các báo cáo mà không ai cần đến. Điều quan trọng là xác định những kết quả đầu ra mong muốn từ SIEM và sau đó theo dõi những đầu vào cần thiết từ các tường lửa, các thiết bị mạng, các máy chủ chính, v.v... để hỗ trợ cho các quyết định đó. Khi một SIEM trưởng thành, hầu hết các nguồn dữ liệu được xác định và được đưa vào, và những gì không được sử dụng sẽ được loại bỏ. Một SIEM được tinh chỉnh bởi nhân viên bảo mật để trả lời cho những câu hỏi liên quan đến môi trường và những rủi ro của họ.

### **Phân tích Hành vi Người dùng**

Các SIEM là những hệ thống được xây dựng để áp dụng các quy tắc để cho các bộ dữ liệu liên quan đến những hình mẫu cụ thể. Theo truyền thông thì điều này có nghĩa là các sự kiện, các lỗi và những điều kiện khác kiểu hệ thống mạng – và máy chủ - cảnh báo cho một nhân viên vận hành rằng hệ thống đã không phản hồi theo cách thức như bình thường. Việc tương quan các sự kiện giữa các hệ thống có thể cho thấy các hình mẫu của hoạt động là bình thường và như đã được kỳ vọng hoặc bất thường và đòi hỏi một cuộc điều tra. Những tiến bộ trong *phân tích hành vi người dùng* đã đem lại một công dụng thú vị khác của SIEM: giám sát những gì mọi người thực hiện với các hệ thống của họ và cách thức mà họ thực hiện điều đó. Nếu mỗi ngày, khi bắt đầu công việc, nhân viên kế toán khởi động cùng một chương trình, và sau đó, khi tài khoản kế toán đăng nhập vào và làm một điều gì đó hoàn toàn khác biệt, chẳng hạn như truy cập vào một hệ thống mà họ chưa từng bao giờ truy cập trước đây thì điều này cho thấy một sự thay đổi mang tính hành vi cần phải được xem xét. Rất nhiều SIEM hiện đại có các mô-đun phân tích các hành vi

của người-dùng-đầu-cuối, tìm kiếm các hình mẫu hành vi bất thường cho thấy một nhu cầu phân tích.

## Phân tích Cảm xúc

Các hệ thống tương tự được sử dụng để đối sánh với các vấn đề bảo mật có thể được điều chỉnh để phù hợp với các hình mẫu dữ liệu chỉ ra cảm xúc cụ thể. Các mức độ gần gũi của cảm xúc có thể được xác định bằng cách sử dụng những đầu vào như email, cuộc trò chuyện, cơ chế thu thập phản hồi và truyền thông mạng xã hội, được kết hợp với các hệ thống AI (trí tuệ nhân tạo) có thể diễn giải giao tiếp bằng văn bản. Người giao tiếp có đang vui, buồn, tức giận hay thất vọng không? Những cảm xúc này và hơn thế nữa có thể được xác định bởi cách thức mà mọi người giao tiếp.



## MÁCH NƯỚC CHO KỲ THI

Phân tích cảm xúc được sử dụng để xác định và theo dõi những hình mẫu trong cảm xúc, ý kiến hoặc thái độ của con người có thể xuất hiện trong dữ liệu.

## Giám sát Bảo mật

*Giám sát bảo mật* là quy trình thu thập và phân tích những thông tin để phát hiện ra hành vi đáng ngờ hoặc những thay đổi trái phép trong hệ thống mạng của bạn và các hệ thống được kết nối mạng. Điều này hàm ý chỉ một quy trình xác định kiểu hành vi nào nên kích hoạt những cảnh báo. Các thiết bị SIEM đời đầu tập trung vào việc thu thập những thông tin cần thiết. Các SIEM sau này đã nâng cao thành quản lý dữ liệu sự kiện tương ứng với các sự kiện đã được phát hiện. Ngày nay, các hệ thống điều phối bảo mật, tự động hóa và ứng phó (SOAR) hoàn thành việc chuyển sang tự động hóa toàn bộ chu trình của quy trình bảo mật. Do sự

phức tạp của các hệ thống CNTT và doanh nghiệp hiện đại, cùng với sự phức tạp của các cuộc tấn công và các hình mẫu hành vi, nếu không có các hệ thống được tự động hóa như SIEM và SOAR, việc giám sát bảo mật chỉ đơn giản là điều bất khả thi.

## Tổng hợp Nhật ký

*Tổng hợp nhật ký* là quy trình kết hợp các nhật ký lại với nhau. Việc này được thực hiện để hỗ trợ các định dạng [nhật ký] khác nhau từ các hệ thống khác nhau để hoạt động cùng nhau. Tổng hợp nhật ký hoạt động để cho phép nhiều nguồn thông tin độc lập được kết nối lại cùng nhau trong một bức tranh về trạng thái của hệ thống toàn diện hơn là do một nguồn đơn lẻ có thể cung cấp. Trong suốt quá trình tổng hợp, các mục nhập nhật ký có thể được phân tích, điều chỉnh, và các trường then chốt được trích xuất hoặc điều chỉnh dựa trên các truy vấn hoặc quy tắc. Mục tiêu của tổng hợp nhật ký là để lấy nhiều nguồn dữ liệu khác nhau và điều chỉnh dữ liệu thành một hình thức có thể tìm kiếm được và hữu dụng cho các mục đích cụ thể.

## Bộ thu thập Nhật ký

Các *Bộ thu thập nhật ký* là những phần của phần mềm hoạt động để thu thập dữ liệu từ nhiều nguồn độc lập và cung cấp nó cho một nguồn được hợp nhất chẳng hạn như một SIEM. Những nguồn khác nhau có thể có những định dạng khác nhau, và bộ thu thập nhật ký có thể điều chỉnh những phần tử trường dữ liệu khác nhau này thành một luồng dữ liệu toàn diện.

## Điều phối, Tự động hóa và Ứng phó Bảo mật (SOAR)

Săn lùng mối đe dọa là một nhiệm vụ tập-trung-cao-độ-vào-dữ-liệu. Các doanh nghiệp sở hữu một loạt dữ liệu liên-quan-đến-bảo-mật. Dữ liệu này đến từ vô số thiết bị mạng, hệ thống phát hiện xâm nhập, tường lửa, và

các thiết bị bảo mật khác. Dữ liệu này thường được cung cấp cho một hệ thống quản lý sự kiện và thông tin bảo mật (SIEM) để có thể thu thập, tổng hợp và áp dụng hình mẫu khớp với khối lượng dữ liệu. Những cảnh báo sau đó có thể được xử lý bởi nhân viên bảo mật. Tuy nhiên, đây chưa phải là tích hợp hoàn toàn. Các hệ thống *điều phối, tự động hóa và ứng phó bảo mật (SOAR)* lấy dữ liệu SIEM cũng như dữ liệu từ nhiều nguồn khác và hỗ trợ việc tạo ra các runbook và playbook (*hai từ này không tìm được nghĩa tương đương ngắn gọn trong tiếng Việt nên sẽ để nguyên gốc tiếng Anh – người dịch*).

Những bộ săn lùng mối đe dọa sử dụng những thông tin này, cả dưới dạng dữ liệu thô từ các hệ thống SOAR hoặc SIEM và dạng đã được xử lý của nó từ các runbook và playbook, để kiểm tra doanh nghiệp giống như là một kẻ tấn công sẽ làm, lập biểu đồ các lộ trình tấn công đến các tài sản thông tin có giá trị. Sau đó, bằng cách sử dụng thông tin này, một người săn lùng mối đe dọa có thể thu hẹp nơi họ tìm kiếm những kẻ tấn công để thu hẹp lộ tuyến cơ hội mà họ đã xác định là các phương pháp truy cập và tấn công khả dĩ.

Thông tin này cũng rất hữu ích đối với những người đánh giá bảo mật, vì nó vạch ra những biện pháp phòng thủ bảo mật theo một định dạng dễ hiểu và dễ-kiểm-tra. Những lỗ hổng có thể được xác định bằng cách kiểm tra cấu trúc và nội dung của các runbook và playbook. Thông tin tìm hiểu thêm về SOAR cũng như các runbook và playbook được tìm thấy trong Chương 29, “Các Biện pháp kiểm soát và Kỹ thuật Giảm nhẹ”.



## MÁCH NƯỚC CHO KỲ THI

Các hệ thống SOAR kết hợp dữ liệu và cảnh báo từ những nền tảng được tích hợp trong toàn bộ doanh nghiệp



và đặt chúng vào một vị trí duy nhất nơi mà các biện pháp ứng phó được tự động hóa sau đó có thể giải quyết các mối đe dọa và các lỗ hổng.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các công cụ và kỹ thuật được sử dụng trong đánh giá bảo mật. Chương mở đầu với một phần nói về săn lùng mối đe dọa. Trong phần này, các chủ đề về hợp nhất thông tin tình báo, nguồn cung cấp dữ liệu về mối đe dọa, lời khuyên và bản tin cũng như cách điều động đã được đề cập. Phần tiếp theo bao gồm quét lỗ hổng bảo mật. Phần này bắt đầu với việc kiểm tra dương tính giả và âm tính giả. Sau đó, xem xét nhật ký được đề cập, tiếp theo là quét [lỗ hổng] được-xác-thực so với không-được-xác-thực và quét-xâm-nhập so với không-xâm-nhập. Việc kiểm tra các ứng dụng, ứng dụng web và quét mạng cũng được nêu ra. Phần này kết thúc bằng việc kiểm tra các hệ thống Lỗ hổng và Phơi nhiễm Phổ biến (CVE) và Hệ thống Chấm điểm Lỗ hổng Phổ biến (CVSS), cũng như xem xét đánh giá cấu hình.

Phần tiếp theo đề cập đến nhật ký hệ thống (syslog) và hệ thống quản lý sự kiện và thông tin bảo mật (SIEM). Trong phần này, các chủ đề bao gồm đánh giá báo cáo, bắt gói tin, đầu vào dữ liệu, phân tích hành vi của người dùng và phân tích cảm xúc. Các chủ đề về giám sát bảo mật, tổng hợp nhật ký và thu thập nhật ký đã kết thúc phần này. Chương này khép lại với một phân tích về các hệ thống điều phối, tự động hóa và ứng phó bảo mật (SOAR).

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Nếu một hệ thống đang gửi một cảnh báo rằng một tài khoản người dùng bị xâm nhập bởi vì rất nhiều lần mật khẩu thất bại, nhưng quá trình phân tích cho thấy rằng thiết bị của nhân viên đã lưu bộ đệm lại mật khẩu cũ và gây ra lỗi, đây là ví dụ về điều gì?

  - A. Âm tính giả
  - B. Dương tính giả
  - C. Phép đo lỗi
  - D. Lỗi phân tích.
2. Phần mềm chống phần mềm độc hại không phát hiện được một cuộc tấn công ransomware đã được cho là nằm trong khả năng phát hiện của nó. Đây là ví dụ về điều gì?

  - A. Âm tính giả
  - B. Dương tính giả
  - C. Phép đo lỗi
  - D. Lỗi phân tích.
3. Đâu là giới hạn chính của một quá trình quét hệ thống mạng được xác thực?

  - A. Tốc độ
  - B. Kiểm tra quá sâu vào các hộp riêng lẻ
  - C. Không có khả năng mở rộng phạm vi qua nhiều hệ thống
  - D. Làm chậm hệ thống mạng của bạn bằng lưu lượng phụ thuộc.

4. Bạn muốn chứng minh rằng một lỗ hổng có thể trở thành một vấn đề. Phương pháp tốt nhất sẽ được sử dụng là một quá trình quét \_\_\_\_\_?

  - A. được chứng thực
  - B. không-xâm-nhập
  - C. không được chứng thực
  - D. xâm nhập.
5. Điều gì dưới đây là mô tả tốt nhất về CVE?

  - A. Một nơi để báo cáo các lỗi và lỗ hổng
  - B. Một thước đo về tính chất nghiêm trọng của một lỗ hổng
  - C. Một danh sách các lỗ hổng đã biết
  - D. Một danh sách các hệ thống có các lỗ hổng.
6. Điều gì dưới đây thường không kết hợp với các quy trình SIEM?

  - A. Các Ứng dụng
  - B. Syslog
  - C. Thu thập nhật ký
  - D. Tổng hợp nhật ký.
7. Điều gì dưới đây không phải là một phần của một SIEM?

  - A. Thu thập dữ liệu
  - B. Tương quan sự kiện
  - C. Cảnh báo/báo cáo
  - D. Điều tra sự cố.
8. Việc săn lùng mối đe dọa liên quan đến những điều nào dưới đây (Chọn mọi đáp án khả dĩ)?

  - A. Phân tích các hành động của địch thủ
  - B. Diễn giải về các mối đe dọa cho các công ty khác
  - C. Báo cáo tuân thủ
  - D. Tìm hiểu cách thức dữ liệu chảy trong một doanh nghiệp như thế nào.

- 9.** Quy trình nào cho phép các tập tin nhật ký được làm giàu với dữ liệu bổ sung để cung cấp bối cảnh?
- A.** Tổng hợp nhật ký
  - B.** Bộ thu thập nhật ký
  - C.** Xem xét nhật ký
  - D.** Syslog.
- 10.** Điều gì dưới đây thường không được quét trong quá trình quét lỗ hổng?
- A.** Người dùng đầu cuối
  - B.** Hệ thống mạng
  - C.** Ứng dụng
  - D.** Các ứng dụng web.

## Đáp án

1. **B.** Đây là một dương tính giả, vì báo cáo là dương tính về một điều gì đó đã xảy ra, nhưng trong thực là đã không xảy ra.
2. **A.** Thất bại trong việc báo cáo về một sự kiện có thể báo cáo được đã biết là một âm tính giả.
3. **C.** Vì một quá trình quét được chứng thực đòi hỏi những thông tin đăng nhập cho từng hệ thống mà nó đang kiểm tra, và những thông tin đăng nhập này sẽ thay đổi trên một hệ thống mạng, do đó kiểu quét này ít có khả năng mở rộng phạm vi bằng tự động hóa.
4. **D.** Một quá trình quét xâm nhập có thể cố gắng thực hiện một lỗ hổng. Điều này dẫn đến rủi ro là nó có thể gây đảo lộn hệ thống, nhưng nếu nó hoạt động, nó là một bằng chứng rõ ràng về rủi ro tương ứng với một lỗ hổng.
5. **C.** Lỗ hổng và Sự phơi nhiễm Phổ biến là một bảng liệt kê hoặc danh sách các lỗ hổng đã biết.
6. **A.** Các ứng dụng có thể ở trên toàn mạng, và có thể cung cấp dữ liệu cho một SIEM, tuy nhiên chúng thường không phải là một phần của SIEM.
7. **D.** Điều tra sự cố diễn ra sau khi và do kết quả của các quy trình SIEM nhưng thường không phải là một phần của chúng [các quy trình SIEM].
8. **A, B và D.** Việc săn lùng mối đe dọa liên quan đến việc phân tích các hành động của đối thủ, diễn giải về mối đe dọa cho các công ty khác và tìm hiểu cách thức dữ liệu luân chuyển trong một doanh nghiệp để những kẻ địch cơ động có thể bị bắt gặp.
9. **A.** Trong quá trình tổng hợp, các mục nhập nhật ký có thể được phân tích cú pháp, sửa đổi, và các trường chính được trích xuất hoặc sửa đổi dựa trên các truy vấn hoặc quy tắc.

- 10. A.** Người dùng đầu cuối không phải là một phần của quá trình quét lỗ hổng, họ tách biệt khỏi hệ thống và không phải là một phần tử để tìm kiếm những lỗ hổng bảo mật.

## Chương 8     Kiểm nghiệm Xâm nhập

---

### Kiểm nghiệm Xâm nhập

Trong chương này, bạn sẽ

- Tìm hiểu về các khái niệm kiểm nghiệm xâm nhập,
  - Tìm hiểu về các kiểu thăm dò chủ động và thụ động,
  - Khám phá các kiểu bài tập nhóm khác nhau tương ứng với kiểm nghiệm xâm nhập.
- 

Kiểm nghiệm xâm nhập là một hình thức có cấu trúc để kiểm nghiệm các biện pháp phòng thủ bằng cách sử dụng những phương pháp luận được sử dụng bởi những kẻ tấn công. Những bài kiểm tra này có thể được thực hiện theo nhiều cách khác nhau, vốn sẽ được khám phá trong những phần tiếp theo đây.

**Mục tiêu Chứng nhận:** Chương này đề cập đến mục tiêu 1.8 của Kỳ thi CompTIA Security+: Giải nghĩa những kỹ thuật được sử dụng trong kiểm nghiệm xâm nhập.

## Kiểm nghiệm Xâm nhập

*Kiểm nghiệm xâm nhập* mô phỏng một cuộc tấn công từ một nguồn độc hại bên ngoài – do thám hệ thống mạng của bạn để tìm kiếm một lối vào (thường là *bất kỳ lối vào nào*). Các kiểm nghiệm xâm nhập, hoặc ngắn gọn là *pen test*, thường là hình thức kiểm tra bảo mật tích cực nhất, và có thể có rất nhiều hình thức, tùy thuộc vào những gì được xem là “trong” hay “ngoài” phạm vi. Ví dụ, một số kiểm nghiệm xâm nhập chỉ đơn giản là tìm một cách để xâm nhập vào trong hệ thống mạng – bất kỳ cách nào. Việc này có thể có phạm vi từ một cuộc tấn công trên các liên kết trong mạng, đến kỹ thuật xã hội, đến việc có được một chuyên gia kiểm nghiệm đột nhập vào tòa nhà. Các kiểm nghiệm xâm nhập khác bị giới hạn – chỉ tấn công qua các liên kết mạng là được phép, không có tấn công vật lý.

Bất kể phạm vi và phương pháp được chấp thuận, mục tiêu của một kiểm nghiệm xâm nhập luôn như nhau: để xác định xem liệu một kẻ tấn công có vượt qua hàng rào bảo mật của bạn và truy cập vào các hệ thống của bạn hay không. Không giống như một đánh giá lỗ hổng, vốn thường chỉ lập danh mục các lỗ hổng, một kiểm nghiệm xâm nhập cố gắng khai thác các lỗ hổng để xem liệu chúng [các lỗ hổng] cho phép bao nhiêu quyền truy cập. Các kiểm nghiệm xâm nhập thường rất hữu ích theo những cách sau:

- Chúng có thể chỉ ra những mối quan hệ giữa một loạt các mục “rủi-ro-thấp” có thể bị khai thác một cách tuẩn tự để có được quyền truy cập (khiến cho về tổng thể, chúng trở thành một mục “rủi-ro-cao”).
- Chúng có thể được sử dụng để kiểm tra việc đào tạo nhân viên, tính hiệu quả của các biện pháp an ninh, và khả năng của nhân viên của bạn để phát hiện và ứng phó với những kẻ tấn công tiềm ẩn.
- Chúng có thể thường xác định và kiểm nghiệm các lỗ hổng vốn rất khó hoặc thậm chí không thể được phát hiện ra bằng các công cụ quét truyền thống.

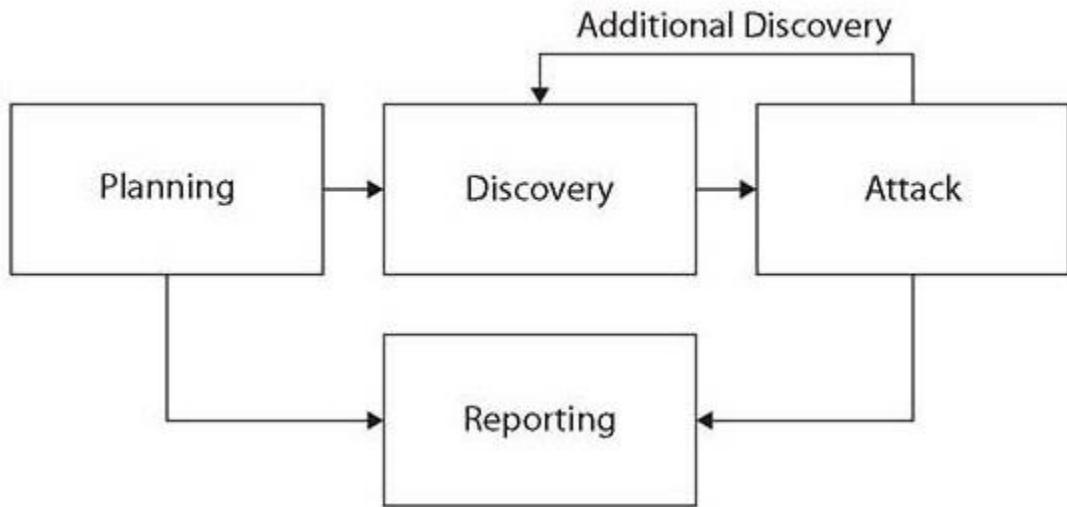


**MÁCH NƯỚC CHO KỲ THI** Các kiểm nghiệm xâm nhập tập trung những nỗ lực để xác định tính hiệu quả của các biện pháp kiểm soát bảo mật đã được sử dụng để bảo vệ một hệ thống.

Một kiểm nghiệm xâm nhập hiệu quả cung cấp một số yếu tố rất quan trọng. Đầu tiên, nó tập trung vào các véc-tơ mối đe dọa được sử dụng phổ biến nhất được nhận thấy trong môi trường mối đe dọa hiện tại. Việc sử dụng các mối đe dọa zero-day mà không ai khác có không giúp cho một công ty hiểu được các biện pháp phòng thủ bảo mật của mình trước môi trường mối đe dọa hiện có. Điều quan trọng là phải bắt chước được những kẻ tấn công trong thế giới thực nếu đó là những gì mà công ty muốn kiểm tra khả năng phòng thủ của mình. Thứ hai, một kiểm nghiệm xâm nhập hiệu quả tập trung vào các mục tiêu của kẻ tấn công trong thế giới thực, chẳng hạn như truy cập và đánh cắp tài sản trí tuệ (IP). Một lần nữa, việc vượt qua hệ thống phòng thủ nhưng không đạt được mục tiêu của kẻ tấn công sẽ không cung cấp một bài kiểm tra năng lực bảo mật đầy đủ.

Rất nhiều phương pháp kiểm nghiệm xâm nhập được sử dụng bởi những người kiểm tra xâm nhập để quản lý quá trình kiểm nghiệm xâm nhập. Được công nhận nhiều nhất là phương pháp Sổ tay hướng dẫn Phương pháp Kiểm nghiệm Bảo mật Nguồn Mở (Open Source Security Testing Methodology Manual - OSSTMM). Đối với các ứng dụng web, Dự án Bảo mật Ứng dụng Web Mở (Open Web Application Security Project - OWASP) là tiêu chuẩn được công nhận nhiều nhất trong ngành. Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (National Institute of Security and Technology - NIST) đã phát hành SP 800-115, "Hướng dẫn Kỹ thuật để Kiểm tra và Đánh giá Bảo mật Thông tin", bao gồm sơ đồ quy trình cơ

bản được thể hiện trong [Hình 8-1](#). Khuôn khổ Tiêu chuẩn và Phương pháp Kiểm nghiệm Xâm nhập (Penetration Testing Methodology and Standard - PTES) và Khuôn khổ Đánh giá Bảo mật Hệ thống Thông tin (Information System Security Assessment Framework - ISSAF) là hai khuôn khổ bổ sung phổ biến. Tất cả các khuôn khổ này xác định một quy trình, với mô hình NIST là đơn giản nhất. Tầm quan trọng của mô hình quy trình là có một kế hoạch mà tất cả các thành viên trong nhóm có thể sử dụng để hiểu họ đang ở đâu trong quy trình và mối quan hệ giữa các nhiệm vụ chính.



**Hình 8.1** – Mô hình quy trình Kiểm nghiệm Xâm nhập NIST từ SP 800-115

### Môi trường đã xác định

Kiểm nghiệm môi trường đã xác định (hộp trắng) gần như là cực đối lập với kiểm nghiệm môi trường chưa xác định (hộp đen) (sẽ được thảo luận tiếp theo). Đôi khi còn được gọi là *kiểm nghiệm hộp rõ ràng (clear box testing)*, các kỹ thuật hộp trắng kiểm tra cấu trúc bên trong và xử lý trong phạm vi một ứng dụng để tìm kiếm các lỗi, các lỗ hổng, v.v... Một chuyên gia kiểm nghiệp hộp trắng sẽ có những kiến thức chi tiết về ứng

dụng mà họ đang kiểm tra – họ sẽ phát triển các kịch bản kiểm tra được thiết kế để kiểm tra từng đường dẫn, cây quyết định, trường dữ liệu đầu vào, và thủ tục xử lý của ứng dụng.

Kiểm nghiệm môi trường đã xác định thường được sử dụng để kiểm tra các đường dẫn trong một ứng dụng (nếu X thì thực hiện điều này, nếu Y thì thực hiện điều kia), luồng dữ liệu, cây quyết định, v.v... Thỉnh thoảng, thuật ngữ *kiểm nghiệm hộp trắng* được áp dụng cho các quá trình đánh giá hệ thống mạng khi chuyên gia kiểm nghiệm sẽ có những kiến thức chi tiết về hệ thống mạng, bao gồm nhưng không giới hạn, các địa chỉ IP, định tuyến mạng, và những thông tin đăng nhập người dùng hợp lệ.

### **Môi trường chưa xác định**

*Kiểm nghiệm môi trường chưa xác định (hộp đen)* là một kỹ thuật kiểm-nghiệm-phần-mềm bao gồm việc tìm kiếm những lỗi triển khai bằng cách sử dụng chèn dữ liệu dị dạng/bán dị dạng theo cách tự động hóa. Các kỹ thuật môi trường chưa xác định kiểm tra chức năng của phần mềm, thường từ một quan điểm bên ngoài hoặc quan điểm của người dùng. Người kiểm tra sử dụng kỹ thuật hộp đen thường không có đủ kiến thức về hoạt động bên trong của phần mềm mà họ đang kiểm tra. Họ coi toàn bộ gói phần mềm như một là "hộp đen" - họ đưa đầu vào và xem kết quả đầu ra. Họ không có khả năng hiển thị về cách thức dữ liệu được xử lý bên trong ứng dụng như thế nào, chỉ có kết quả đầu ra được trả về cho họ. Các trường hợp kiểm nghiệm để kiểm tra môi trường chưa xác định thường được xây dựng xung quanh chức năng đã dự kiến (những gì phần mềm được cho là phải thực hiện) và tập trung vào việc cung cấp cả đầu vào hợp lệ và không hợp lệ.

Các kỹ thuật kiểm nghiệm phần mềm môi trường chưa xác định rất hữu ích để kiểm tra bất kỳ ứng dụng dựa-trên-nền-web nào, các ứng dụng này thường phải chịu một loạt các đầu vào hợp lệ, không hợp lệ, không

đúng định dạng và độc hại ngay từ khi chúng tiếp xúc với lưu lượng truy cập công cộng. Bằng cách thực hiện việc kiểm nghiệm môi trường chưa xác định trước khi ứng dụng được phát hành, các nhà phát triển có thể có khả năng tìm và sửa các lỗi trong giai đoạn phát triển hoặc thử nghiệm.

Kiểm nghiệm môi trường chưa xác định cũng có thể được áp dụng cho các mạng hoặc các hệ thống. Các bài kiểm nghiệm xâm nhập và đánh giá lỗ hổng thường được thực hiện từ góc độ bên ngoài hoàn toàn, khi người kiểm tra không có kiến thức bên trong về mạng hoặc hệ thống mà họ đang kiểm tra.

### **Môi trường đã xác định Một phần**

Vậy điều gì xảy ra nếu bạn pha trộn một chút kiểm nghiệm môi trường đã xác định và một chút kiểm nghiệm môi trường chưa xác định? Bạn sẽ có cái được gọi là kiểm nghiệm môi trường đã xác định một phần (hộp xám). Trong một kiểm nghiệm *môi trường đã xác định một phần*, người kiểm tra thường sẽ có một ít kiến thức về phần mềm, mạng, hoặc các hệ thống mà họ đang kiểm tra. Vì lý do này, kiểm nghiệm môi trường đã xác định một phần có thể rất có hiệu quả và hiệu suất bởi vì những người kiểm tra thường có thể nhanh chóng loại bỏ toàn bộ các đường dẫn kiểm tra, các trường hợp kiểm nghiệm, và các bộ công cụ và có thể loại trừ những thứ đơn giản là không hoạt động hoặc không đáng để kiểm tra.



### **MÁCH NƯỚC CHO KỲ THI**

Sự khác biệt chính giữa kiểm nghiệm môi trường đã xác định, xác định một phần và chưa xác định là góc nhìn và kiến thức của người kiểm tra. Những người kiểm tra môi trường chưa xác định không có kiến thức về những hoạt động bên trong và thực hiện các kiểm nghiệm của họ từ một góc nhìn bên ngoài. Các chuyên gia kiểm tra môi trường đã xác định có kiến thức chi tiết về những hoạt động bên

trong và thực hiện các kiểm tra của họ từ một góc nhìn bên trong nội bộ. Những người kiểm tra các môi trường đã xác định một phần có một phần kiến thức [về những hệ thống và hoạt động bên trong]. Đây là một sự tách biệt khỏi yếu tố ủy quyền: các hoạt động đã được ủy quyền (mũ trắng) so với trái phép (mũ đen).

### Các Quy tắc Tham gia

*Các quy tắc tham gia* tương ứng với một kiểm nghiệm xâm nhập là điều tối quan trọng vì một vài nguyên nhân. Đầu tiên và quan trọng nhất, các hoạt động liên quan đến kiểm tra xâm nhập sẽ là bất hợp pháp nếu không được cho phép và các quy tắc tham gia chỉ rõ thẩm quyền pháp lý mà người kiểm tra xâm nhập sẽ có trong việc thực hiện nhiệm vụ của họ. Các quy tắc tham gia cũng thiết lập nên các ranh giới liên quan đến thử nghiệm để việc kiểm nghiệm thực sự thực hiện kiểm tra các chức năng mà khách hàng mong muốn. Nếu một chuyên gia kiểm tra xâm nhập thực hiện các hoạt động nằm ngoài các quy tắc tham gia, chúng có thể sẽ không có giá trị gì đối với doanh nghiệp và do đó gây ra sự lãng phí nỗ lực, và trong nhiều trường hợp có thể gây ra vấn đề. Trong trường hợp chức năng ứng phó sự cố của doanh nghiệp là một phần của kiểm nghiệm hoặc đã được thông báo là bỏ qua các hoạt động cụ thể, thì việc điều phối thông tin này thông qua các quy tắc tham gia và quản lý đang sử dụng thích hợp là điều cần thiết. Việc nhóm phản ứng sự cố (IR) được kích hoạt và tiêu tốn năng lượng khi không phải là một phần của kiểm nghiệm sẽ gây ra lãng phí đối với một nhóm lớn hơn là chỉ cho nhóm [kiểm nghiệm] xâm nhập.

Các quy tắc tham gia điển hình sẽ bao gồm một ranh giới của những gì thuộc phạm vi [kiểm nghiệm] và những gì không. Nếu các địa chỉ IP của máy đang được cung cấp cho nhóm kiểm tra xâm nhập, thì danh sách các địa chỉ nằm trong và ngoài giới hạn sẽ được cung cấp. Nếu các máy trong

phạm vi được phát hiện thì một ký hiệu rõ ràng về những gì không nằm trong giới hạn là cần thiết. Các mục khác có thể là các yếu tố như thời gian của hoạt động kiểm nghiệm. Bạn có thể không nên thực hiện kiểm tra trong thời gian kinh doanh bận rộn vì các vấn đề về băng thông và tải trọng xử lý. Phạm vi của các hoạt động sẽ được thực hiện rõ ràng phải là không gây ra thiệt hại trong khi kiểm nghiệm, nhưng điều gì tạo nên bằng chứng về sự xâm phạm cần phải được xác định. Bất kỳ thay đổi nào đối với môi trường cần phải được lưu ý và loại bỏ hoặc cung cấp rõ ràng cho nhóm xanh lam (blue team). Cách thức người kiểm tra xâm nhập nên tương tác với các nhân viên khác khi được phát hiện cũng nên được đưa vào, cũng như danh sách liên hệ đầy đủ để gọi cho ai đó khi có điều gì đó xảy ra đòi hỏi sự chú ý của doanh nghiệp ngay lập tức.

### **Chuyển động Bên rìa**

*Chuyển động bên rìa*, đôi khi còn được gọi là *chuyển động bên rìa [hệ thống] mạng*, đề cập đến tiến trình được sử dụng bởi những kẻ tấn công để di chuyển sâu hơn vào trong một hệ thống mạng để đánh cắp được dữ liệu mục tiêu. Trong hầu hết các trường hợp, điểm truy nhập ban đầu vào một hệ thống là thông qua một tài khoản người dùng không có quyền tiếp cận vào tài liệu mong muốn, hoặc tài khoản không mức quyền hạn truy cập không tương ứng. Thông qua một loạt các hành động cụ thể, một kẻ tấn công có thể leo thang mức độ đặc quyền của chúng, như được trình bày trong phần tiếp theo, đồng thời chuyển các máy khác vào sâu hơn trong hệ thống mạng. Tiến trình di chuyển ngang qua một hệ thống mạng được gọi là *chuyển động bên rìa* và là một sự kiện phổ biến đối với những kẻ tấn công được tăng cường. Nó cũng đại diện cho một trong những điểm nơi mà những người phòng thủ có thể bắt được một kẻ tấn công, bởi vì trong hầu hết các trường hợp, những chuyển động bên rìa không phải là những hoạt động bình thường đối với tài khoản người dùng đang được sử dụng.

## Leo thang Đặc quyền

*Leo thang đặc quyền* là tiến trình có được đặc quyền được gia tăng đối với một tài khoản. Việc này có thể được thực hiện theo nhiều cách thức khác nhau – đôi khi là hợp pháp, đôi khi thông qua một lỗ hổng. Việc có được quyền truy cập root hoặc admin luôn là một mục tiêu của một kẻ tấn công, bởi vì điều này mang lại cho chúng những quyền lực bổ sung trên một hệ thống khiến cho công việc của chúng trở nên dễ dàng hơn và mở ra những đường dẫn mà nếu không thì đang bị đóng lại với chúng. Những đường dẫn đối với leo thang đặc quyền đối với một chuyên gian kiểm nghiệm xâm nhập bao gồm những thứ chẳng hạn như sử dụng một tài khoản quản trị viên cục bộ, đánh cắp thông tin đăng nhập đối với một tài khoản có quyền của quản trị viên, và khai thác một lỗ hổng dẫn đến sự leo thang đặc quyền.

Một vài trong số những đường dẫn đó rất dễ ngăn chặn – khóa các tài khoản quản trị viên cục bộ và giới hạn đáng kể số lượng người dùng với bản chất quản trị viên là điều rất quan trọng. Ngoài ra, việc giám sát một số sự kiện quản trị chẳng hạn như tạo tài khoản và leo thang tài khoản có thể cho phép những người phòng thủ xem xét khi một kẻ tấn công sử dụng một đặc quyền đã được leo thang cho những hành động cụ thể.

Có hai kiểu leo thang đặc quyền: theo chiều ngang và theo chiều dọc. Trong leo thang đặc quyền theo chiều ngang, kẻ tấn công mở rộng đặc quyền của chúng bằng cách chiếm đoạt tài khoản khác và lạm dụng những đặc quyền hợp pháp đã được cấp cho người dùng khác. Điều này thường được thực hiện cùng với chuyển động bên rìa. Đây cũng là lý do tại sao việc giới hạn các tài khoản với quyền truy cập quản trị lại rất quan trọng, vì nó làm giảm thiểu các đích nhắm mục tiêu cho leo thang đặc quyền theo chiều ngang.

Với leo thang đặc quyền theo chiều dọc, kẻ tấn công có thể được nhiều quyền hạn hoặc quyền truy cập trong phạm vi một tài khoản hiện hữu mà chúng đã xâm phạm. Một kẻ tấn công sử dụng một tài khoản mức người-dùng thông thường trên một hệ thống mạng có thể cỗ gắng có được quyền quản trị thông qua việc khai thác các lỗ hổng trong những tiến trình hoặc dịch vụ đang chạy với đặc quyền quản trị. Đây là lý do vì sao việc hạn chế số lượng các tiến trình hoặc dịch vụ với quyền quản trị là điều quan trọng, vì nó làm giảm thiểu thiểu khả năng bẻ mặt này. Leo thang đặc quyền theo chiều dọc đòi hỏi kỹ thuật tinh vi hơn và là kỹ thuật chính được sử dụng bởi các mối đe dọa dai dẳng được tăng cường (APTs).

### Bền bỉ

*Bền bỉ* là khả năng tồn tại sau khi một máy được khởi động lại hoặc sau khi bị ngắt kết nối. Thuật ngữ *mối đe dọa dai dẳng được tăng cường (APT)* đề cập đến một phương pháp tập trung trước hết và quan trọng nhất vào việc duy trì tính bền bỉ (dai dẳng). Điều này có nghĩa là kẻ tấn công có thể và sẽ quay trở lại hệ thống mạng, và cùng với việc sử dụng những cơ chế dai dẳng hiệu quả và các tài khoản khác, sẽ không quan sát được khi chúng xâm nhập trở lại. Tính bền bỉ có thể đạt được thông qua một loạt các cơ chế, chẳng hạn như bằng cách tạo ra các tài khoản giả mạo, cài đặt các cổng hậu, sử dụng các bot gọi ra ngoài thông qua mạng để cho phép một kẻ tấn công có một phương tiện để quay trở lại hệ thống mạng, và thao túng những mục Hệ điều hành (OS) chẳng hạn như các Thư viện Liên kết Động (DLL) hoặc những quyền hạn.



**MÁCH NƯỚC CHO KỲ THI** Chuyển động bên rìa, leo thang đặc quyền và tính bền bỉ là những công cụ phổ biến trong hộp công cụ của những kẻ tấn công và những chuyên gia kiểm nghiệm xâm nhập. Chúng

thường được sử dụng cùng với nhau, nhưng từng công cụ đều có những được đặc tính độc đáo. Đối với những câu hỏi có liên quan đến chúng, hãy chắc chắn đã kiểm tra những đặc tính độc đáo mà câu hỏi đang đề cập nhằm chọn được đáp án chính xác.

### **Dọn dẹp**

Việc tấn công một hệ thống có thể để lại rất nhiều bằng chứng nằm rải rác. Việc kiểm tra các lỗ hổng và cố gắng thử hệ thống kiểm soát truy cập tạo ra một loạt những sự kiện thất bại liên quan đến kiểm nghiệm xâm nhập và tấn công hệ thống. Một trong những bước quan trọng có thể được thực hiện để tránh bị phát hiện là dọn dẹp những thứ mà bạn đã tạo ra. *Dọn dẹp*, hoặc che đậy dấu vết của một người là một bước thiết yếu trong bộ công cụ của một chuyên gia. Việc xóa nhật ký, chặn ghi nhật ký từ xa, làm xáo trộn lịch sử hệ thống và sử dụng các shell đảo ngược và đường hầm Giao thức Thông điệp Kiểm soát Internet (ICMP) để tránh bị phát hiện và ghi nhật ký là một trong số các phương pháp được sử dụng. Việc sử dụng rootkit hoặc trojan để sửa đổi hệ điều hành để từ đó, các hoạt động dựa trên tài khoản cụ thể không được ghi lại là một trong những phương pháp được sử dụng bởi các cuộc tấn công APT. Khi một kẻ tấn công di chuyển ngang trong mạng và leo thang đặc quyền, việc che giấu dấu vết của chúng phía sau khiến người phòng thủ rất khó tìm ra kẻ tấn công khi chúng đã chuyển sang một tài khoản khác hoặc một máy khác.

### **Săn lỗi để Nhận thưởng (Bug Bounty)**

Các chương trình *săn lỗi để nhận thưởng* là các cơ chế khi các công ty trả tiền cho tin tức để phát hiện ra những chi tiết về lỗ hổng mà họ khám phá được, mang lại cho các công ty cơ hội để khắc phục các vấn đề. Hầu hết tiền thưởng cho lỗi đều trả một số hình thức phần thưởng bằng tiền mặt, với một số công ty lớn như Microsoft, Apple và Google trả phần

thưởng lên tới sáu chữ số cho các lỗ hổng rất nghiêm trọng. Một trong những yếu tố quan trọng cần hiểu là để khiếu nại việc săn lỗi trở thành hợp pháp, công ty phải có một chương trình săn lỗi để nhận tiền thưởng đã được thiết lập và hoạt động săn lỗi phải thích hợp với chương trình đó. Việc truy cập vào hệ thống và khai thác lỗ hổng bảo mật trên mạng của người khác hoặc công ty khác mà không được phép là một tội ác và chương trình săn lỗi nhận thưởng có thể cung cấp quyền như vậy nếu nó được tuân thủ một cách đúng đắn. Việc tìm ra lỗ hổng bảo mật và cố gắng bán nó cho một công ty không có chương trình tiền thưởng lỗ thường gặp phải phản ứng pháp lý rất mạnh và có khả năng bị điều tra tội phạm.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng một chương trình săn lỗi nhận thưởng là một phương pháp tiếp cận chính thức để xác định các lỗi. Những chương trình này thường được mở công khai, và công ty chạy chương trình sẽ xác lập các quy tắc tham gia.

### Pivoting

*Pivoting [di chuyển bên trong một mạng]* là một kỹ thuật tương tự như di chuyển bên rìa. Trong pivoting, một ai đó di chuyển đến một vị trí mới trong một mạng và bắt đầu lại tiến trình tấn công, thực hiện quá trình quét để tìm kiếm những máy không hữu hình đối với bên ngoài. Toàn bộ mục đích của di chuyển bên rìa là để đi đến nơi đang chứa dữ liệu, và pivoting là một trong những phương pháp chủ yếu về việc tìm hiểu nơi di chuyển đến tiếp theo. Tiến trình hoạt động như sau: Có được chỗ đặt chân ban đầu dựa trên những gì bạn có thể thấy và thực hiện từ bên ngoài hệ thống mạng. Sau đó, từ máy mới này bên trong hệ thống mạng, hãy bắt đầu lại quá trình và di chuyển sâu hơn. Dọn sạch và lặp lại. Để

vượt qua một mảng con được sàng lọc (Demilitarized Zone - DMZ) sẽ cần một vài lần di chuyển trong mạng (pivot). Để di chuyển vào một vùng được bảo vệ cần một hoặc hai pivot khác. Xoay, di chuyển, xoay lại, lại di chuyển — đây là cách kẻ tấn công hoặc người kiểm nghiệm xâm nhập xâm nhập sâu hơn vào trong mạng.

Một trong những dấu hiệu của hoạt động này là việc quét nội bộ. Mặc dù người ta thường nhận thấy nhiều lần quét xảy ra bên ngoài mạng, nhưng một khi kẻ tấn công ở bên trong mạng ở một khu vực không có lý do chính đáng cho hoạt động quét, quá trình quét cho thấy rằng ai đó đang "tìm kiếm". Làm chậm quá trình quét của họ là một phương pháp mà kẻ tấn công có thể sử dụng để tránh bị phát hiện, nhưng điều này làm kéo dài thời gian tham gia của họ, đây là một yếu tố chi phí cho những người kiểm nghiệm xâm nhập nhưng không nhất thiết là một đối với APT.



**MÁCH NƯỚC CHO KỲ THI** Di chuyển bên rìa và pivoting hoạt động cùng với nhau. Mục đích của di chuyển bên rìa là để đi đến nơi chứa dữ liệu và pivoting là một trong những phương pháp chủ yếu để tìm hiểu về nơi sẽ di chuyển đến tiếp theo đó.

### **Do thám Chủ động và Thụ động**

Do thám có thể là một trong hai kiểu: thu động hoặc chủ động. *Do thám thụ động* được thực hiện bằng cách sử dụng những phương pháp để có được thông tin về các máy tính và mạng được nhắm mục tiêu mà không tham gia một cách chủ động vào các hệ thống mục tiêu và do đó tránh bị phát hiện. Sử dụng những nghiên cứu từ Google và những kho chứa dữ liệu bên-thứ-ba như các hồ sơ đăng ký DNS và IP là những kỹ thuật mà kẻ tấn công có thể sử dụng để cung cấp rất nhiều thông tin mà thậm chí

không cần phải tiếp xúc với các mục tiêu, từ đó hoàn toàn tránh được việc bị phát hiện.

Trong *do thám chủ động*, kẻ tấn công liên quan đến các hệ thống mục tiêu, thường bằng việc tiến hành một tiến trình quét các cổng để tìm ra bất kỳ cổng đang mở nào. Do thám chủ động liên quan đến việc sử dụng các gói tin có thể được truy nguyên, nó liên quan đến việc dính líu đến các dịch vụ có thể được ghi nhật ký. Ngoài ra, khi do thám chủ động tấn công một máy được thiết lập như một bẫy mật ong (honey trap), nó cung cấp những bằng chứng về các hoạt động trông có vẻ như hợp pháp nhưng thực tế là bất hợp pháp, bởi vì những thiết bị này đặc biệt không được sử dụng như là một phần của doanh nghiệp – ngoại trừ việc đây là một cái bẫy.

Do thám thụ động có những giới hạn về việc lượng [thông tin] mà một kẻ tấn công có thể tìm hiểu nhiều đến mức nào, nhưng nó hoàn toàn lút. Do thám chủ động còn nhiều hơn là cung cấp thông tin, mà nó còn nói cho các máy móc rằng chúng đang bị "tấn công". Chìa khóa là sử dụng do thám thụ động trước, sau đó chỉ sử dụng do thám chủ động khi cần thiết để hoàn thành công việc. Khi một kẻ tấn công lén vào một hệ thống mạng, trở nên âm thầm lặng lẽ là điều rất quan trọng.



**MÁCH NƯỚC CHO KỲ THI** Hãy chắc chắn nắm được sự khác biệt giữa các kỹ thuật do thám thụ động và do thám chủ động, vì đây là một câu hỏi kiểm tra khá dễ. Do thám thụ động là lén lút và không liên quan một cách chủ động vào hệ thống mục tiêu. Do thám chủ động tham gia vào hệ thống hoặc mạng và có thể thu thập được nhiều thông tin, nhưng nó cũng vẫn có thể được truy nguyên.

## Drones

Các drone là những thiết bị bay không người lái có khả năng mang theo máy quay phim, thiết bị di động, và các vật dụng khác qua những ranh giới bình thường như các bức tường, hàng rào, và các trạm kiểm soát. Điều này mang lại cho người kiểm nghiệm xâm nhập một phương tiện để tiến gần hơn đến các tín hiệu chẳng hạn như các mạng không dây và sau đó ghi nhận lại lưu lượng. Mặc dù việc sử dụng các máy bay không người lái để bắt lưu lượng mạng trông có vẻ khó hiểu nhưng kỹ thuật này có một tên gọi, chiến tranh bay (*war flying*), và nó được mô tả trong phần tiếp theo.

## War Flying

Việc sử dụng một thiết bị không người lái bay qua một cơ sở vật chất và bắt lưu lượng mạng không dây được gọi là *chiến tranh bay (war flying)*. Ví dụ, nếu một văn phòng nằm ở tầng 28 của một tòa nhà, với thang máy và truy cập vật lý bị giới hạn, việc cho một thiết bị không người lái bay lên bên ngoài cửa sổ có thể mang lại cho người kiểm nghiệm xâm nhập quyền tiếp cận tới tín hiệu không dây, vốn không thể tiếp cận từ tầng trệt. Và mặc dù việc cho một thiết bị không người lái bay qua một địa điểm nhạy cảm như một cơ sở quân sự có thể không được khuyến cáo, tuy nhiên việc thực hiện điều này trong khu vực đô thị để có được quyền truy cập, bao gồm tiếp cận trực quan qua cửa sổ, không phải là điều hiếm có như người ta có thể tưởng tượng. Những gì bạn có thể sử dụng thiết bị bay không người lái bị giới hạn bởi trí tưởng tượng của bạn. Hãy chỉ tưởng tượng rằng nếu như bạn có thể định vị máy trạm của mình ở nơi bạn đặt thiết bị bay không người lái của bạn – bạn có thể nhìn thấy và tương tác với những gì? Bạn có thể có khả năng bắt được những gói tin cùng với mật khẩu, ví dụ, bởi vì trong những câu chuyện ở tầng 28 trong không khí, không ai lo lắng gì về những kẻ nghe lén. Bạn có thể bắt được tên máy tính, các địa chỉ IP, và còn hơn thế nữa.

## War Driving

*Chiến tranh lái xe (war driving)* là một khái niệm tương tự như chiến tranh bay nói trên, nhưng thay vì sử dụng một thiết bị bay không người lái để bắt lưu lượng, chiến tranh lái xe chỉ đơn giản là lái xe qua các điểm truy cập. Việc lập bản đồ các điểm truy cập, bao gồm những thông tin địa lý, đã trở thành một hoạt động phổ biến, với rất nhiều bản đồ như vậy thực sự đã được công bố trực tuyến. Dù là mục tiêu của một kiểm nghiệm xâm nhập chỉ nằm trong phạm vi khu vực đã được lập bản đồ hay bạn sử dụng các điểm truy cập ẩn danh để ẩn giấu vị trí của bạn, việc tìm kiếm và sử dụng các điểm truy cập mở là một công cụ hữu ích trong bộ công cụ kiểm nghiệm xâm nhập của bạn. Có rất nhiều gói phần mềm hỗ trợ cho các chức năng chiến tranh lái xe, và bộ tính năng của một vài trong số những gói phần mềm này đã trở nên khá phổ biến, bao gồm cả việc bổ sung những thông tin địa lý cũng như các cơ sở dữ liệu tòa nhà của siêu dữ liệu được liên kết với một điểm truy cập mở.

Chiến tranh lái xe là một kỹ thuật kế tiếp của chiến tranh đánh dấu (war chalking), vốn là việc đánh dấu lề đường và vỉa hè bằng phấn để tạo ra các đại diện tượng trưng cho các mạng không dây mở được quan sát thấy trong khu vực. Đây là một tập hợp các dấu hiệu hobo hiện đại, cung cấp thông tin cho những người bạn đồng hành về vị trí và tính khả dụng của các mạng không dây mở.

Một biến thể khác của các phương pháp tấn công này là chiến tranh vận chuyển, trong đó kẻ tấn công vận chuyển một điện thoại di động được thiết lập một cách đặc biệt đến một địa điểm. Thiết bị này có pin bên ngoài lớn và một phần mềm đặc biệt. Điện thoại liên tục chạy và thu thập dữ liệu mạng, và theo các khoảng thời gian định kỳ, nó sử dụng khả năng di động của mình để đóng gói và gửi đi hàng loạt dữ liệu đã thu thập được. Nếu bạn chuyển một chiếc điện thoại cho một ai đó khi họ đang trong kỳ nghỉ, ví dụ, chiếc hộp điện thoại có thể nằm trên bàn của nạn

nhân trong vài ngày, không được mở ra, trong khi đó thiết bị nghe lén ghi lại và gửi đi lưu lượng trong những ngày đó. Một lần nữa, đây là một phương pháp vượt qua các cổng và nhân viên an ninh, và bị ngăn chặn một cách dễ dàng nếu như một phòng thư trung tâm mở tất cả các gói hàng và kiểm tra nội dung của chúng.

## **Footprinting**

*Footprinting*, còn được gọi là *do thám*, là bước đầu tiên trong việc thu thập thông tin chủ động trên một hệ thống mạng. Sử dụng footprinting, một người kiểm nghiệm xâm nhập có thể thu thập thông tin về các hệ thống máy tính và các thực thể mà chúng [các hệ thống máy tính] thuộc về, và trong một số trường hợp, là những thông tin người dùng. Phương pháp chủ yếu để thu thập những thông tin này là thông qua thu thập (sniffing) tín hiệu mạng và sử dụng các phần mềm quét. Khi một mạng được lập bản đồ thông qua việc do thám, người kiểm nghiệm xâm nhập có thể đưa ra quyết định về việc những máy nào để thực hiện lập bản đồ lõi hổng, và trong một số trường hợp, những máy nào cần tránh, ví dụ như các honeypots.



## **MÁCH NƯỚC CHO KỲ THI**

Footprinting là bước đầu tiên trong việc thu thập những thông tin chủ động trên một hệ thống mạng trong quá trình do thám.

## **OSINT**

*OSINT* (*thông tin tình báo nguồn mở*) là kỹ thuật sử dụng những nguồn thông tin sẵn có công khai để thu thập thông tin về một hệ thống. OSINT không phải là phương pháp đơn lẻ mà là một tập hợp toàn bộ các phương pháp định tính và định lượng có thể được sử dụng để thu thập những thông tin hữu ích. Nếu như một cuộc tấn công dự định sẽ sử dụng các

phương pháp kỹ thuật xã hội, thì các bước OSINT được sử dụng để thu thập thông tin về người dùng và tìm kiếm các phương pháp sẽ cải thiện tỷ lệ thành công của chiến dịch. Nếu mục tiêu là các máy tính mạng thì có thể hữu ích khi thu thập thông tin từ các trang web như nhà đăng ký địa chỉ IP, máy chủ DNS cho địa chỉ của máy chủ thư và các hệ thống bên ngoài khác yêu cầu địa chỉ của chúng phải được biết để có thể hoạt động.

Các mục chẳng hạn như những thông báo PR từ một công ty về việc họ áp dụng một phần mềm mới có thể cung cấp cho những người kiểm nghiệm xâm nhập những thông tin vô giá về các hệ thống mà họ đang tìm kiếm. Từ việc nhân viên đăng trên phương tiện xã hội cho đến các bài đăng của bộ phận Nhân sự về những vị trí công việc đang mở, danh sách các nguồn tiềm năng và mức độ chi tiết tương ứng với thông tin có thể rất đáng kể và, trong rất nhiều trường hợp, cực kỳ hữu ích. Tại thời điểm bắt đầu, một người kiểm nghiệm xâm nhập có thể không có chút kiến thức nào về một hệ thống và các thành phần của nó, tuy nhiên sau một vài hoạt động OSINT, mức độ của thông tin có thể gia tăng một cách đáng kể, từ đó thay đổi kiểu truy nhập môi trường chưa xác định (hộp đen) thành ít nhất là kiểu truy nhập môi trường đã xác định một phần (hộp xám).



## MÁCH NƯỚC CHO KỲ THI

OSINT mô tả việc sử dụng những nguồn thông tin công khai để thu thập những thông tin về một mục tiêu và tìm kiếm những phương pháp sẽ làm gia tăng tỷ lệ thành công của một chiến dịch.

### Các kiểu Bài tập

Các kiểu bài tập bảo mật bao gồm những bài tập tập trung vào biện pháp tấn công, biện pháp phòng thủ hoặc sự kết hợp giữa tấn công và phòng thủ. Những màu sắc khác nhau được sử dụng chỉ rõ các nhóm khác nhau

tham gia vào một bài tập. Những bài tập này có thể được tạo ra để kiểm tra các khía cạnh khác nhau – từ kỹ thuật cho đến quản lý cho đến các hành động quản lý cấp-cao-nhất. Mục tiêu của các bài tập là để kiểm tra khả năng, kỹ năng thực tế, các phương án học tập, và phát triển các chiến lược trong một môi trường không đe dọa.

### **Nhóm Đỏ**

Các nhóm đỏ được cấu thành từ những thành viên tập trung vào tấn công. Các thành viên của nhóm đỏ sử dụng các kỹ năng của họ để bắt chước một môi trường mối đe dọa trong thế-giới-thực và cung cấp một bài kiểm tra năng lực phòng thủ của một công ty. Các nhóm đỏ thường là các nhà thầu bên-thứ-ba, vì bộ kỹ năng của họ được chuyên môn hóa và mức kỹ năng cần thiết là cao. Tùy thuộc vào phạm vi của một bài tập, các thành viên của nhóm đỏ có thể sẽ khác nhau theo các hệ thống và giao thức đang được kiểm tra, và việc có được nhiều cá nhân có kinh nghiệm là một nguyên nhân khác lý giải cho việc tại sao hầu hết công việc của nhóm đỏ được thuê ngoài cho những công ty chuyên về lĩnh vực này và giữ các nhóm cho các hợp đồng.

### **Nhóm Xanh dương**

Nhóm xanh dương là một nhóm phòng thủ và, do vậy, thường là một hoạt động trong nội bộ, trừ khi những nỗ lực phòng thủ được thuê ngoài. Khi bạn thuê ngoài những biện pháp phòng thủ của bạn, việc này bổ sung thêm một lớp phức tạp vào việc sử dụng các bài tập, vì hoạt động này sẽ phải được thương lượng và ký hợp đồng với nhà cung cấp bảo mật được thuê ngoài của bạn. Các thành viên của nhóm xanh dương đến từ các bộ phận CNTT và vận hành bảo mật, và họ thường thực hiện cả hai chức năng. Đầu tiên là thiết lập nền các biện pháp phòng thủ, thiết lập cấu hình của các phần tử phòng thủ như các tường lửa và các thiết bị bảo mật, quản lý các quyền, và ghi nhật ký. Việc thứ hai có liên quan đến các

chức năng giám sát và ứng phó sự cố. Trong vai trò này, họ canh chừng các cuộc tấn công và quản lý phản ứng của hệ thống đối với bất kỳ hành vi trái phép nào được quan sát thấy.

### Nhóm Trắng

Khi một bài tập liên quan đến việc chấm điểm và/hoặc quan điểm cạnh tranh, nhóm đánh giá được gọi là *nhóm trắng*. Nếu bài tập đòi hỏi phải có một nhóm điều phối viên bên ngoài để quản lý nó, độc lập với nhóm phòng thủ thì những người điều phối này cũng được gọi là nhóm trắng. Các thành viên của nhóm trắng ở đó để đảm bảo rằng bài tập thực sự đi đúng hướng và sử dụng các yếu tố mong muốn của một hệ thống.

### Nhóm Tím

Một *nhóm tím* được cấu thành từ cả các thành viên của nhóm đó và nhóm xanh dương. Những thành viên này làm việc cùng nhau để thiết lập và kiểm tra các biện pháp phòng thủ. Rất nhiều lần, khi bạn giao tranh với nhóm đỏ của bên-thứ-ba, nhóm này sẽ bao gồm một vài thành viên trong nhóm xanh dương để giúp quản lý ứng phó của nhóm của bạn đối với các véc-tơ tấn công đang được sử dụng. Đôi khi, việc để một thành viên trong nhóm đỏ làm việc với nhóm xanh dương của bạn cũng có thể hữu ích, giúp họ hiểu được các bước tiếp theo từ quan điểm của nhóm đỏ (kẻ tấn công). Mục tiêu của tất cả các nhóm thực tập là cải thiện thế trận an ninh mạng của một công ty và việc có các chuyên gia phù hợp ở cả hai bên để giúp đào tạo các chiến lược và hoạt động tổng thể của nhóm xanh dương của một công ty là một phương pháp hiệu quả để nâng cao năng lực phòng thủ.



### MÁCH NƯỚC CHO KỲ THI

Hãy nhớ rằng nhóm đỏ là kẻ tấn công, nhóm xanh dương là những người phòng thủ, nhóm trắng là người đánh



ADMINISTRATION & SECURITY  
VIETNAM

giá/nhà quản lý bài tập, và nhóm tím được cấu thành từ các thành viên của nhóm đỏ và nhóm xanh dương.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các công cụ và kỹ thuật của những người kiểm tra xâm nhập. Chương được mở đầu bằng việc kiểm tra kiểm nghiệm xâm nhập và các đặc tính của môi trường. Phần đầu tiên bao gồm thông tin về các môi trường đã xác định, chưa xác định và đã xác định một phần và đặc điểm của từng môi trường. Sau đó, các quy tắc tham gia được đề cập, tiếp theo là các kỹ thuật di chuyển bên rìa và leo thang đặc quyền. Các chủ đề về tính bền bỉ và dọn dẹp cũng được đề cập đến. Các chương trình tiền thường để săn tìm lối và pivoting đã kết thúc phần chính đầu tiên.

Việc kiểm tra các công cụ và kỹ thuật do thám chủ động và thụ động đã được đề cập trong phần chính tiếp theo. Các chủ đề bao gồm máy bay không người lái, chiến tranh bay, chiến tranh lái xe và footprinting. Phần này kết thúc bằng một cuộc thảo luận về thông tin tình báo nguồn mở (OSINT).

Chương này khép lại với phần kiểm tra các dạng bài tập khác nhau và các nhóm được sử dụng trong các bài tập này. Phần này bao gồm thành phần và sử dụng các nhóm màu đỏ, xanh dương, trắng và tím.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Nhóm nào dưới đây thường được sử dụng cho kiểm nghiệm xâm nhập chủ động?

  - A. Nhóm đỏ
  - B. Nhóm xanh dương
  - C. Nhóm trắng
  - D. Nhóm tím.
2. Chiến tranh bay là thuật ngữ để mô tả điều nào dưới đây?

  - A. Kiểm nghiệm xâm nhập trên các máy bay thương mại
  - B. Sử dụng các nền tảng trên không để có được quyền truy cập và các mạng không dây
  - C. Lái xe xung quanh và lấy mẫu các mạng Wi-Fi mở
  - D. Sử dụng các kỹ thuật kiểm nghiệm xâm nhập để chống lại Bộ Quốc phòng.
3. Khi một kẻ tấn công di chuyển qua một máy mới và quét lại mạng để tìm kiếm những máy không hiển thị trước đó, kỹ thuật này được gọi là gì?

  - A. Di chuyển bên rìa
  - B. Leo thang đặc quyền
  - C. Tính bền bỉ
  - D. Pivoting.
4. Bước đầu tiên quan trọng nhất trong một kiểm nghiệm xâm nhập là gì?

  - A. OSINT
  - B. Quy tắc tham gia

- C. Do thám**
- D. Leo thang đặc quyền.**
- 5.** Việc che đậy dấu vết của một ai đó để ngăn chặn việc bị phát hiện còn được gọi là gì?
- A. Di chuyển bên rìa**
- B. OSINT**
- C. Dọn dẹp**
- D. Pivoting.**
- 6.** Khi một người kiểm nghiệm xâm nhập sử dụng OSINT để thu thập thông tin về một hệ thống, kiểu môi trường có thể thay đổi từ \_\_\_\_\_ sang \_\_\_\_\_.
- A. đóng, mở**
- B. chưa xác định, đã xác định**
- C. an toàn, dễ tổn thương**
- D. chưa xác định, đã xác định một phần.**
- 7.** Nhóm nào bao gồm các thành viên cạnh tranh cho cả người tấn công và người phòng thủ?
- A. Nhóm tím**
- B. Nhóm vàng**
- C. Nhóm xanh dương**
- D. Nhóm trắng.**
- 8.** OSINT liên quan đến điều gì dưới đây?
- A. Do thám thụ động**
- B. Do thám chủ động**
- C. Quét cổng**
- D. Tính bền bỉ.**
- 9.** Điều gì dưới đây là một phương pháp tiếp cận chính thức để xác định những điểm yếu của hệ thống hoặc của mạng và đang mở công khai?

- A.** Do thám chủ động
  - B.** Do thám thụ động
  - C.** OSINT
  - D.** Săn lõi kiếm tiền thưởng.
- 10.** Mục đích của nhóm trắng là gì?
- A.** Đại diện cho quản lý cấp cao
  - B.** Đưa ra những nhận xét để chấm điểm hoặc lập quy tắc trong một bài kiểm nghiệm
  - C.** Đại diện cho các bên là mục tiêu của một kiểm nghiệm xâm nhập
  - D.** Cung cấp một tập hợp các thành viên với các kỹ năng tấn công và phòng thủ (mọi ngôi sao).

## Đáp án

1. **A.** Nhóm đó là một nhóm bao gồm các tác nhân tấn công được sử dụng trong một kiểm nghiệm xâm nhập.
2. **B.** Chiến tranh bay là việc sử dụng thiết bị bay không người lái, máy bay, và các phương tiện bay khác để có được quyền truy cập vào các mạng không dây mà nếu không là không thể tiếp cận được.
3. **D.** Phần then chốt của câu hỏi là việc quét lại. Pivoting liên quan đến việc quét lại các kết nối mạng để tìm kiếm những kết nối chưa được xác định hoặc chưa từng thấy trước đó.
4. **B.** Các quy tắc tham gia mô tả phạm vi của sự tham gia [vào kiểm nghiệm xâm nhập] và cung cấp những thông tin quan trọng liên quan đến các liên hệ và quyền hạn. Việc có được những quy tắc này là điều thiết yếu trước khi bắt kỳ công việc kiểm nghiệm xâm nhập nào được bắt đầu.
5. **C.** Dọn dẹp liên quan đến các bước làm sạch các nhật ký và các bằng chứng khác để ngăn một ai đó khỏi việc bị phát hiện một cách dễ dàng.
6. **D.** OSINT cung cấp những thông tin về các hệ thống và các địa chỉ và các kết nối của chúng, bao gồm các ứng dụng. Việc này chuyển trạng thái của một hệ thống từ một môi trường hoàn toàn chưa xác định thành môi trường đã được xác định một phần.
7. **A.** Các nhóm tím có cả các nhân viên tấn công (đỏ) và phòng thủ (xanh dương) để mang lại một biện pháp ứng phó được cân bằng.
8. **A.** OSINT là một hoạt động thu động, do đó, do thám thu động là đáp án chính xác. Tất cả mọi câu trả lời khác đều liên quan đến các biện pháp chủ động.
9. **D.** Các chương trình săn lỗi kiểm tiền thường có thể mở ra lỗ hổng khai phá được cho công chúng cùng với một bộ các quy tắc quản lý quá trình tiết lộ và sự tham gia của các hệ thống.

**10. B.** Khi một bài tập liên quan đến tính điểm và/hoặc quan điểm cạnh tranh, đội đánh giá được gọi là đội trắng. Nếu bài tập đòi hỏi phải có một nhóm điều phối viên bên ngoài để quản lý nó, độc lập với đội phòng thủ, họ cũng được gọi là đội trắng. Các thành viên trong nhóm trắng ở đó để đảm bảo rằng bài tập thực sự đi đúng hướng và liên quan đến các thành phần mong muốn của một hệ thống.

## Phần II

### Kiến trúc và Thiết kế

- Chương 9 Kiến trúc Bảo mật Doanh nghiệp
- Chương 10 Bảo mật Ảo hóa và Bảo mật Đám mây
- Chương 11 Các Khái niệm về Bảo mật Phát triển, Triển khai và Tự động hóa Ứng dụng
- Chương 12 Xác thực và Cấp phép
- Chương 13 Khả năng phục hồi An ninh mạng
- Chương 14 Các Hệ thống Nhúng và Hệ thống Chuyên biệt
- Chương 15 Các Biện pháp kiểm soát Bảo mật Vật lý
- Chương 16 Các Khái niệm về Mật mã

## Chương 9     Kiến trúc Bảo mật Doanh nghiệp

---

### Kiến trúc Bảo mật Doanh nghiệp

Trong chương này bạn sẽ

- Xem xét các khái niệm về quản lý cấu hình,
  - Nghiên cứu về chủ quyền và các phương pháp bảo vệ dữ liệu,
  - Xem xét một loạt các công nghệ được sử dụng trong các kiến trúc để bảo vệ dữ liệu,
  - Xem xét các phương pháp được sử dụng để bảo vệ dữ liệu, bao gồm khả năng phục hồi địa điểm và các kỹ thuật đánh lừa dữ liệu.
- 

Các doanh nghiệp khác với các máy tính đơn lẻ đơn giản. Khi bạn có nhiều hệ thống hoạt động cùng với nhau, sẽ có những mối quan tâm về kiến trúc để đảm bảo rằng các phần tử có thể hoạt động cùng nhau một cách đáng tin cậy và an toàn. Kiến trúc sư doanh nghiệp là tất cả về việc thiết lập và tuân theo một biểu mẫu được tiêu chuẩn hóa cho các hệ thống của họ, xác định cấu hình và các giao diện để các hệ thống có thể hoạt động cùng nhau. Rất nhiều tùy chọn có sẵn cho rất nhiều thứ khi thiết lập cấu hình hệ thống và kiến trúc doanh nghiệp ở đó để hướng dẫn mọi người trong việc đưa ra các lựa chọn cấu hình hỗ trợ cho khả năng tương tác cũng như bảo mật.

#### Mục tiêu chứng nhận

Chương này đề cập đến mục tiêu 2.1 của kỳ thi CompTIA Security+: Diễn giải tầm quan trọng của các khái niệm bảo mật trong môi trường doanh nghiệp.

## Quản lý Cấu hình

Các cấu hình thích hợp là điều thiết yếu trong doanh nghiệp. *Quản lý cấu hình* là điều thiết yếu để bảo mật hệ thống bằng cách sử dụng cấu hình cụ thể mà việc triển khai đã dự định. Việc thay đổi cấu hình có thể bổ sung thêm chức năng, loại bỏ chức năng và thậm chí thay đổi hoàn toàn chức năng hệ thống bằng cách thay đổi các phần tử của chương trình để bao gồm mã phần mềm bên ngoài. Việc giám sát và bảo vệ hệ thống khỏi những thay đổi cấu hình trái phép là điều rất quan trọng đối với bảo mật.

Có một loạt các tài nguyên tồn tại để cung cấp hướng dẫn cho việc thiết lập và vận hành các hệ thống máy tính ở một mức độ an toàn được hiểu rõ và được lập thành văn bản. Bởi vì mọi doanh nghiệp đều khác nhau nên điều thiết yếu là mỗi doanh nghiệp phải xác định các tiêu chuẩn và khuôn khổ mà họ sử dụng để hướng dẫn cho việc quản lý cấu hình. Có rất nhiều nguồn cho các hướng dẫn này, nhưng có ba nguồn chính tồn tại cho một lượng lớn các hệ thống này. Bạn có thể nhận được hướng dẫn so sánh điểm chuẩn từ các nhà sản xuất phần mềm, từ chính phủ và từ một tổ chức độc lập được gọi là Trung tâm An ninh Internet (Center for Internet Security - CIS). Không phải tất cả các hệ thống đều có điểm chuẩn, cũng như không phải tất cả các nguồn đều đề cập đến tất cả các hệ thống, nhưng việc xác định chúng cho doanh nghiệp và tuân theo các hướng dẫn cấu hình và thiết lập chính xác có thể giúp ích rất nhiều trong việc thiết lập bảo mật.

## Sơ đồ

Các *sơ đồ* thường được sử dụng trong những đặc tả kỹ thuật kiến trúc để truyền đạt về cách thức doanh nghiệp được thiết lập cấu hình như thế nào – từ các sơ đồ mạng để mô tả các kết nối vật lý và luận lý, đến các sơ đồ được chú giải để cung cấp các thiết lập thiết yếu. Những sơ đồ dạng đồ họa được sử dụng bởi vì đôi khi chúng có thể dễ theo dõi hơn và

những hình ảnh có thể cung cấp khả năng truy cập sẵn sàng tới thông tin trong hầu hết các tình huống. Ngoài ra, trong môi trường có nội-dung-phong-phú về các danh sách đặc tả kỹ thuật, sẽ dễ dàng sắp đặt và hiểu được các mối quan hệ khi được trình bày thông qua sơ đồ.

## Cấu hình Đường cơ sở

*Cấu hình đường cơ sở* là điểm khởi đầu cho mọi đánh giá đường cơ sở trong tương lai. Đường cơ sở này nguyên thủy được tạo ra khi tạo ra hệ thống và là một bài thuyết trình về cách mà hệ thống được thiết lập cấu hình. Theo thời gian và các bản cập nhật đã được áp dụng, cấu hình này sẽ đòi hỏi sự cập nhật, khiến cho nó hiện hành cùng với cấu hình hệ thống mong muốn. Việc lập đường cơ sở là việc đo lường trạng thái hiện tại của mức độ sẵn sàng bảo mật của hệ thống. Có nhiều công cụ khác nhau đang có sẵn mà bạn có thể sử dụng để kiểm tra hệ thống để xem liệu hệ thống có những điểm yếu cụ thể khiến nó dễ bị tấn công hay không - những điểm yếu như mật khẩu mặc định, các vấn đề với quyền, v.v... Cách thức mà việc lập đường cơ sở hoạt động rất đơn giản: bạn thiết lập một hệ thống, đo đường cơ sở, khắc phục sự cố và khai báo cấu hình hệ thống kết quả làm đường cơ sở của bạn. Sau đó, trong tương lai, sau khi thay đổi các ứng dụng và tương tự như thế, bạn có thể đo đường cơ sở một lần nữa và tìm kiếm bất kỳ sai lệch nào. Bất cứ khi nào bạn cập nhật, vá lỗi hoặc bổ sung thêm ứng dụng, bạn có thể đo lường khoảng cách rủi ro bảo mật dựa trên các phép đo đường cơ bản trước và sau.

Độ sai lệch đường cơ sở là sự thay đổi so với giá trị đường cơ sở ban đầu. Sự thay đổi này có thể là tích cực, giảm rủi ro hoặc tiêu cực và làm tăng rủi ro. Nếu sự thay đổi làm gia tăng rủi ro thì bạn cần phải đánh giá mức độ rủi ro mới này để có thể khắc phục. Thách thức lớn nhất là chạy các tiến trình quét đường cơ sở hoặc tự động hóa chúng để xác định thời điểm xảy ra sai lệch.

## Quy ước Đặt tên Tiêu chuẩn

*Quy ước đặt tên tiêu chuẩn* là điều quan trọng trong một doanh nghiệp để từ đó, thông tin giao tiếp có thể rõ ràng và dễ hiểu. Các doanh nghiệp áp dụng các quy ước đặt tên tiêu chuẩn để giảm các nguồn gây lỗi và gia tăng mức độ rõ ràng của thông tin giao tiếp. Việc có được một bộ các quy tắc dành cho những gì mà người ta đặt tên cho mọi thứ - từ các tập tin, các thiết bị, các đối tượng, bao gồm cả người dùng – trong Active Directory cải thiện khả năng giao tiếp và nhận diện các phần tử trong quá trình làm việc. Nếu mọi máy chủ được đặt tên một cách ngẫu nhiên bằng cách sử dụng chuỗi 20-ký-tự chữ và số thì việc nói về việc máy chủ nào cần được sửa chữa sẽ trở thành một công việc rất khó khăn. Việc đặt tên chúng theo cách thức tạo điều kiện giao tiếp rõ ràng giúp loại bỏ được những sai sót.

## Lược đồ Giao thức Internet (IP)

Các địa chỉ Giao thức Internet phiên bản 4 (IPv4) là một con số 32 bit – hầu như không hữu ích cho một ai đó để hiểu được. Do đó, một ký hiệu chia số thành bốn bộ 8 bit, được biểu thị là xxx.xxx.xxx.xxx, trong đó x nằm trong khoảng từ 0 đến 255, đã được tạo ra. Địa chỉ thực cấu thành từ hai phần: một phần mạng và một phần máy vật chủ. Việc xác định cách phân chia những phần này để tối đa hóa việc sử dụng không gian địa chỉ chính là quá trình phân chia mạng con. Có hai lược đồ đánh địa chỉ chính: lược đồ Lớp A/B/C và phương pháp ký hiệu CIDR. Lược đồ Lớp A/B/C chia mạng và máy vật chủ ở các điểm thập phân của ký hiệu được liệt kê trước đó. Lược đồ CIDR chi tiết hơn, với địa chỉ của phần mạng được liệt kê trong các bit trước ký hiệu “/”.

Đối với một địa chỉ IP được chia thành mạng Lớp A, bit đứng đầu theo định nghĩa là 0, tiếp theo là 7 bit dành cho không gian mạng và 24 bit dành cho máy vật chủ. Điều này cho phép 128 mạng gồm 16.777.216 máy

vật chủ và được ký hiệu là “/8” trong ký hiệu CIDR. Mạng lớp B bắt đầu với 10 cho hai bit đầu tiên [*nghĩa là bit đầu tiên có giá trị là 1, bit thứ hai là 0*], sau đó là 14 bit cho mạng (tổng cộng 16,384) và 16 bit cho máy vật chủ (tổng cộng 65,536), hoặc “/16” trong ký hiệu CIDR. Ký hiệu CIDR làm cho việc chú thích sơ đồ mạng trở nên dễ hiểu và dễ nhận thức về cách thức mà mạng được bố trí. Chìa khóa để làm việc này là lập kế hoạch nâng cao và định nghĩa lược đồ đánh địa chỉ, do đó ngăn chặn các lược đồ phân đoạn mạng phi logic gây ra lãng phí không gian.



**MÁCH NƯỚC CHO KỲ THI** Quản lý cấu hình bao gồm việc phát triển các sơ đồ vật lý và luận lý, thiết lập đường cơ sở bảo mật, tạo ra các quy ước đặt tên tiêu chuẩn dễ hiểu, và triển khai các lược đồ IP an toàn.

### **Chủ quyền dữ liệu**

*Chủ quyền dữ liệu* là một loại luật tương đối mới mà một số quốc gia đã ban hành gần đây để quy định rằng dữ liệu được lưu trữ trong phạm vi biên giới của họ phải tuân theo luật của họ và trong một số trường hợp, dữ liệu có nguồn gốc trong biên giới của họ phải được lưu trữ ở đó. Trong nền kinh tế đa quốc gia ngày nay, với sự thiếu vắng biên giới của Internet, điều này đã thực sự trở thành một vấn đề. Một số công ty công nghệ cao đã thay đổi chiến lược kinh doanh và dịch vụ của họ để tuân thủ các quy tắc và quy định về chủ quyền dữ liệu. Ví dụ, LinkedIn, một trang mạng xã hội kinh doanh gần đây đã được chính quyền Nga thông báo rằng họ cần phải lưu trữ tất cả dữ liệu của mình về công dân Nga trên các máy chủ đặt tại Nga. LinkedIn đã đưa ra quyết định kinh doanh rằng chi phí bỏ ra không xứng đáng với lợi ích và từ bỏ thị trường Nga. Chủ quyền dữ liệu có thể định hướng cho các quyết định về kiến trúc trong các doanh nghiệp có nguồn gốc đa quốc gia. Một số quốc gia có những quy định

mạnh mẽ về mà nơi dữ liệu về công dân của họ có thể được lưu trữ và xử lý. Việc này sẽ định hướng cho các kiến trúc và thiết kế của cơ sở dữ liệu và ứng dụng dữ liệu.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng các đạo luật chủ quyền dữ liệu áp dụng cho dữ liệu được lưu trữ trong một quốc gia cụ thể. Ví dụ, nếu dữ liệu được lưu trữ ở Châu Âu thì các đạo luật và quy định về quyền riêng tư của EU áp dụng cho cách mà dữ liệu được lưu trữ và xử lý.

### Bảo vệ Dữ liệu

*Bảo vệ dữ liệu* là một bộ các chính sách, thủ tục, công cụ, và kiến trúc được sử dụng để đảm bảo sự kiểm soát thích hợp đối với dữ liệu trong doanh nghiệp. Các phần tử dữ liệu khác nhau đòi hỏi những mức bảo vệ khác nhau và vì những lý do khác nhau. Dữ liệu về khách hàng là đối tượng của một loạt các quy tắc pháp lý và quy định được thiết kế để bảo vệ dữ liệu của khách hàng. Những dữ liệu nhạy cảm khác cũng cần được bảo vệ, cũng như các hạng mục khác như tài sản trí tuệ có thể gây ra những thiệt hại đáng kể cho doanh nghiệp nếu như bị thất thoát. Một loạt các kỹ thuật được sử dụng như một phần của kế hoạch bảo vệ dữ liệu, và những kỹ thuật này được nêu bật trong những phần sau.

Dữ liệu là phần tử quan trọng nhất cần được bảo vệ trong doanh nghiệp. Các thiết bị có thể được mua sắm, thay thế, và chia sẻ mà không có hệ quả gì, chỉ có thông tin đang được xử lý [trong các thiết bị] mới có giá trị. *Bảo mật dữ liệu* đề cập đến những hành động được thực hiện trong doanh nghiệp để bảo vệ dữ liệu, bao gồm dữ liệu đang lưu trú ở đâu: đang truyền tải/di chuyển, còn lại, hoặc đang xử lý.

## Ngăn ngừa Thất thoát Dữ liệu

Các giải pháp *Ngăn ngừa thất thoát dữ liệu* (DLP) là để ngăn chặn những dữ liệu nhạy cảm rời khỏi mạng mà không có thông báo. Chương 18, "Bảo mật Máy chủ và Ứng dụng", bao gồm các vấn đề về kiểm tra mất mát dữ liệu ở các điểm đầu cuối, nhưng doanh nghiệp cũng cần có các biện pháp bảo vệ DLP. Vì dữ liệu được lưu trữ trong doanh nghiệp, thường là trong những cơ sở dữ liệu, do đó, nó có thể bị thất thoát trực tiếp từ những điểm này. Điều này đã dẫn đến việc giám sát DLP cấp-độ-doanh-nghiệp, nơi hoạt động trên tập tin được báo cáo tới các hệ thống tập trung và các dịch vụ DLP chuyên biệt như các thiết bị DLP nội dung được cung cấp bởi nhiều công ty bảo mật. Việc thiết kế các giải pháp bảo mật này thành kiến trúc doanh nghiệp là một phần của kiến trúc bảo mật của một doanh nghiệp hiện đại.



### MÁCH NƯỚC CHO KỲ THI

Các giải pháp DLP được thiết kế để bảo vệ dữ liệu đang truyền tải/di chuyển, tại chỗ, hoặc đang xử lý khỏi việc sử dụng hoặc lọc trái phép.

### Chắn mặt nạ (che giấu dữ liệu)

*Chắn mặt nạ dữ liệu* bao gồm việc ẩn dữ liệu bằng cách thay thế các giá trị đã được thay đổi. Một phiên bản phản chiếu của cơ sở dữ liệu được tạo và các kỹ thuật sửa đổi dữ liệu như xáo trộn ký tự, mã hóa và thay thế các từ hoặc ký tự được áp dụng để thay đổi dữ liệu. Một hình thức khác là chỉnh sửa vật lý các phần tử bằng cách thay thế bằng một ký hiệu như \* hoặc x. Điều này được nhìn thấy trên các biên lai thẻ tín dụng, nơi mà phần lớn các chữ số được xóa theo cách này. Việc che giấu dữ liệu khiến cho việc nhận diện hoặc kỹ thuật thiết kế ngược không thể thực hiện được. Việc sử dụng mặt nạ dữ liệu để tạo tập tin dữ liệu để kiểm tra

và tải lên honeypots với dữ-liệu-giả-mạo-có-thể-sử-dụng-được (usable-yet-fake data) là một thực tế phổ biến.

## Mã hóa

Mã hóa dữ liệu tiếp tục là giải pháp tốt nhất để bảo mật dữ liệu. Được mã hóa một cách đúng đắn, dữ liệu sẽ không thể đọc được bởi một bên không được phép. Có rất nhiều cách để ban hành mức độ bảo vệ này trong doanh nghiệp.

*Mã hóa* là việc sử dụng các kỹ thuật toán học tinh vi để ngăn ngừa những người truy cập trái phép vào dữ liệu khỏi việc thực sự đọc được dữ liệu. Tin tốt là điều này có thể được thực hiện với các phương pháp và ứng dụng đã được tiêu chuẩn hóa, bao gồm các chức năng tích hợp sẵn trong máy chủ cơ sở dữ liệu. Việc mã hóa các trường chính trong bộ nhớ ngăn chặn việc thất thoát chúng, vì mọi thông tin bị tiết lộ đều không thể đọc được. Việc phát triển các chính sách và thủ tục để đảm bảo rằng các trường dữ liệu chính xác được mã hóa một cách đúng đắn và các ứng dụng nghiệp vụ cần sử dụng dữ liệu được thiết lập cấu hình để đọc dữ liệu là một phần của sơ đồ kiến trúc doanh nghiệp tổng thể. Việc sử dụng mã hóa là một trong những yếu tố mà doanh nghiệp có thể thực hiện, khi được triển khai đúng cách, việc mất dữ liệu không phải là một sự kiện. Tuy nhiên, điều này đòi hỏi các sử dụng yếu tố kiến trúc cụ thể.

Mã hóa, bao gồm cả việc sử dụng và khoa học về nó, được đề cập chi tiết trong Chương 16, “Các khái niệm về Mật mã”.

## Dữ liệu còn lại

*Dữ liệu còn lại* đề cập đến dữ liệu đang được lưu trữ. Dữ liệu được lưu trữ theo một loạt định dạng: trong các tập tin, trong các cơ sở dữ liệu, và như các phần tử có cấu trúc. Bất kể dưới dạng ASCII, XML, JavaScript Object Notation (JSON), hay một cơ sở dữ liệu, và bất kể nó đang được lưu trữ trên phương tiện nào, dữ liệu còn lại vẫn đòi hỏi sự bảo vệ tương

xứng với giá trị của nó. Một lần nữa, như với dữ liệu đang truyền tải, mã hóa là phương tiện tốt nhất để bảo vệ [dữ liệu] chống lại việc truy cập hoặc thay thế trái phép.

### **Đang Truyền tải/Di chuyển**

Dữ liệu có những giá trị trong doanh nghiệp, nhưng để doanh nghiệp nhận thức rõ được giá trị, các phần tử dữ liệu cần phải được chia sẻ và di chuyển giữa các hệ thống. Bất kể dữ liệu *đang truyền tải/di chuyển*, được di chuyển từ một hệ thống sang hệ thống khác, nó cần phải được bảo vệ. Phương pháp phổ biến nhất là bảo vệ bằng mã hóa. Điều quan trọng là đảm bảo rằng dữ liệu luôn được bảo vệ một cách tương xứng với mức độ rủi ro liên quan đến lỗi bảo mật dữ liệu.

### **Đang Xử lý**

Dữ liệu được xử lý trong các ứng dụng, được sử dụng cho các chức năng khác nhau và có thể gặp rủi ro khi ở trong bộ nhớ hệ thống hoặc thậm chí trong quá trình xử lý. *Dữ liệu đang trong quá trình xử lý* là dữ liệu đang được sử dụng một cách chủ động, trong bộ xử lý hoặc phần tử tính toán khác. Bảo vệ dữ liệu khi đang sử dụng là một đề xuất phức tạp hơn nhiều so với việc bảo vệ dữ liệu đang trong quá trình vận chuyển hoặc đang được lưu trữ. Mặc dù mã hóa có thể được sử dụng trong những trường hợp khác nhau nhưng việc thực hiện các thao tác trên dữ liệu đã được mã hóa là không thực tế. Điều này có nghĩa là cần phải thực hiện các biện pháp khác để bảo vệ dữ liệu. Các lược đồ bộ nhớ được bảo vệ và ngẫu nhiên hóa bối cảnh không gian địa chỉ là hai công cụ có thể được sử dụng để ngăn chặn các lỗi bảo mật dữ liệu đang trong quá trình xử lý. Các nguyên tắc mã hóa an toàn, bao gồm xóa sạch dứt khoát các phần tử dữ liệu quan trọng khi chúng không còn cần thiết nữa, có thể hỗ trợ cho việc bảo vệ dữ liệu đang trong quá trình xử lý.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ về ba trạng thái quan trọng của dữ liệu và cách nó được bảo vệ khi đang được lưu trữ, truyền tải/di chuyển và đang trong quá trình xử lý.

### **Tokenization**

*Tokenization* là việc sử dụng một giá trị ngẫu nhiên để thay thế cho một phần tử dữ liệu có ý nghĩa có thể truy nguyên được. Một ví dụ điển hình về điều này là quy trình phê duyệt thẻ tín dụng, bạn không cần phải giữ một hồ sơ về số thẻ, tên chủ thẻ hoặc bất kỳ dữ liệu nhạy cảm nào liên quan đến mã xác minh thẻ (card verification code - CVC) vì nhân viên giao dịch trả lại mã phê duyệt, là mã thông báo duy nhất cho giao dịch đó. Bạn có thể lưu trữ mã phê duyệt này, mã thông báo, trong hệ thống của mình và nếu có lúc bạn cần tham chiếu giao dịch ban đầu, mã thông báo này cung cấp cho bạn khả năng truy nguyên đầy đủ đối với nó. Tuy nhiên, nếu nó được tiết lộ cho một bên ngoài, nó sẽ không hiển lộ điều gì.

Mã thông báo được sử dụng mọi lúc trong các hệ thống truyền dữ liệu liên quan đến thương mại vì chúng bảo vệ những thông tin nhạy cảm khỏi việc bị tái sử dụng hoặc chia sẻ, nhưng chúng vẫn duy trì các đặc điểm không khước từ mong muốn của sự kiện. Tokenization không phải là một bước mã hóa vì dữ liệu được mã hóa có thể được giải mã. Bằng cách thay thế một giá trị ngẫu nhiên không liên quan, tokenization sẽ bẻ gãy khả năng bất kỳ thực thể bên ngoài nào “đảo ngược” hành động vì không có kết nối.

Việc sử dụng tokenization để tạo ra và kiểm nghiệm các tập tin dữ liệu là một cách sử dụng phổ biến khác của công nghệ này. Quá trình mã hóa

bảo toàn tính toàn vẹn quan hệ, nhưng các mã thông báo không có ý nghĩa cho mục đích sử dụng khác.



**MÁCH NƯỚC CHO KỲ THI** Tokenization sử dụng một giá trị ngẫu nhiên để thay thế cho một phần tử dữ liệu có ý nghĩa có thể truy nguyên được.

### Quản lý Quyền

Việc bảo vệ dữ liệu có nhiều ý nghĩa khác nhau trong những bối cảnh khác nhau. *Quản lý quyền* là việc thiết lập một cách có hệ thống các quy tắc và trình tự đối với các quyền khác nhau mà người dùng có thể yêu cầu đổi với các đối tượng kỹ thuật số. Ví dụ, ở cấp độ tập tin, có đọc, ghi và các tùy chọn kiểm soát truy cập khác. Ở cấp độ ngữ cảnh, các tùy chọn đi xa hơn, bao gồm kiểm soát các khía cạnh chi tiết như chỉnh sửa, in, sao chép, phát lại, v.v... Quản lý quyền kỹ thuật số (DRM) là thuật ngữ được sử dụng để mô tả các trường hợp quyền điển hình liên quan đến các loại tập tin đa phương tiện khác nhau, bao gồm phát chung, sao chép, chỉnh sửa và lưu chúng vào thiết bị của riêng bạn. Các quyền này được thiết kế để ngăn chặn việc phân phối lại hoặc sử dụng trái phép nội dung kỹ thuật số. Quản lý quyền sẽ tiến xa hơn khi bạn bổ sung thêm các đề mục như tài liệu văn bản. Ai có thể chỉnh sửa, sao chép, xóa hoặc di chuyển tài liệu trong tài liệu hoặc cơ sở dữ liệu của công ty là mối quan tâm của doanh nghiệp. Việc phát triển một bộ chính sách và thủ tục cấp công ty để quản lý các quyền là điều cần thiết khi doanh nghiệp có nhu cầu đáng kể trong lĩnh vực này. Một phương pháp tiếp cận đột xuất sẽ dẫn đến những lỗ hổng và thất bại trong những gì mà một giải pháp cấp-degree-doanh-nghiệp có thể mang lại. Các nền tảng nội dung chính có khả

năng quản lý quyền ở quy mô cấp-độ-doanh-nghiệp, tuy nhiên, điều cần thiết là định nghĩa về lược đồ quyền được mong muốn.

### **Những cân nhắc về Vị trí địa lý**

Internet là một kết nối các hệ thống toàn cầu, và khi đã kết nối với Internet, theo đúng nghĩa đen, bạn được kết nối với thế giới. Điều này khiến cho *cân nhắc về vị trí địa lý* trở thành một chủ đề thực tế, vì có một loạt các đạo luật và quy định không dừng lại ở biên giới vật lý. Bạn muốn lưu trữ thông tin về các công dân của EU tại Hoa Kỳ? Các thành phần của GDPR vẫn có thể được áp dụng nếu bạn đang kinh doanh với họ. Bạn muốn lưu trữ dữ liệu về mọi người trong một quốc gia nước ngoài? Các đạo luật bảo vệ dữ liệu của họ có thể bắt buộc những phần tử dữ liệu nhất định phải được lưu trữ trên các máy chủ nằm trong phạm vi biên giới quốc gia của họ. Việc nghiên cứu và tìm hiểu về những tác động của vị trí địa lý và kiến tạo nên những cân nhắc về vị trí địa lý thích hợp để đảm bảo sự tuân thủ không chỉ dành cho các công ty đa quốc gia lớn.

Với hàng loạt sự chuyển đổi sang hội nghị từ xa do hậu quả của đại dịch vào năm 2020, đã có sự giám sát chặt chẽ hơn về nơi dữ liệu được lưu trữ và truyền đi. Zoom, một nhà cung cấp lớn trong thị trường hội nghị từ xa, đã phải đổi mới với phản ứng dữ dội đáng kể về việc dữ liệu được định tuyến qua các máy chủ ở Trung Quốc. Điều này bổ sung thêm khía cạnh của các lực lượng thị trường và ý kiến của công luận vào lĩnh vực xem xét khu vực địa lý, và là một khía cạnh cần được giải quyết trước khi nó trở thành một vấn đề ảnh-hưởng-đến-kinh-doanh.

### **Các biện pháp kiểm soát Ứng phó và Khôi phục**

Các doanh nghiệp được thiết kế với cơ sở hạ tầng hỗ trợ cho việc dữ liệu trở thành mạch máu của một tổ chức hiện đại. Nhưng với cơ sở hạ tầng này, cần có hướng dẫn vận hành để làm cho nó hoạt động. Hai trong số

các yếu tố phải được thiết kế vào doanh nghiệp là khả năng khôi phục sau thảm họa (disaster recovery - DR) và liên tục kinh doanh (business continuity - BC). Việc có các bản sao lưu là rất tốt, nhưng chúng sẽ không có ích gì nếu bạn không thể khôi phục và phục hồi chúng. Việc tạo ra các chương trình ứng phó sự cố, cùng với các nỗ lực của DR và BC, được tạo điều kiện thuận lợi rất nhiều bởi việc bao gồm các biện pháp kiểm soát ứng phó và khôi phục thích hợp vào trong doanh nghiệp. Như đã đề cập trước đó, việc sao lưu dữ liệu là một nửa của vấn đề. Có sẵn các cơ chế để khôi phục dữ liệu từ các bản sao lưu và tiếp tục hoạt động bình thường là những yếu tố cần được thiết kế cho doanh nghiệp. Những yếu tố này đòi hỏi việc lập trình tự đặc biệt, bạn cần có cấu trúc và quyền trước dữ liệu, cũng như băng thông để phục hồi dữ liệu lớn. Trong nhiều trường hợp, việc khôi phục dữ liệu hoàn chỉnh có thể là một nỗ lực kéo dài nhiều ngày và cần phải được thiết kế sẵn để bắt đầu trong khi vẫn hoạt động ở chế độ DR/BC và sau đó chuyển trở lại sau khi dữ liệu được đồng bộ hóa.

### **Secure Socket Layer (SSL)/Transport Layer Security (TLS)**

Sử dụng Transport Layer Security (TLS) trong một doanh nghiệp có thể mang lại sự bảo vệ rất lớn cho dữ liệu, nhưng nó cũng ngăn cản các công cụ bảo mật điều tra dữ liệu để phát hiện việc lọc [dữ liệu] và các mối quan tâm khác. Giao thức TLS được thiết kế để cho phép các ứng dụng giao tiếp trong một mạng để đảm bảo tính bảo mật và toàn vẹn của giao tiếp. Để kiểm tra dữ liệu đã được mã hóa đòi hỏi một điểm nơi mà dữ liệu có thể được giải mã và được kiểm tra trước khi tiếp tục hành trình của nó. Rất nhiều thiết bị bảo mật được thiết kế để bao gồm các dịch vụ kiểm tra TLS để từ đó việc sử dụng mã hóa SSL/TLS không khiến cho thiết bị phải dừng công việc của nó. Để hoàn thành nhiệm vụ *kiểm tra Secure Socket Layer (SSL)/Transport Layer Security (TLS)*, thiết bị phải nhận được một bộ các khóa mã hóa thích hợp. Sau đó thiết bị có thể nhận dữ

liệu, giải mã dữ liệu, thực hiện nhiệm vụ bảo mật của nó, mã hóa lại dữ liệu sử dụng dụng một khóa, và gửi dữ liệu đi đến đích của nó.

Các tường lửa thế hệ tiếp theo (next-generation firewall - NGFW) thường được tích hợp sẵn tính năng kiểm tra TLS, cung cấp mức độ bảo vệ này cho cả dữ liệu gửi đến và đi. Kiểm tra TLS bao gồm hai kết nối: bảo vệ máy chủ và bảo vệ máy khách. Tính năng bảo vệ máy chủ kiểm tra các kết nối đến máy chủ. Tính năng bảo vệ máy khách kiểm tra các kết nối TLS gửi đi được khởi tạo bởi các máy khách bên trong hệ thống mạng. Để thực hiện kiểm tra TLS, đòi hỏi phải có hai kết nối an toàn riêng biệt: một từ máy khách đến tường lửa và kết nối còn lại từ tường lửa đến máy chủ. Bạn có thể sử dụng một mình tính năng bảo vệ máy khách, một mình tính năng bảo vệ máy chủ hoặc bảo vệ máy khách và máy chủ cùng nhau. Bằng cách giải mã dữ liệu giao tiếp tại tường lửa, thiết bị có thể thực hiện kiểm tra sâu gói tin và các chức năng bảo mật khác trước khi mã hóa lại dữ liệu và gửi dữ liệu theo cách của nó nếu đó là cách truyền tải được cho phép. Tính năng này ngăn các kênh đã được mã hóa bỏ qua các yếu tố bảo mật trong mạng.

## Băm

*Băm* là một công nghệ mà theo đó, tính duy nhất của một phần tử dữ liệu có thể được đại diện bởi một chuỗi có độ-dài-cố-định. Băm có rất nhiều công dụng trong một doanh nghiệp, đại diện cho các phần tử dữ liệu, nhưng không phải nhường lại nội dung của phần tử [dữ liệu] cho người khác. Công nghệ mật mã đăng sau quá trình băm được đề cập trong Chương 16, “Các khái niệm về Mật mã”. Từ quan điểm kiến trúc doanh nghiệp, người ta nên xem băm là một phương tiện cho phép bảo vệ dữ liệu trong khi vẫn hỗ trợ sử dụng những dữ liệu cơ bản. Giá trị băm của phần tử dữ liệu có thể đóng vai trò như một sự thay thế cho dữ liệu và, nếu bị tiết lộ, giá trị băm không thể bị hoàn nguyên trở lại dữ liệu.



**MÁCH NƯỚC CHO KỲ THI** Một hàm băm là một hàm toán học đặc biệt thực hiện mã hóa một-chiều, có nghĩa rằng khi thuật toán được xử lý, không có cách nào khả thi để sử dụng mật mã để trích xuất văn bản thô đã được sử dụng để tạo ra nó.

### Những cân nhắc về API

Giao diện lập trình ứng dụng, hay API, là một thành phần quan trọng trong các doanh nghiệp kỹ thuật số, cho phép một phương pháp tích hợp các kết nối giữa các ứng dụng khác nhau. Tuy nhiên, với khả năng kết nối dễ dàng hơn này, nguy cơ cũng bị gia tăng, và bảo mật API thường bị bỏ qua, dẫn đến các vấn đề về bảo mật. API giống như các cửa ra vào và cửa sổ của những ứng dụng hiện đại. Chúng cung cấp quyền truy cập vào các ứng dụng và dữ liệu đăng sau chúng. Các API không được bảo mật hoặc được triển khai kém có thể tương đương với việc cửa ra vào và cửa sổ bị trực trặc, khiến cho việc bảo vệ các vật có giá trị trong nhà trở nên khó khăn hơn nhiều. Chúng ta không thể chỉ cấm các API vì chúng là một phương thức kết nối dữ liệu phổ biến trong hệ thống của chúng ta. Chúng ta cần xem xét các tác động về mặt bảo mật của chúng - đặc biệt là trong một doanh nghiệp nơi quyền truy cập có thể mở rộng một cách đáng kể cùng với kích thước và độ phức tạp của mạng - và sử dụng các biện pháp kiểm soát bảo mật để giảm thiểu rủi ro từ các API cho phép truy cập vào hệ thống của chúng ta. Việc thiết kế theo đúng bộ giao thức xác thực và cấp phép là điều cần thiết để hỗ trợ cho công nghệ cần thiết này với khả năng hoạt động một cách đáng tin cậy và an toàn trong doanh nghiệp.

### Khả năng Phục hồi của Địa điểm

Khả năng phục hồi của một địa điểm nên bao gồm sự cân nhắc về những địa điểm được sử dụng để tiếp tục hoạt động. *Khả năng phục hồi của địa*

điểm có thể được liên kết với ý tưởng về các địa điểm khôi phục và khả năng của chúng. Liên quan đến vị trí của nơi lưu trữ bản sao lưu là nơi mà các dịch vụ khôi phục sẽ được xác định. Nếu như tổ chức đã gánh chịu những thiệt hại về mặt vật chất đối với cơ sở vật chất của mình, việc có được nơi lưu trữ dữ liệu ngoại biên chỉ là một phần của giải pháp. Dữ liệu này sẽ cần phải được xử lý ở nơi nào đó, vốn có nghĩa là những phương tiện tính toán đó tương tự như những gì đã được sử dụng trong hoạt động bình thường là điều bắt buộc. Những địa điểm này còn được gọi là các địa điểm khôi phục. Vấn đề khôi phục có thể được tiếp cận theo một số cách, bao gồm những địa điểm nóng, địa điểm ấm, và địa điểm lạnh.

### **Địa điểm Nóng (Hot Sites)**

Một *địa điểm nóng* là một môi trường được thiết lập cấu hình đầy đủ, tương tự như mô hình hoạt động bình thường để có thể trở lại hoạt động ngay tức thì hoặc trong vài giờ, tùy thuộc vào thiết lập cấu hình của nó và nhu cầu của doanh nghiệp.

### **Địa điểm Ấm (Warm Sites)**

Một *địa điểm ấm* được thiết lập cấu hình một phần, thường có các thiết bị ngoại vi và phần mềm nhưng có thể không có các máy tính xử lý chính đắt tiền. Nó được thiết kế để được quay lại vận hành trong vài ngày.

### **Địa điểm Lạnh (Cold Sites)**

Một *địa điểm lạnh* sẽ chỉ có các biện pháp kiểm soát môi trường cơ bản cần thiết để vận hành với một ít các thành phần tính toán cần thiết để xử lý. Vận hành một địa điểm lạnh có thể mất vài tuần.



### **MÁCH NƯỚC CHO KỲ THI**

Các địa điểm thay thế được kiểm tra rất nhiều trong kỳ thi CompTIA Security+. Điều quan trọng là biết được liêu

dữ liệu có sẵn sàng hay không tại từng địa điểm. Ví dụ, một địa điểm nóng đã nhân bản dữ liệu hoặc sao lưu gần-như-sẵn-sàng từ địa điểm chính nguyên thủy. Một địa điểm lạnh không có các bản sao hoặc sao lưu hiện hành của dữ liệu từ địa điểm gốc. Một địa điểm ấm có các bản sao lưu, nhưng chúng thường là từ vài ngày hoặc vài tuần trước.

## Lừa dối và Phá hoại

*Lừa dối và phá hoại* đã trở thành những công cụ trong kho vũ khí của người bảo vệ để chống lại các mối đe dọa tiên tiến. Bởi vì tác nhân đe dọa chỉ có những thông tin hạn chế về cách hệ thống được cấu trúc nên việc bổ sung các yếu tố lừa đảo như honeypots/honeynets có thể dẫn đến các tình huống mà kẻ thù có thể được phát hiện. Sau khi phát hiện ra kẻ thù, một chiến dịch có thể được tiến hành để chống lại chúng, bao gồm cả việc sử dụng thêm các yếu tố đánh lừa để phá vỡ phương pháp tấn công của kẻ tấn công. Hành vi lừa dối tạo thêm một lớp giả mạo cho doanh nghiệp của bạn bằng cách đặt các tài sản giả mạo, dữ liệu giả mạo và các hiện vật khác trong doanh nghiệp của bạn. Công nghệ giả mạo này không phải là một phần của cấu hình doanh nghiệp của bạn, vì vậy không hệ thống hoặc cá nhân nào được phép chạm vào thứ gì đó giả mạo trừ khi họ đang chủ động tìm kiếm thứ gì đó hoặc có cấu hình sai.

## Honeypots

Một *honeypot* (*hũ mật ong*) là một máy chủ được thiết kế để hoạt động giống như một máy chủ thực trên hệ thống mạng của một công ty, nhưng thay vì có dữ liệu thực, honeypot chỉ xử lý những dữ liệu giả mạo. Các honeypot đóng vai trò như những mục tiêu hấp dẫn đối với những kẻ tấn công. Một honeypot đóng vai trò như là một cái bẫy những kẻ tấn công, vì lưu lượng trong honeypot có thể được giả định là độc hại. Nhiều honeypot có thể được kết nối thành một honeynet, trở thành một mục

tiêu hấp dẫn cho những tin tức khám phá trong giai đoạn do thám của chúng.

### **Honeyfiles**

Một *honeyfile* là một tập tin được thiết kế để trông giống như một tập tin thực tế trên một máy chủ, nhưng dữ liệu đang chứa trong nó là giả mạo. Các *honeyfile* đóng vai trò như một mục tiêu hấp dẫn đối với những kẻ tấn công. Một *honeyfile* giống như một cái bẫy những kẻ tấn công, và dữ liệu trong tập tin có thể chứa các yếu tố kích hoạt để cảnh báo cho các giải pháp DLP. Truy cập đến các tập tin cũng có thể được giám sát. Một biến thể của một *honeyfile* là một *honeyrecord* trong một cơ sở dữ liệu. Những bản ghi này phục vụ cho cùng một mục đích: chúng là giả mạo và không bao giờ được sử dụng, nhưng nếu chúng được sao chép, bạn sẽ biết ngay là có một hành động trái phép.

Các *honeyfile* và *honeyrecord* có thể đi kèm với các tập tin và bản ghi hợp lệ, khiến cho việc khám phá và khai thác chúng trở nên có nhiều khả năng hơn. Những phần tử này hoạt động như những bẫy dây (*tripwires*) và có thể được truy nguyên để cảnh báo về hoạt động trái phép.

### **Honeynets**

Một *honeynet* là một mạng được thiết kế để trông giống như một mạng công ty nhưng được tạo ra để thu hút những kẻ tấn công. Một *honeynet* là một tập hợp các *honeypots*. Nó trông giống như mạng công ty, nhưng bởi vì nó được biết là một bản sao giả mạo nên mọi lưu lượng truy cập được cho là không hợp pháp. Điều này giúp bạn dễ dàng mô tả lưu lượng truy cập của kẻ tấn công và cũng có thể hiểu được nguồn gốc của các cuộc tấn công đến từ đâu. Các *honeynet* sẽ không được truy cập hoặc sử dụng bởi các hệ thống hợp pháp vì các hệ thống hợp pháp có những kết nối với các máy chủ thực, vì vậy bất kỳ lưu lượng nào trên *honeynet* đều

được coi là cửa một kẻ tấn công hoặc một hệ thống được định cấu hình sai.

### **Phép đo từ xa Giả tạo**

Khi bạn đang ở trên một hệ thống và bạn nhận ra rằng không có lưu lượng truy cập nào khác, suy nghĩ đầu tiên là bạn không còn ở trong mạng doanh nghiệp nữa. Để tránh việc thiếu những lưu lượng truy cập “bình thường” trở thành một món quà chết chóc mà bạn đã đưa vào một phần giả của mạng, phép đo từ xa giả được sử dụng. *Phép đo từ xa giả tạo* là lưu lượng mạng tổng hợp tương tự như thông tin liên lạc chính thức, được phân phối ở một khối lượng thích hợp để làm cho honeynet và honeypots trông giống như thật.



**MÁCH NƯỚC CHO KỲ THI** Phép đo từ xa giả tạo là một công nghệ lừa dối được sử dụng để khiến cho các honeynet và honeypot trông giống như thật và hấp dẫn đối với những kẻ tấn công tiềm năng.

### **Hố sụt (Sinkhole) DNS**

Một *Hố sụt DNS* là một nhà cung cấp DNS trả về các yêu cầu DNS cụ thể với kết quả sai. Điều này dẫn đến việc người yêu cầu được gửi đến địa chỉ sai, thường là một địa chỉ không thể định tuyến được. Khi một máy tính ghé thăm một máy chủ DNS để phân giải tên miền, máy chủ sẽ đưa ra kết quả, nếu đang sẵn có, nếu không, nó sẽ gửi yêu cầu phân giải đến một máy chủ DNS cấp cao hơn để giải quyết. Điều này có nghĩa là hố sụt DNS nằm càng cao trong chuỗi này, thì càng có nhiều yêu cầu mà nó ảnh hưởng đến và nó có thể mang lại hiệu quả có lợi hơn. Hố sụt DNS điển hình là một máy chủ DNS tiêu chuẩn đã được thiết lập cấu hình để trả về các địa chỉ không thể truy xuất cho mọi tên miền nằm trong danh sách hố sụt để mọi yêu cầu sẽ không thể truy cập vào trang web thực. Một số

botnet lớn hơn đã bị các hổ sụt của miền cấp cao nhất (top-level domain - TLD) kết xuất là không thể sử dụng được, có thể trải dài trên toàn bộ Internet. Hổ sụt DNS là một công cụ hữu ích để chặn lưu lượng độc hại và chúng được sử dụng để chống lại bot và các phần mềm độc hại khác dựa vào phản hồi DNS để giao tiếp. Một ví dụ nổi tiếng về điều này là việc sử dụng hổ sụt DNS để ngăn chặn phần mềm độc hại WannaCry vào năm 2017.

---



### MÁCH NƯỚC CHO KỲ THI

Một hổ sụt DNS là một công nghệ lừa dối và phá hoại để trả về những kết quả sai cho những yêu cầu DNS nhất định. Các hổ sụt DNS có thể được sử dụng theo cách thức xây dựng và phá hoại Khi được sử dụng theo cách xây dựng, một hổ sụt DNS sẽ ngăn chặn người dùng truy cập vào những tên miền độc hại.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các yếu tố về khái niệm bảo mật trong môi trường doanh nghiệp. Chương mở đầu với chủ đề quản lý cấu hình. Trong quản lý cấu hình, các chủ đề phụ về các sơ đồ, cấu hình đường cơ sở, quy ước đặt tên tiêu chuẩn và lược đồ giao thức Internet (IP) đã được đề cập. Chủ đề tiếp theo là chủ quyền dữ liệu.

Quyền riêng tư dữ liệu là phần thứ ba, với các chủ đề phụ về ngăn ngừa thất thoát dữ liệu, tạo mặt nạ và mã hóa. Các chủ đề phụ tiếp tục với mô tả dữ liệu đang được lưu trữ, đang truyền tải/di chuyển và đang xử lý. Phần bảo vệ dữ liệu đã kết thúc với một cuộc thảo luận về mã hóa và quản lý quyền. Sau đó, chương tiếp tục với một loạt các chủ đề độc lập, bao gồm cân nhắc địa lý, các biện pháp kiểm soát phục hồi và khôi phục cũng như kiểm tra Secure Socket Layer (SSL)/Transport Layer Security (TLS).

Phần này của chương đã kết thúc với những xem xét về hàm băm và API. Hai phần cuối của chương là khả năng phục hồi của địa điểm, trong đó các địa điểm nóng, ấm và lạnh được đề cập, tiếp theo là các công nghệ phát hiện và gián đoạn. Trong phần nói về phát hiện và gián đoạn, các chủ đề về honeypots, honeyfiles và honeynet đã được trình bày. Hai mục cuối cùng trong phần này là phép đo từ xa giả tạo và hổ sụt DNS.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Điều nào dưới đây không phải là một trạng thái của dữ liệu trong doanh nghiệp?

  - A. Đang được lưu trữ
  - B. Trong bộ lưu trữ
  - C. Đang xử lý
  - D. Đang truyền tải/di chuyển.
2. Việc tạo ra một lưu lượng mạng giả tạo để đánh lừa những kẻ tấn công trong các phân đoạn của hệ thống mạng để đánh lừa chúng được gọi là gì?

  - A. Hỗn sụt DNS
  - B. Honeytraffic
  - C. Phép đo từ xa giả tạo
  - D. Chắn mặt nạ.
3. Nếu mã hóa từ-đầu-đến-cuối được sử dụng, công nghệ nào dưới đây tạo điều kiện cho việc giám sát bảo mật của các kênh giao tiếp đã được mã hóa?

  - A. Phép đo từ xa giả tạo
  - B. Tokenization
  - C. Băm
  - D. Kiểm tra TLS.
4. Các doanh nghiệp có thể sử dụng \_\_\_\_\_ để chặn lưu lượng điều-khiển-và-kiểm-soát độc hại từ phần mềm độc hại?

  - A. mã hóa
  - B. các honeyfile

- C.** các hổ sụt DNS
  - D.** các honeynet.
- 5.** Điều gì dưới đây có thể cung cấp khả năng truy nguyên hoàn chỉnh đến một giao dịch nguyên thủy mà không phát lộ bất kỳ thông tin cá nhân nào nếu như bị tiết lộ cho một bên bên ngoài?
- A.** Tokenization
  - B.** Chủ quyền dữ liệu
  - C.** Quản lý quyền
  - D.** Thiết lập đường cơ sở cấu hình.
- 6.** Một hệ thống sẵn sàng để sử dụng ngay tức khắc sau một sự kiện gián đoạn được gọi là gì?
- A.** Hệ thống chờ
  - B.** Địa điểm khôi phục sau thảm họa
  - C.** Địa điểm sao lưu
  - D.** Địa điểm nóng.
- 7.** Bảo vệ dữ liệu bao gồm tất cả những chủ đề nào dưới đây ngoại trừ? (Chọn tất cả đáp án khả dĩ)
- A.** Các honeypot
  - B.** Chắn mặt nạ
  - C.** Tokenization
  - D.** Các hổ sụt DNS.
- 8.** Điều nào dưới đây là điều quan trọng cần cân nhắc khi kiểm tra cụ thể việc quản lý cấu hình?
- A.** Ngăn ngừa thất thoát dữ liệu
  - B.** Quy ước đặt tên tiêu chuẩn
  - C.** Quản lý quyền
  - D.** Băm.
- 9.** Chắn mặt nạ là gì ?

- A.** Việc sử dụng dữ liệu dự-phòng để thay thế cho dữ liệu thời gian thực
  - B.** Đánh dấu các khu vực mà dữ liệu không được chấp thuận theo chính sách
  - C.** Việc sử dụng các bản sao lưu để bảo toàn dữ liệu trong các sự kiện gián đoạn
  - D.** Viết lại các phần dữ liệu bằng cách sử dụng ký hiệu bao trùm như \* hoặc x.
- 10.** Mục đích của lừa dối trong một doanh nghiệp là gì ? (Chọn mọi đáp án khả dĩ)
- A.** Lừa những kẻ tấn công đánh cắp dữ liệu giả mạo
  - B.** Xác định các hệ thống bị định cấu hình sai
  - C.** Cho phép dễ dàng xác định các tác nhân trái phép
  - D.** Cung cấp một khu vực để kiểm tra các hệ thống mới mà không gây ảnh hưởng đến hoạt động hợp thức.

## Đáp án

1. **B.** Trong bộ lưu trữ không phải là một thuật ngữ chính xác được sử dụng trong việc mô tả trạng thái của dữ liệu. Những trạng thái đúng bao gồm đang được lưu trữ, đang truyền tải/di chuyển, và đang xử lý.
2. **C.** Phép đo từ xa giả tạo là tên gọi của lưu lượng mạng giả tạo trong một môi trường dựa-trên-lừa-dối (deception-based).
3. **D.** Các hệ thống kiểm tra TLS cho phép các kênh TLS được phá vỡ và thiết lập lại, cho phép việc giám sát lưu lượng bảo mật.
4. **C.** Các hổ sụt DNS có thể ngăn chặn giao tiếp trên các hệ thống điều khiển và kiểm soát có liên quan đến phần mềm độc hại và các mạng botnet bằng cách chặn địa chỉ đích thông qua việc cố ý định tuyến sai lưu lượng đến một ngõ cụt.
5. **A.** Tokenization là việc sử dụng một giá trị ngẫu nhiên để thay thế cho một phần tử dữ liệu có ý nghĩa truy nguyên được. Điều này cung cấp khả năng truy xuất nguồn gốc hoàn chỉnh cho giao dịch ban đầu, nhưng nếu được tiết lộ cho bên ngoài, nó sẽ không tiết lộ gì thêm. Chủ quyền dữ liệu liên quan đến các đạo luật cụ thể của một quốc gia về việc lưu trữ và truyền tải dữ liệu cá nhân. Quản lý quyền là việc thiết lập có hệ thống các quy tắc và trật tự đối với các quyền khác nhau mà người dùng có thể sử dụng trên các đối tượng kỹ thuật số. Một cấu hình đường cơ sở ban đầu được tạo khi tạo ra hệ thống và là một bản thuyết trình về cách hệ thống được định cấu hình.
6. **D.** Một địa điểm nóng là một địa điểm sẵn sàng để sử dụng ngay lập tức trong trường hợp bị lỗi. Tất cả các tùy chọn khác là tên gọi được tạo ra bằng cách sử dụng các từ ngữ đánh lạc hướng.
7. **A và D.** Các honeypot và hổ sụt DNS là thành phần của các hoạt động lừa dối và phá hoại, không phải là bảo vệ dữ liệu.

8. **B.** Các quy ước đặt tên tiêu chuẩn cải thiện giao tiếp của các phần tử quan trọng, từ đó hỗ trợ tốt hơn cho các hoạt động quản lý cấu hình.
9. **D.** Chắn mặt nạ là việc đánh dấu các phần thông tin để ngăn chặn việc tiết lộ (ví dụ: sử dụng các x cho tất cả trừ bốn số cuối của một thẻ tín dụng).
10. **A, B và C.** Các kỹ thuật lừa đảo như honeynet và honeypots có thể lừa những kẻ tấn công lấy cắp dữ liệu giả và giúp chúng dễ dàng bị phát hiện hơn trong mạng. Các kỹ thuật này cũng có thể giúp xác định các hệ thống bị thiết lập cấu hình sai.

## Chương 10    Bảo mật Ảo hóa và Bảo mật Đám mây

---

### Bảo mật Ảo hóa và Bảo mật Đám mây

Trong chương này bạn sẽ

- Làm quen với điện toán đám mây,
  - Tìm hiểu các khái niệm về ảo hóa.
- 

Ảo hóa và các dịch vụ đám mây đang trở thành các công cụ doanh nghiệp phổ biến để quản lý chi phí, công suất, độ phức tạp và rủi ro. Bạn cần phải tìm hiểu về cách thức những dịch vụ này đóng góp như thế nào cho một giải pháp bảo mật trong doanh nghiệp ngày nay, như đã được mô tả trong chương trước đó.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 2.2 của kỳ thi CompTIA Security+: Tóm tắt các khái niệm ảo hóa và điện toán đám mây.

## Các Mô hình Đám mây

Có rất nhiều *mô hình triển khai đám mây* khác nhau. Các đám mây có thể được tạo ra bởi rất nhiều thực thể, cả trong nội bộ lẫn bên ngoài đối với tổ chức. Rất nhiều dịch vụ đám mây thương mại đang sẵn có từ một loạt các công ty khác nhau, từ Google đến Amazon đến những nhà cung cấp địa phương nhỏ hơn. Về nội bộ, một dịch vụ riêng của tổ chức có thể sao chép những lợi thế của điện toán đám mây trong khi cải thiện được tính tiện dụng của các nguồn lực bị hạn chế. Cam kết của điện toán đám mây là tính tiện dụng được cải thiện và được tiếp thị theo các khái niệm Nền tảng như một Dịch vụ (PaaS), Phần mềm như một Dịch vụ (SaaS) và Cơ sở hạ tầng như một Dịch vụ (IaaS).

Có những ưu và nhược điểm đối với điện toán dựa-trên-đám-mây. Và đối với từng mục đích sử dụng, các yếu tố kinh tế cũng có thể khác nhau (các vấn đề về chi phí, hợp đồng, v.v...). Tuy nhiên, đối với một người nào đó đang xây dựng một dự án thử nghiệm mà họ có thể không muốn gánh chịu chi phí phần cứng liên quan đến việc mua các máy chủ có thể tồn tại ngoài dự án thử nghiệm, thì việc "thuê" không gian trên đám mây sẽ có ý nghĩa. Khi nhiều địa điểm có liên quan và vẫn dễ phân phối dữ liệu và các giải pháp sao lưu là một mối quan tâm thì các dịch vụ đám mây sẽ mang lại lợi thế. Tuy nhiên, với việc kiểm soát ít hơn sẽ dẫn đến các chi phí khác, chẳng hạn như điều tra pháp y, ứng phó sự cố, lưu trữ dữ liệu, hợp đồng dài hạn và kết nối mạng. Đối với mỗi trường hợp, việc phân tích nghiệp vụ đều phải được thực hiện để xác định lựa chọn chính xác giữa các tùy chọn điện toán đám mây và điện toán tại-chỗ.

## Cơ sở hạ tầng như một Dịch vụ (IaaS)

*Cơ sở hạ tầng như một Dịch vụ (IaaS)* là một thuật ngữ tiếp thị được sử dụng để mô tả các hệ thống dựa-trên-đám-mây được cung cấp như một giải pháp ảo để tính toán. Thay vì công ty cần phải xây dựng các trung

tâm dữ liệu, IaaS cho phép họ ký hợp đồng cho tiện ích tính toán khi cần thiết. IaaS đặc biệt được tiêu thụ trên cơ sở thanh-toán-khi-sử-dụng, có thể mở rộng một cách trực tiếp theo nhu cầu.

### **Nền tảng như một Dịch vụ (PaaS)**

*Nền tảng như một Dịch vụ (PaaS)* là một thuật ngữ tiếp thị được sử dụng để mô tả việc cung cấp một nền tảng điện toán trên đám mây. Rất nhiều bộ phần mềm hoạt động cùng nhau để cung cấp các dịch vụ, chẳng hạn như các dịch vụ cơ sở dữ liệu, có thể được cung cấp thông qua đám mây như một nền tảng. Các đề xuất của PaaS thường tập trung vào bảo mật và khả năng mở rộng, cả hai đều là những đặc trưng phù hợp với nhu cầu về đám mây và nền tảng.

### **Phần mềm như một Dịch vụ (SaaS)**

*Phần mềm như một Dịch vụ (SaaS)* là việc cung cấp phần mềm cho người dùng đầu cuối từ trong phạm vi đám mây. Thay vì cài đặt phần mềm trên các máy khách, SaaS hoạt động như phần mềm theo nhu cầu, khi phần mềm hoạt động từ đám mây. Việc này có một số ưu điểm: các bản cập nhật có thể liên mạch đối với người dùng đầu cuối, và sự tích hợp giữa các thành phần có thể được tăng cường. Các ví dụ phổ biến về SaaS là các sản phẩm được cung cấp thông qua Web như các dịch vụ thuê bao, chẳng hạn như Microsoft Office 365 và Adobe Creative Suite.

### **Bất kỳ điều gì như một Dịch vụ (XaaS)**

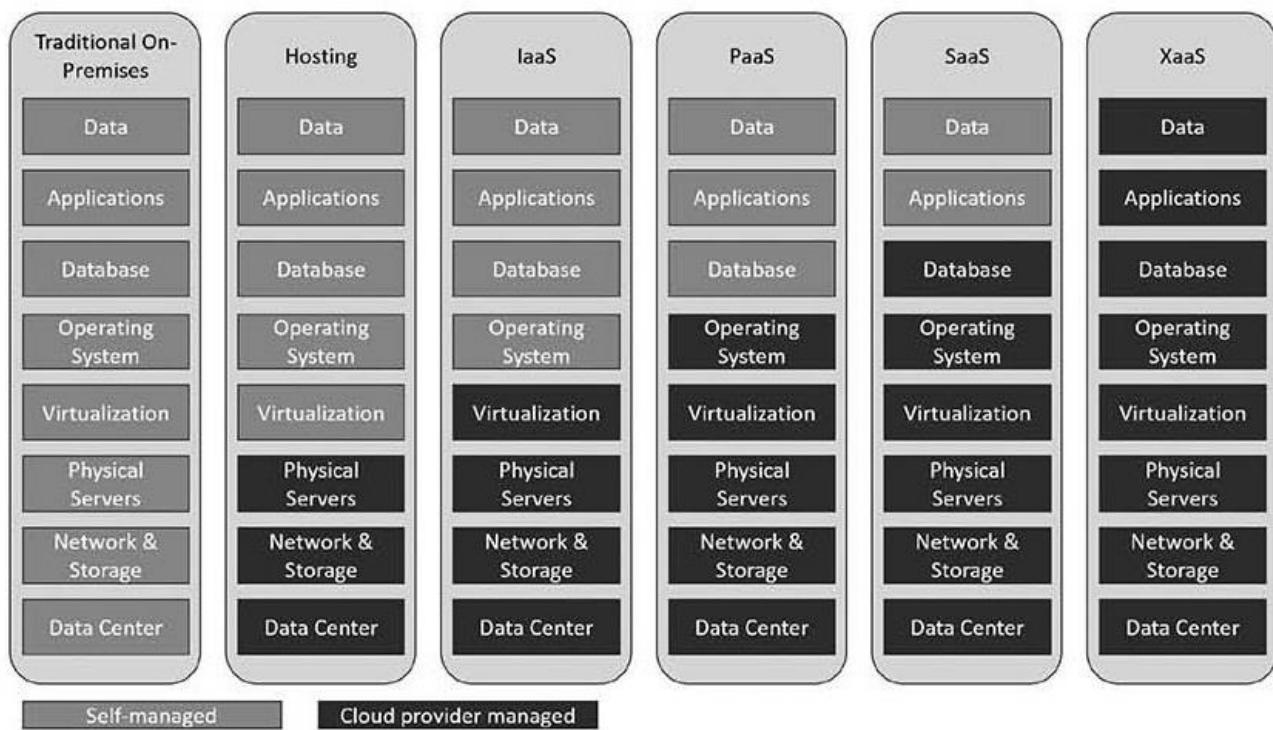
Cùng với sự phát triển của các dịch vụ đám mây, các ứng dụng, lưu trữ, và xử lý, quy mô được cung cấp bởi các nhà cung cấp đám mây đã mở ra các dịch vụ mới được gọi chung là *Bất kỳ điều gì như một Dịch vụ (XaaS)*. Việc đóng gói những thành phần SaaS và IaaS đã được đề cập trước đây thành một dịch vụ cụ thể (ví dụ, Khôi phục sau Thảm họa như một Dịch vụ) tạo ra một mặt hàng mới có thể được bày bán trên thị trường.



**MÁCH NƯỚC CHO KỲ THI** Hãy chắc chắn bạn hiểu được sự khác biệt giữa các mô hình dịch vụ điện toán đám mây Nền tảng như một Dịch vụ, Phần mềm như một Dịch vụ, Cơ sở hạ tầng như một Dịch vụ, và Bất kỳ điều gì như một Dịch vụ.

### **Mức độ Kiểm soát trong các Mô hình Lưu trữ'**

Một cách để kiểm tra sự khác biệt giữa các mô hình điện toán đám mây và điện toán tại-chỗ là xem xét việc ai đang kiểm soát những khía cạnh nào của mô hình. Trong Hình 10-1, bạn có thể thấy rằng mức kiểm soát các hệ thống đi từ tự-kiểm-soát hoàn toàn trong điện toán tại-chỗ đến nhà cung cấp kiểm soát hoàn toàn trong XaaS.



**Hình 10-1** So sánh mức độ kiểm soát trong các mô hình lưu trữ khác nhau

## Công cộng

Thuật ngữ *đám mây công cộng* đề cập đến một dịch vụ đám mây được kết xuất trên một hệ thống mở để sử dụng công cộng. Trong hầu hết các trường hợp, có rất ít sự khác biệt về mặt vận hành giữa các kiến trúc đám mây công cộng và riêng tư, nhưng các phân nhánh bảo mật có thể sẽ rất đáng kể. Mặc dù các dịch vụ đám mây công cộng sẽ phân tách người dùng bằng các hạn chế bảo mật, nhưng theo định nghĩa, mức độ và độ sâu của những hạn chế này sẽ ít hơn đáng kể trong một đám mây công cộng.

## Công đồng

Một hệ thống *đám mây công đồng* là một hệ thống nơi một số tổ chức với những mối quan tâm chung cùng chia sẻ một môi trường đám mây cho những mục đích cụ thể của những nỗ lực chung. Ví dụ, những thực thể công tại địa phương và những công ty then chốt tại địa phương có thể chia sẻ một đám mây cộng đồng chuyên biệt để phụng sự cho những lợi ích của các sáng kiến cộng đồng. Đây có thể là một cơ chế chia-sẻ-chi-phí hấp dẫn cho các sáng kiến chia-sẻ-dữ-liệu cụ thể.

## Riêng tư

Nếu như tổ chức của bạn đặc biệt nhạy cảm với việc chia sẻ tài nguyên, bạn sẽ có thể mong muốn sử dụng một *đám mây riêng tư*. Các đám mây riêng tư về cơ bản là những nguồn tài nguyên chỉ được sử dụng bởi tổ chức của bạn – đám mây nhỏ của riêng bạn trong một đám mây. Thiết lập này sẽ tốn kém hơn một cách đáng kể, nhưng nó cũng sẽ ít tiếp xúc với rủi ro hơn và sẽ cho phép tổ chức của bạn xác định tốt hơn các yếu tố bảo mật, xử lý và quản lý dữ liệu, v.v... xảy ra trong phạm vi đám mây của bạn.

## Lai

Một cấu trúc *đám mây lai* là một cấu trúc nơi các thành phần từ những cấu trúc đám mây riêng tư, công cộng và cộng đồng được kết hợp lại với nhau. Khi xem xét một cấu trúc lai, bạn cần nhận thức được rằng, về mặt vận hành, các môi trường khác nhau này không thực sự được *kết hợp* với nhau mà là *được sử dụng* cùng nhau. Ví dụ, những thông tin nhạy cảm có thể được lưu trữ trong đám mây riêng tư và thông tin liên-quan-đến-vấn-đề có thể được lưu trữ trong đám mây cộng đồng, tuy nhiên, tất cả thông tin này đều được truy cập bởi cùng một ứng dụng. Điều này khiến cho hệ thống tổng thể trở thành một hệ thống đám mây lai.



**MÁCH NƯỚC CHO KỲ THI** Hãy chắc chắn bạn đã hiểu và nhận biết được sự khác biệt giữa các hệ thống đám mây – riêng tư, công cộng, lai, và cộng đồng – bởi vì bạn sẽ nhìn thấy tất cả chúng trong những lựa chọn đáp án cho một câu hỏi về đám mây. Đáp án tốt nhất thường sẽ thuộc vào một yếu tố hoặc chi tiết duy nhất trong câu hỏi.

## Các nhà cung cấp Dịch vụ Đám mây

Các *nha cung cap dich vu dam may (CSPs)* có nhiều quy mô và hình thức, với vô số các dịch vụ, mức giá và mức dịch vụ khác nhau. Có những nhà cung cấp đám mây siêu-lớn, như Amazon, Google, Microsoft và Oracle, hầu như không có giới hạn về quy mô mà họ có thể mở rộng khi cần thiết. Có những công ty nhỏ hơn, với một số dịch vụ được bán lại từ các đám mây lớn hơn và những công ty khác lưu trữ trung tâm dữ liệu của riêng họ. Mỗi một trong số này đều có những ưu đãi dành cho doanh nghiệp và điều thách thức là xác định xem ưu đãi nào phù hợp nhất với nhu cầu của dự án hoặc công ty của bạn. Rất nhiều vấn đề phải được giải quyết xoay quanh việc dịch vụ nào đang được cung cấp và dịch vụ nào không, cũng như các mức giá và điều khoản hợp đồng. Một điều quan trọng cần nhớ

rằng: nếu điều gì đó không có trong hợp đồng, nó sẽ không được thực hiện. Lấy các mục bảo mật, ví dụ, nếu bạn muốn nhà cung cấp đám mây cung cấp chức năng bảo mật cụ thể thì nó phải nằm trong gói mà bạn đăng ký sử dụng, nếu không, bạn sẽ không nhận được chức năng này.

### **Nhà cung cấp Dịch vụ Được quản lý (MSP)/Nhà cung cấp Dịch vụ Bảo mật Được quản lý (MSSP)**

*Nhà cung cấp dịch vụ được quản lý (MSP)* là một công ty quản lý cơ sở hạ tầng CNTT của khách hàng từ xa. Một *nhà cung cấp dịch vụ bảo mật được quản lý (MSSP)* thực hiện điều tương tự như một bên-thứ-ba quản lý các dịch vụ bảo mật. Đối với mỗi dịch vụ này, điều quan trọng nằm trong các chi tiết. Phạm vi của cam kết, những gì có trong chi tiết của hợp đồng, chính là những gì đang được cung cấp bởi bên-thứ-ba, và không gì khác. Ví dụ, nếu bạn không quản lý các bản sao lưu như một phần của hợp đồng, hoặc là bạn có thể tự mình thực hiện hoặc bạn phải sửa đổi lại hợp đồng. Các dịch vụ được quản lý cung cấp sức mạnh của một công ty lớn nhưng với một phần nhỏ chi phí mà một công ty nhỏ sẽ phải trả để đạt được lợi thế về quy mô của một công ty lớn. Vì vậy, rõ ràng là sẽ có những lợi thế. Tuy nhiên, nhược điểm nằm ở tính linh hoạt, vì sẽ không có chỗ cho sự thay đổi nếu không thương lượng lại hợp đồng dịch vụ.

### **On-Premises so với Off-Premises**

Các hệ thống có thể tồn tại ở rất nhiều nơi - từ *tại-chỗ* (on-premises), đến *đến* được lưu trữ, đến trên đám mây. *Tại-chỗ* có nghĩa là hệ thống nằm cục bộ trong tòa nhà của tổ chức. Cho dù đó là một máy ảo (VM), thiết bị lưu trữ hay thậm chí là một dịch vụ, nếu giải pháp được thiết lập và duy trì cục bộ, nó được gọi là "*tại-chỗ*". Ưu điểm là tổ chức có toàn quyền kiểm soát hệ thống và nhìn chung có khả năng kết nối cao tới hệ thống. Điểm bất lợi là nó đòi hỏi nguồn lực cục bộ và không nhất thiết sẽ dễ dàng mở rộng quy mô. Dịch vụ *ngoại-biên (off-premises)* hoặc dịch vụ

được lưu trữ đề cập đến việc các dịch vụ được lưu trữ ở một nơi khác, thường là trong một môi trường được chia sẻ. Việc sử dụng một bên-thứ-ba cho các dịch vụ được lưu trữ sẽ cung cấp cho bạn một mức chi phí định sẵn dựa trên tổng số lượng dịch vụ mà bạn sử dụng. Điều này có lợi thế về chi phí, đặc biệt là khi bao gồm cả quy mô - liệu có hợp lý khi có tất cả cơ sở hạ tầng cục bộ, bao gồm cả nhân sự, cho một trang web nhỏ chỉ để cung cấp thông tin không? Dĩ nhiên là không, bạn sẽ có trang web đó được lưu trữ. Lưu trữ hoạt động ngược lại với quy mô. Nhu cầu lưu trữ quy mô nhỏ dễ dàng được đáp ứng cục bộ, trong khi nhu cầu lưu trữ quy mô lớn thường được lưu trữ trên máy chủ hoặc trên đám mây.



**MÁCH NƯỚC CHO KỲ THI** *Tại-chỗ* có nghĩa là hệ thống nằm tại vị trí của bạn. *Ngoại-biên* nghĩa là nó nằm ở đâu đó khác – một vị trí cụ thể. Cụm từ “trên đám mây” đề cập đến việc có hệ thống được phân tán trên một cơ sở hạ tầng có thể truy cập được từ xa thông qua một mạng, với những đặc trưng cụ thể của đám mây, chẳng hạn như khả năng mở rộng, v.v... Điều này đúng cho cả *tại-chỗ* lẫn *ngoại-biên*.

### **Điện toán Sương mù**

Điện toán đám mây đã được mô tả bởi các chuyên gia là sử dụng máy tính của một ai đó khác. Nếu đúng như vậy thì *điện toán sương mù* đang sử dụng máy tính của người khác. Điện toán sương mù là một hình thức điện toán đám mây được phân tán, trong đó khối lượng công việc được thực hiện trên một kiến trúc phân tán và phi tập trung. Ban đầu được phát triển bởi Cisco, điện toán sương mù di chuyển một số công việc sang không gian cục bộ để quản lý các vấn đề về độ trễ, với đám mây kém đồng bộ hơn. Dưới hình thức này, nó tương tự như điện toán biển, được mô tả trong phần tiếp theo.

Điện toán sương mù là một kiến trúc nơi các thiết bị làm trung gian xử lý giữa phần cứng cục bộ và máy chủ từ xa. Nó quy định thông tin nào được gửi đến đám mây và thông tin nào được xử lý cục bộ, với kết quả được gửi đến người dùng ngay lập tức và lên đám mây cùng với độ trễ của nó. Người ta có thể coi điện toán sương mù là sử dụng các cửa ngõ thông minh giúp xử lý các nhu cầu tức thì trong khi quản lý việc xử lý và lưu trữ dữ liệu hiệu quả hơn của đám mây. Điều này khiến cho điện toán sương mù trở thành một phương tiện hỗ trợ cho đám mây chứ không phải một sự thay thế cho nó.

## **Điện toán Biên**

*Điện toán biên* đề cập đến việc tính toán được thực hiện ở rìa của một mạng. Điện toán biên được thúc đẩy bởi các nhà cung cấp mạng, những người có năng lực xử lý trên mạng và mong muốn có thị trường mới hơn là chỉ dựa vào các thị trường hiện có. Điện toán biên tương tự như điện toán sương mù ở chỗ nó là một công cụ hỗ trợ cho các kiến trúc máy tính hiện có - một kiến trúc được thiết kế dành cho tốc độ. Sự phát triển thực sự trong lĩnh vực điện toán biên đã xảy ra với cuộc cách mạng Internet Vạn vật - Internet of Things (IoT). Điều này là do điện toán biên dựa trên cái mà người ta định nghĩa là "cạnh", cùng với mức độ xử lý cần thiết. Trong rất nhiều môi trường, cạnh biên thực tế không lớn như người ta nghĩ và cái mà một số người gọi là điện toán biên được thực hiện tốt hơn bằng cách sử dụng điện toán sương mù. Nhưng khi bạn nhìn vào một hệ thống chẵng hạn như IoT, nơi mà hầu như mọi thiết bị đều có thể là một lợi thế, thì vấn đề là nơi thực hiện tính toán - trên thiết bị IoT nhỏ bé với nguồn tài nguyên hạn chế hoặc ở thiết bị gần nhất có sức mạnh tính toán. Điều này đã khiến các công ty mạng tạo ra các thiết bị có thể quản lý luồng dữ liệu và thực hiện quá trình tính toán.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng điện toán biên mang quá trình xử lý đến gần cạnh biên của mạng hơn, vốn sẽ tối ưu hóa các ứng dụng web và các thiết bị IoT.

### **Thin Client**

Một *think client* (*máy tính có cấu hình tối thiểu*) là một máy tính hạng nhẹ, có nguồn tài nguyên hạn chế, mục đích chính là để giao tiếp với máy khác. Các thin client có thể sẽ rất tiết kiệm khi chúng được sử dụng để kết nối với các hệ thống mạnh hơn. Thay vì có bộ nhớ 32 GB, bộ xử lý cấp cao nhất, card đồ họa cao cấp và thiết bị lưu trữ lớn trên mọi máy tính để bàn, nơi hầu hết năng lực đã không được sử dụng hết, thin client cho phép truy cập vào một máy chủ có tài nguyên thích hợp có sẵn và có thể được chia sẻ. Với điện toán đám mây và ảo hóa, nơi việc xử lý, lưu trữ và thậm chí bản thân các ứng dụng đều tồn tại trên các máy chủ trong đám mây, những gì cần thiết là một thiết bị kết nối với nguồn năng lực đó và hoạt động như một thiết bị nhập/xuất.

### **Containers**

Ảo hóa cho phép nhiều phiên bản hệ điều hành cùng tồn tại trên một nền tảng phần cứng duy nhất. Khái niệm về *vùng chứa* (*containers*) cũng tương tự như vậy, nhưng thay vì có nhiều HĐH độc lập, vùng chứa có chứa các phần của HĐH cần tách biệt với phần hạt nhân (kernel). Do đó, nhiều vùng chứa có thể cùng chia sẻ một hệ điều hành nhưng sẽ có bộ nhớ, CPU và luồng lưu trữ riêng biệt, đảm bảo rằng chúng sẽ không tương tác với các vùng chứa khác. Điều này cho phép nhiều phiên bản của một ứng dụng hoặc các ứng dụng khác nhau cùng chia sẻ một hệ điều hành chủ mà hầu như không có chi phí. Điều này cũng cho phép tính di động của ứng dụng đến một mức độ tách biệt với ngăn xếp hệ điều hành. Nhiều nền tảng vùng chứa chính đang tồn tại, chẳng hạn như Docker. Thay vì

áp dụng một giải pháp ngành cụ thể, ngành này đã liên kết lại với nhau theo một hình thức tiêu chuẩn được gọi là Open Container Initiative (tạm dịch Sáng kiến Vùng chứa Mở - OCI), được thiết kế để cho phép tiêu chuẩn hóa và sự ổn định của thị trường về môi trường. Các nhà cung cấp khác nhau trong không gian vùng chứa có các thuật ngữ hơi khác nhau, vì vậy bạn cần phải kiểm tra việc triển khai cụ thể của nhà cung cấp của bạn để hiểu định nghĩa chính xác về vùng chứa và ô (cell) trong môi trường của họ.

Bạn có thể coi vùng chứa là sự tiến hóa của khái niệm VM (máy ảo) đối với không gian ứng dụng. Một vùng chứa cấu thành từ toàn bộ môi trường thời gian chạy được đóng gói thành một gói: một ứng dụng, bao gồm tất cả các phụ thuộc, thư viện và các tập tin nhị phân khác và các tập tin cấu hình cần thiết của nó để chạy ứng dụng. Điều này giúp loại bỏ sự khác biệt giữa các môi trường phát triển, thử nghiệm và sản xuất, vì sự khác biệt nằm trong thùng chứa như một giải pháp tiêu chuẩn. Bằng cách đóng gói nền tảng ứng dụng, bao gồm cả các phụ thuộc của nó, bất kỳ sự khác biệt nào về phân phối hệ điều hành, thư viện và cơ sở hạ tầng cơ bản đều được trừu tượng hóa và được đưa ra tranh luận.



**MÁCH NƯỚC CHO KỲ THI** Các vùng chứa (container) là một hình thức ảo hóa hệ điều hành. Chúng [các vùng chứa] là sự kết hợp được-đóng-gói của mã phần mềm và những phụ thuộc của nó để giúp các ứng dụng hoạt động một cách nhanh chóng trong các môi trường điện toán khác nhau.

### **Vì dịch vụ/API**

Một *giao diện lập trình ứng dụng (API)* là một phương tiện để chỉ định cách người ta tương tác với một phần mềm như thế nào. Hãy sử dụng

một dịch vụ web làm ví dụ: nếu nó sử dụng API chuyển trạng thái biểu thị (representational state transfer - REST) thì giao diện đã được xác định là một tập hợp bao gồm bốn hành động được thể hiện trong HTTP:

- NHẬN (GET) Nhận một mục đơn lẻ hoặc một bộ sưu tập.
- ĐĂNG (POST) Thêm một mục vào bộ sưu tập.
- ĐẶT (PUT) Chính sửa một mục đã tồn tại trong một bộ sưu tập.
- XÓA (DELETE) Xóa một mục trong bộ sưu tập.

*Vi dịch vụ (Microservices)* là một phong cách kiến trúc khác. Thay vì xác định đầu vào và đầu ra, vi dịch vụ chia hệ thống thành một loạt các mô-đun nhỏ có thể được ghép nối với nhau để tạo ra một hệ thống hoàn chỉnh. Mỗi mô-đun trong kiến trúc vi dịch vụ được thiết kế đơn nhẹ, với giao diện đơn giản và hoàn chỉnh về mặt cấu trúc. Điều này cho phép phát triển và bảo trì mã nhanh hơn.

### **Cơ sở hạ tầng như Mã phần mềm**

*Cơ sở hạ tầng như mã phần mềm* là việc sử dụng các tập tin định nghĩa mà máy-có-thể-đọc-được cũng như mã phần mềm để quản lý và cung cấp các hệ thống máy tính. Bằng cách khiến cho quá trình quản lý trở nên có thể lập trình được, sẽ có những lợi thế đáng kể về khả năng mở rộng và tính linh hoạt. Thay vì phải quản lý cấu hình phần cứng vật lý bằng cách sử dụng các công cụ cấu hình tương tác, cơ sở hạ tầng dưới dạng mã phần mềm cho phép thực hiện điều này theo chương trình. Một ví dụ điển hình về điều này là trong thiết kế mạng do-phần-mềm-xác-định.

### **Kết nối mạng do Phần mềm-Xác định (SDN)**

*Mạng do-phần-mềm-xác-định (software-defined networking - SDN)* là một kiến trúc mạng trong đó mặt phẳng điều khiển và mặt phẳng dữ liệu được tách biệt với nhau. Điều này cho phép phần cứng mạng được kiểm soát theo chương trình, ngay cả khi đang trong quá trình xử lý dữ liệu. Các kiến trúc mạng truyền thống có mặt phẳng dữ liệu và mặt phẳng điều

khiển cùng tồn tại, và một trong những kết quả là tính linh hoạt của việc thay đổi mạng bị giảm đi. Điều này xuất phát từ phạm vi giao tiếp liên quan đến dữ liệu. Nơi mà luồng dữ liệu không đi đến chỉ có các tùy chọn khả năng lập trình bị hạn chế. Với SDN, sẽ tồn tại một ngăn xếp lập trình mạng hoàn chỉnh, tách biệt với các luồng dữ liệu và có thể lập trình trên toàn bộ mạng. Điều này mang lại tính linh hoạt và khả năng lập trình đáng kể trong mạng SDN, mặc dù với chi phí phức tạp. Thành phần then chốt của SDN là ảo hóa chức năng mạng (network function virtualization - NFV). NFV là một kiến trúc ảo hóa các dịch vụ mạng, chẳng hạn như các bộ định tuyến, tường lửa và bộ cân bằng tải, trái ngược với việc chạy chúng trên phần cứng chuyên dụng và cụ thể. Cùng với nhau, SDN và NFV tạo ra một mạng đầy đủ chức năng dưới cơ sở hạ tầng là mô hình kiến trúc mã phần mềm.

### **Tính tường minh do Phần-mềm-Xác-định (SDV)**

Đối với một thiết bị mạng hoạt động dựa trên dữ liệu, nó phải nhìn thấy luồng dữ liệu. Tường lửa không thể quản lý dữ liệu mà chúng không nhìn thấy, vì vậy, tường lửa được định vị một cách vật lý trên toàn mạng phù hợp với kiến trúc vật lý của hệ thống. Cũng giống như mạng do-phần-mềm-xác-định đã thay đổi cách thức mạng được quản lý, *tính tường minh do-phần-mềm-xác-định (SDV)* là một phần mở rộng của cơ sở hạ tầng này dưới dạng ý tưởng mã phần mềm cho vấn đề tính tường minh của mạng. Thay vì tường lửa thế hệ tiếp theo (NGFW) được định vị một cách chiến lược phù hợp với các luồng dữ liệu về mặt vật lý, nó sẽ được thực hiện thông qua mã phần mềm thông qua kết cấu SDN. Điều này cho phép sự linh hoạt trong thiết kế và khả năng tái cấu hình lại mạng một cách nhanh chóng, bao gồm cả các thành phần bảo mật.

## Kiến trúc Không máy chủ (Serverless)

Khi cơ sở hạ tầng được thiết lập “tại chỗ”, đơn vị của sức mạnh tính toán là một máy chủ. Để thiết lập [hệ thống] email, bạn phải thiết lập một máy chủ. Để thiết lập một trang web, bạn phải thiết lập một máy chủ. Các vấn đề tương tự cũng tồn tại đối với lưu trữ: Bạn cần lưu trữ? Hãy mua đĩa. Vâng, tất cả các đĩa này đều có thể được chia sẻ, nhưng cuối cùng, tính toán là máy chủ, lưu trữ là đĩa. Với đám mây, mọi thứ đều thay đổi. Đám mây giống như tài nguyên được chia sẻ cuối cùng và với rất nhiều nhà cung cấp lớn, bạn không chỉ định các máy chủ hoặc đĩa mà bạn sẽ chỉ định dung lượng. Sau đó, nhà cung cấp quay các tài nguyên cần thiết. *Kiến trúc không máy chủ* này đơn giản hóa rất nhiều thứ và bổ sung các khả năng đáng kể. Bằng cách chỉ định các tài nguyên cần thiết về năng lực xử lý, nhà cung cấp đám mây có thể tạo ra các tài nguyên cần thiết. Bởi vì về bản chất, bạn đang thuê từ một nhóm lớn các tài nguyên, và điều này mang lại cho bạn khả năng có công suất tăng đột biến, trong đó bạn gia tăng công suất cho một số xu hướng gia tăng sử dụng cụ thể trong một khoảng thời gian. Một trong những lợi thế về mặt vận hành của việc này là các nhà cung cấp dịch vụ đám mây có thể thực hiện những thay đổi này thông qua các tập lệnh kịch bản tự động có thể xảy ra gần như ngay lập tức, trái ngược với những vấn đề về mua sắm và cấu hình tại-chỗ. Kiến trúc này cũng hỗ trợ tích hợp dịch vụ, do đó mở rộng tiện ích của khả năng tính toán đối với doanh nghiệp.



## MÁCH NƯỚC CHO KỲ THI

Hãy biết rằng kiến trúc không máy chủ là một cách để phát triển và vận hành các ứng dụng và dịch vụ mà không cần sự sở hữu và quản lý một cơ sở hạ tầng. Các máy chủ vẫn được sử dụng nhưng chúng được sở hữu và quản lý “ngoại-biên (off-premises)”.

## Tích hợp các Dịch vụ

*Tích hợp các dịch vụ* là sự kết nối các thành phần cơ sở hạ tầng và phần mềm để cung cấp các dịch vụ cụ thể cho một thực thể doanh nghiệp. Việc kết nối quá trình xử lý, lưu trữ, cơ sở dữ liệu, web, truyền thông và các chức năng khác thành một giải pháp toàn diện được tích hợp là mục tiêu của hầu hết các tổ chức CNTT. Cơ sở hạ tầng dựa-trên-đám-mây là môi trường lý tưởng để đạt được mục tiêu này. Thông qua các tập lệnh kịch bản đã được thiết kế trước, nhà cung cấp đám mây có thể quản lý việc tích hợp dịch vụ theo cách có thể mở rộng hơn nhiều so với các doanh nghiệp riêng lẻ. Đối với một doanh nghiệp, mỗi tích hợp là một lần sáng tạo duy-nhất, trong khi nhà cung cấp dịch vụ đám mây có thể tận dụng khả năng tái tạo của việc thực hiện các tích hợp giống nhau cho rất nhiều khách hàng. Và với điều này, quy mô và trải nghiệm trở thành tiết kiệm chi phí và độ tin cậy.

## Các Chính sách Tài nguyên

Khi bạn đang chỉ định những chi tiết về tương tác với đám mây, mức độ năng lực xử lý nào, ứng dụng nào, yêu cầu bảo mật nào, dung lượng lưu trữ và kiểm soát truy cập, tất cả đều là tài nguyên. Việc quản lý các hạng mục này được thực hiện thông qua các *chính sách tài nguyên*. Mỗi nhà cung cấp dịch vụ đám mây có một cách khác nhau để cho phép bạn tương tác với trình đơn dịch vụ của họ, nhưng cuối cùng, bạn đang chỉ định các chính sách tài nguyên mà bạn muốn áp dụng cho tài khoản của mình. Thông qua các chính sách tài nguyên, bạn có thể xác định cái gì, ở đâu hoặc cách thức tài nguyên sẽ được cung cấp. Điều này cho phép tổ chức của bạn thiết lập nên các hạn chế, quản lý tài nguyên và quản lý chi phí của đám mây.

## Cửa ngõ Chuyển tiếp

Một *cửa ngõ chuyển tiếp* là một kết nối mạng được sử dụng để kết nối các đám mây riêng tư ảo (VPCs) và các mạng tại-chỗ với nhau. Thông

qua việc sử dụng cửa ngõ chuyển tiếp, các tổ chức có thể xác định và kiểm soát giao tiếp giữa những tài nguyên trên mạng của nhà cung cấp dịch vụ đám mây và cơ sở hạ tầng của riêng mình. Các cửa ngõ chuyển tiếp là duy nhất đối với từng nhà cung cấp và được triển khai một cách phổ biến để hỗ trợ cho việc quản trị môi trường đám mây của nhà cung cấp.

## Ảo hóa

Công nghệ *ảo hóa* được sử dụng để cho phép một máy tính có nhiều hơn một Hệ điều hành hiện diện và, trong rất nhiều trường hợp, hoạt động tại cùng một thời điểm.

Ảo hóa là một phần trừu tượng của lớp Hệ điều hành, tạo ra khả năng lưu trữ nhiều hệ điều hành trên cùng một phần cứng. Để kích hoạt ảo hóa, một hypervisor sẽ được sử dụng. *Hypervisor* là một chương trình cấp-thấp cho phép nhiều hệ điều hành chạy đồng thời trên một máy tính vật chủ duy nhất. Hypervisor sử dụng một lớp mỏng (thin layer) mã phần mềm để phân bổ tài nguyên theo thời gian thực. Hypervisor hoạt động như một cảnh sát giao thông điều khiển I/O và quản lý bộ nhớ. Một trong những ưu điểm chính của ảo hóa là sự tách biệt giữa phần mềm và phần cứng, tạo ra một rào cản có thể cải thiện nhiều chức năng của hệ thống, bao gồm cả bảo mật. Phần cứng nền tảng bên dưới được gọi là máy vật chủ và trên đó là hệ điều hành vật chủ. Hệ điều hành vật chủ có khả năng hypervisor được tích hợp sẵn hoặc cần có ứng dụng để cung cấp chức năng hypervisor để quản lý các máy ảo (virtual machine - VM). Các máy ảo thường được gọi là hệ điều hành khách. Có hai kiểu hypervisor tồn tại bao gồm: Kiểu I và Kiểu II.



## MÁCH NƯỚC CHO KỲ THI

Một hypervisor là một tương tác giữa một máy ảo và phần cứng của máy vật chủ. Các hypervisor bao gồm các lớp cho phép sự ảo hóa.

### Kiểu I

Các *hypervisor* Kiểu I hoạt động trực tiếp trên phần cứng của hệ thống. Chúng được gọi là hypervisor tự nhiên, bare-metal hoặc được nhúng trong tài liệu về nhà cung cấp điển hình. Các hypervisor kiểu I được thiết kế dành cho tốc độ và hiệu quả, vì chúng không phải hoạt động qua một lớp hệ điều hành khác. Ví dụ về hypervisor Loại I bao gồm KVM (Kernel-based Virtual Machine - Máy ảo Dựa-trên-Lõi-hạt-nhân, một triển khai của Linux), Xen (triển khai của Citrix Linux), Microsoft Windows Server Hyper-V (phiên bản headless của lõi hệ điều hành Windows) và nền tảng vSphere/ESXi của VMware. Tất cả các hypervisor Kiểu I này được thiết kế cho thị trường máy chủ cao cấp trong doanh nghiệp và được thiết kế để cho phép rất nhiều máy ảo hoạt động trên một tập hợp phần cứng máy chủ. Những nền tảng này đi kèm với các bộ công cụ quản lý để tạo điều kiện thuận lợi cho việc quản lý VM trong doanh nghiệp.

### Kiểu II

Các *hypervisor* Kiểu II hoạt động trên hệ điều hành vật chủ. Trong thời kỳ đầu của phong trào ảo hóa, các hypervisor kiểu II là phổ biến nhất. Các quản trị viên có thể mua phần mềm VM và cài đặt nó trên máy chủ mà họ thực sự đang chạy. Các hypervisor kiểu II điển hình bao gồm VirtualBox của Oracle và VMware Player của VMware. Chúng được thiết kế cho số lượng máy ảo giới hạn, thường chạy trong một môi trường máy tính để bàn hoặc máy chủ nhỏ.

## Máy ảo Tránh Ngổn ngang

Ngổn ngang (sprawl) là sự lan rộng và vô tổ chức của tình trạng không kiểm soát được do thiếu cơ cấu tổ chức khi có rất nhiều yếu tố giống nhau đòi hỏi sự quản lý. Cũng giống như bạn có thể mất dấu một tập tin trong thư mục tập tin lớn và phải tìm kiếm nó, bạn cũng có thể mất dấu một máy ảo trong số nhiều máy ảo khác đã được tạo ra. Về cơ bản, máy ảo là các tập tin chứa bản sao của cấu trúc đĩa và bộ nhớ của máy đang hoạt động. Việc tạo ra một máy ảo mới là một quá trình đơn giản. Nếu một tổ chức chỉ có một vài máy ảo, việc theo dõi chúng tương đối dễ dàng. Nhưng khi số lượng VM gia tăng nhanh chóng theo thời gian, sự ngổn ngang có thể sẽ xuất hiện. Sự ngổn ngang của VM là một triệu chứng của một cấu trúc vô tổ chức. Một tổ chức cần phải triển khai *tránh sự ngổn ngang của VM* thông qua chính sách. Nó có thể tránh sự ngổn ngang của máy ảo thông qua các quy ước đặt tên và kiến trúc lưu trữ thích hợp để từ đó, các tập tin nằm trong danh bạ/thư mục chính xác, giúp cho việc tìm kiếm chính xác máy ảo trở nên dễ dàng và hiệu quả. Nhưng cũng như trong bất kỳ hệ thống lưu trữ nào, nó sẽ chỉ hoạt động nếu mọi người thường xuyên tuân theo các chính sách và thủ tục đã được thiết lập để đảm bảo rằng việc đặt tên và lưu trữ VM một cách phù hợp đã được thực hiện.

Một trong những đề án kinh doanh mạnh nhất cho một công cụ quản lý VM được tích hợp như Máy chủ eSXi từ VMware là khả năng cho phép quản trị viên quản lý các máy ảo và tránh sự ngổn ngang. Khả năng xác định vị trí và sử dụng tài nguyên khi cần thiết là một yếu tố bảo mật, đặc biệt là tính sẵn sàng và sự ngổn ngang gây ra các vấn đề về tính sẵn sàng.

## Bảo vệ Thoát khỏi Máy ảo

Khi nhiều máy ảo đang hoạt động trên một nền tảng phần cứng duy nhất, một mối quan tâm là *thoát máy ảo*, nơi phần mềm, phần mềm độc hại hoặc kẻ tấn công, thoát ra từ một máy ảo đến hệ điều hành nền tảng. Khi việc thoát máy ảo xảy ra, kẻ tấn công có thể tấn công hệ điều hành nền tảng hoặc lại xuất hiện trong một máy ảo khác. Khi bạn xem xét vấn đề theo quan điểm logic, cả hai máy ảo đều sử dụng cùng một bộ nhớ RAM, cùng một bộ xử lý, v.v... sự khác biệt ở đây là một trong những kết hợp cụ thể và đúng thời điểm. Trong khi hệ thống VM được thiết kế để cung cấp sự bảo vệ, cũng như với tất cả những thứ có quy mô lớn hơn, điều quan trọng nằm ở chi tiết. Môi trường VM quy-mô-lớn có các mô-đun cụ thể được thiết kế để phát hiện quá trình thoát và cung cấp khả năng *bảo vệ thoát VM* (*VM escape protection*) cho các mô-đun khác.



## MÁCH NƯỚC CHO KỲ THI

Các môi trường ảo hóa có một số những khái niệm cụ thể mà kỳ thi có thể phải giải quyết. Hãy hiểu về sự khác biệt giữa sự ngốn ngang của VM và thoát VM và các vấn đề mà chúng gây ra. Hãy dự kiến các câu hỏi cho những gì mà bạn đã được cung cấp về những thuật ngữ này như là các tùy chọn và phải lựa chọn đúng đáp án.

## Tóm tắt Chương

Trong chương này, bạn đã được làm quen với các dịch vụ ảo hóa và đám mây. Chương này mở đầu với mô tả về các mô hình đám mây khác nhau, bao gồm Cơ sở hạ tầng như một Dịch vụ, Nền tảng như một Dịch vụ, Phần mềm như một Dịch vụ và Bất kỳ thứ gì như một Dịch vụ. Các mô hình đám mây riêng tư, công cộng, lai và cộng đồng cũng đã được khám phá. Tiếp theo, các chủ đề về nhà cung cấp dịch vụ đám mây, nhà cung cấp dịch vụ được quản lý và nhà cung cấp dịch vụ bảo mật được quản lý đã được đề cập, sau đó là các vấn đề liên quan đến cung cấp tại-chỗ, được lưu trữ và dựa-trên-đám-mây.

Kế tiếp, các thành phần thuộc kiến trúc của điện toán sương mù, điện toán biên và điện toán thin client được đề cập, đồng thời các vùng chứa và API/vi dịch vụ cũng được khám phá. Việc quản lý tài nguyên đám mây thông qua cơ sở hạ tầng dưới dạng mã phần mềm, kiến trúc không máy chủ, tích hợp dịch vụ, chính sách tài nguyên và cửa ngõ chuyển tiếp đã được đề cập. Chương này kết thúc với việc kiểm tra về ảo hóa, hypervisor, cả kiểu I và II, và các vấn đề với sự ngổn ngang của VM và thoát VM.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Một hypervisor cho phép nhiều hệ điều hành khách hoạt động một cách đồng thời trên một máy tính chủ như thế nào?

  - A. Thông qua một gói trình điều khiển được chuyên biệt hóa
  - B. Bằng cách trừu tượng hóa phần cứng từ hệ điều hành khách
  - C. Bằng cách cung cấp phần cứng ảo cụ thể cho từng Hệ điều hành khách
  - D. Bằng cách ẩn đi hệ điều hành Linux nền tảng.
2. Bạn đã triển khai một mạng bao gồm các cảm biến được-kết-nối-Internet qua một khu vực địa lý rất rộng. Những cảm biến này là các thiết bị IoT nhỏ có mức-điện-năng-thấp, và bạn cần phải thực hiện việc chuyển đổi và thu thập dữ liệu về nhiệt độ trong một cơ sở dữ liệu. Những tính toán tốt nhất sẽ được quản lý bởi kiến trúc nào?

  - A. Điện toán sương mù
  - B. Điện toán biên
  - C. Thin client
  - D. Cơ sở dữ liệu phân tán trên đám mây.
3. Ứng dụng mới của bạn có nhiều tiến trình nhỏ để cung cấp dịch vụ cho mạng. Bạn muốn khiến cho ứng dụng này hoạt động một cách hiệu quả hơn bằng cách ảo hóa nó. Phương pháp tiếp cận tốt nhất để ảo hóa ứng dụng này là gì?

  - A. Hypervisor kiểu II
  - B. Linux KVM
  - C. Đóng gói (containerization)

**D. Hypervisor kiểu I.**

- 4.** Tại sao sự ngắn ngang của VM lại là một vấn đề?
  - A.** VM ngắn ngang sử dụng quá nhiều tài nguyên trên các chức năng song song
  - B.** Càng nhiều máy ảo được sử dụng thì càng khó để chuyển đổi một VM thành máy chủ thực
  - C.** Các máy ảo rất dễ tạo ra, bạn sẽ kết thúc với hàng trăm máy chủ nhỏ chỉ để thực hiện một chức năng duy nhất
  - D.** Khi các máy chủ không còn là vật lý nữa, có thể sẽ rất khó để định vị một máy cụ thể.
- 5.** Khi tiến hành ứng phó sự cố cho công ty của bạn, bạn đánh giá pháp y về một số máy chủ ảo và bạn thấy kẻ tấn công trên máy chủ web đang chèn mã vào các khôi bộ nhớ chưa được khởi tạo. Kẻ tấn công có khả năng đang cố gắng thực hiện cuộc tấn công nào?
  - A.** Tấn công từ-chối-dịch-vụ vào hypervisor
  - B.** Thoát VM
  - C.** Tấn công containerization
  - D.** Phá vỡ CASB
- 6.** Bạn đang có kế hoạch chuyển một số ứng dụng lên đám mây, bao gồm cả ứng dụng kế toán của tổ chức bạn, và ứng dụng này được tùy chỉnh cao và không mở rộng quy mô tốt. Mô hình triển khai đám mây nào là tốt nhất cho ứng dụng này?
  - A.** SaaS
  - B.** PaaS
  - C.** IaaS
  - D.** Không có lựa chọn nào như trên.
- 7.** Bạn cần chuyển một mô-đun dịch vụ khách hàng cụ thể có giao diện người dùng web sang đám mây. Ứng dụng này có khả năng

mở rộng cao và có thể được cung cấp theo yêu cầu. Mô hình triển khai đám mây nào là tốt nhất cho ứng dụng này?

- A. SaaS**
  - B. PaaS**
  - C. IaaS**
  - D. Không có lựa chọn nào như trên.**
- 8.** Một trong những tài nguyên chính đang được sử dụng tại tổ chức của bạn là một cơ sở dữ liệu tiêu chuẩn mà nhiều ứng dụng gắn liền vào đó. Mô hình triển khai đám mây nào là tốt nhất cho loại ứng dụng này?
- A. SaaS**
  - B. PaaS**
  - C. IaaS**
  - D. Không có lựa chọn nào như trên.**
- 9.** Mô hình triển khai đám mây nào có ít biện pháp kiểm soát bảo mật nhất?
- A. Riêng tư**
  - B. Công cộng**
  - C. Lai**
  - D. Cộng đồng.**
- 10.** Nhược điểm chính của mô hình triển khai đám mây riêng tư là gì?
- A. Các quy tắc truy cập hạn chế**
  - B. Chi phí**
  - C. Khả năng mở rộng**
  - D. Thiếu sự hỗ trợ của nhà cung cấp.**

## Đáp án

1. **B.** Hypervisor tách phần cứng khỏi hệ điều hành khách để cho phép nhiều hệ điều hành khách hoạt động đồng thời trên một máy tính chủ.
2. **B.** Điện toán biên trên đường lên đám mây sẽ phù hợp nhất với khả năng xử lý hạng nhẹ của các thiết bị IoT.
3. **C.** Containerization chạy các ứng dụng nhỏ trên hệ điều hành chủ mà hầu như không tốn chi phí.
4. **D.** Sự ngổn ngang của máy ảo là một vấn đề vì khi máy ảo phát triển mạnh mẽ, chúng có thể dễ dàng được di chuyển và có khả năng dễ dàng được sao chép đến các vị trí ngẫu nhiên. Điều này có thể khiến việc tìm kiếm một máy cụ thể trở nên khó khăn nếu không có một cơ cấu tổ chức được xây dựng một cách cẩn thận và được quản lý một cách nhất quán.
5. **B.** Mặc dù tất cả mọi hypervisor đều tích cực cố gắng ngăn chặn nó, nhưng bất kỳ sai sót nào trong việc xử lý bộ nhớ đều có thể cho phép mã được đặt một cách độc hại trong một khối sẽ được đọc bởi hypervisor hoặc một máy khác. Điều này còn được gọi là thoát VM. Kịch bản chỉ ra máy chủ ảo, loại bỏ câu trả lời C và D và các khối mã vận hành trong bộ nhớ chưa được khởi tạo sẽ không gây ra từ chối dịch vụ, loại bỏ được đáp án A.
6. **C.** Cơ sở hạ tầng như một Dịch vụ thích hợp cho các giải pháp được tùy chỉnh cao, có khả năng mở rộng kém và yêu cầu các tài nguyên cụ thể để hoạt động.
7. **A.** Phần mềm như một Dịch vụ thích hợp để cung cấp các ứng dụng theo-nhu-cầu, có khả năng mở rộng cao mà không cần cài đặt phần mềm điểm đầu cuối.
8. **B.** Nền tảng như một Dịch vụ phù hợp với các tài nguyên tiêu chuẩn đang được sử dụng bởi nhiều ứng dụng khác.

9. **B.** Môi trường dùng chung của đám mây công cộng có ít biện pháp kiểm soát bảo mật nhất.
10. **B.** Mô hình đám mây riêng tư đặt hơn đáng kể, vì nó là một tài nguyên chuyên dụng, phủ nhận một số lợi thế của việc thuê ngoài cơ sở hạ tầng ngay từ ban đầu.

## Chương 11 Các Khái niệm về Phát triển, Triển khai và Tự động hóa Ứng dụng An toàn

### Các Khái niệm về Phát triển, Triển khai và Tự động hóa Ứng dụng An toàn

Trong chương này bạn sẽ

- Tìm hiểu cách để triển khai việc phát triển ứng dụng an toàn,
- Tìm hiểu các khái niệm phát triển an toàn,
- Khám phá bổ sung về bảo mật đối với các quy trình tự động hóa/nhanh nhẹy (agile).

Phát triển phần mềm là một quá trình phức tạp với rất nhiều vấn đề khác nhau, từ thiết kế đến lập trình, đến kiểm nghiệm và triển khai, đều cần phải được xem xét và quản lý để đạt được những mục đích mong muốn về phần mềm được bảo mật. Việc phát triển và sử dụng quy trình phát triển một ứng dụng bao-gồm-bảo-mật là một điều thiết yếu. Việc mở rộng quy trình này để bao gồm cả các vấn đề cung cấp và sau-phát-triển cũng là điều tối quan trọng, và một trong những công cụ chính để đạt được những mục tiêu này là sử dụng tự động hóa và viết [tập lệnh] kịch bản. Chương này đề cập đến các vấn đề liên quan đến các mục tiêu kỳ thi Security+ Phiên bản 6.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 2.3 của kỳ thi CompTIA Security+: Tóm tắt các khái niệm phát triển, triển khai và tự động hóa ứng dụng

## Môi trường

Hầu hết các tổ chức đều có các *môi trường* điện toán tách biệt và đa dạng, được thiết kế để mang lại sự cô lập giữa các chức năng về phát triển, kiểm nghiệm, phân giai đoạn, và sản xuất. Mục đích chủ yếu của việc tách biệt các môi trường này là để ngăn chặn các sự cố bảo mật phát sinh từ các đoạn mã phần mềm chưa được kiểm nghiệm đi vào môi trường sản xuất. Phần cứng của những môi trường này được tách biệt và danh sách kiểm soát truy cập được sử dụng để ngăn chặn việc người dùng truy cập vào nhiều môi trường cùng một lúc. Việc di chuyển mã phần mềm giữa các môi trường đòi hỏi một tài khoản đặc biệt có thể truy cập cả hai, nhằm giảm thiểu các vấn đề lây nhiễm chéo.

## Phát triển

*Môi trường phát triển* được định cỡ, thiết lập cấu hình và cài đặt để phát triển các ứng dụng và hệ thống. Không giống như phần cứng [của môi trường] sản xuất, phần cứng [của môi trường] phát triển không nhất thiết phải có khả năng mở rộng và nó có thể không cần phải đáp ứng nhanh đổi với một số các giao dịch nhất định. Nền tảng phát triển cần phải sử dụng cùng một loại và phiên bản của hệ điều hành như đang được sử dụng trong môi trường sản xuất, vì việc phát triển trên Windows và triển khai lên Linux gặp rất nhiều khó khăn mà có thể tránh được bằng cách phù hợp với môi trường về kiểu và phiên bản hệ điều hành. Sau khi mã được phát triển thành công, nó sẽ được chuyển sang hệ thống thử nghiệm.

## Kiểm nghiệm

*Môi trường kiểm nghiệm* mô phỏng một cách khá chặt chẽ môi trường sản xuất - các phiên bản phần mềm giống nhau, đến mức bản vá lỗi, cùng bộ phân quyền, cùng cấu trúc tập tin, v.v... Mục đích của môi trường thử nghiệm là để kiểm tra toàn bộ hệ thống trước khi triển khai vào môi trường sản xuất để đảm bảo rằng hệ thống đó không có lỗi và sẽ không gây ra gián đoạn cho môi trường sản xuất. Môi trường kiểm nghiệm có

thể không có quy mô như môi trường sản xuất, nhưng xét về khía cạnh phần mềm/phần cứng, nó sẽ giống hệt như môi trường sản xuất. Đây là điều rất quan trọng để đảm bảo rằng các thiết lập dành-riêng-cho-hệ-thống được kiểm tra trong một môi trường giống hệt với môi trường mà chúng sẽ được vận hành.

### **Chia giai đoạn**

*Môi trường chia giai đoạn* là một môi trường tùy chọn, nhưng nó thường được sử dụng khi một tổ chức có rất nhiều môi trường sản xuất. Sau khi vượt qua quá trình kiểm nghiệm, hệ thống được chuyển sang giai đoạn chia giai đoạn, để từ đó nó có thể được triển khai cho các hệ thống sản xuất khác nhau. Mục đích chính của phân đoạn là phục vụ như một hộp cát (sandbox) sau khi thử nghiệm, do đó, hệ thống kiểm nghiệm có thể kiểm tra giai đoạn tiếp theo trong khi giai đoạn hiện tại được triển khai trên toàn bộ doanh nghiệp. Một phương pháp triển khai là triển khai theo giai đoạn, trong đó phần mềm được triển khai cho một phần của doanh nghiệp và sau đó được tạm dừng để theo dõi các vấn đề chưa được nhìn thấy. Nếu không có gì xảy ra, việc triển khai tiếp tục, theo từng giai đoạn, cho đến khi tất cả các hệ thống sản xuất đều được thay đổi. Bằng cách chuyển đổi phần mềm theo cách này, bạn sẽ không bao giờ mất hệ thống sản xuất cũ cho đến khi kết thúc quá trình chuyển đổi, giúp bạn có đủ thời gian theo dõi và nắm bắt mọi vấn đề đã không lường trước được. Điều này cũng ngăn chặn việc mất toàn bộ quá trình sản xuất đối với một bản cập nhật thất bại.

### **Sản xuất**

*Môi trường sản xuất* là nơi các hệ thống hoạt động với những dữ liệu thực, thực hiện quy trình nghiệp vụ mà hệ thống đã được dự kiến để hoàn thành. Đây là một môi trường nơi mà, theo thiết kế, có rất ít thay đổi

xảy ra, và những gì cần phải được thực hiện trước tiên hết phải được phê duyệt và kiểm nghiệm thông qua quy trình quản lý thay đổi của hệ thống.



**MÁCH NƯỚC CHO KỲ THI** Hãy tìm hiểu về cấu trúc và mục đích của các môi trường khác nhau để từ đó khi được cung cấp một kịch bản và được yêu cầu xác định môi trường nào là thích hợp, bạn có thể chọn được đáp án đúng nhất: phát triển, kiểm nghiệm, chia giai đoạn, hay sản xuất.

### **Đảm bảo Chất lượng (QA)**

*Đảm bảo chất lượng (QA)* là một bước phổ biến trong bất kỳ quy trình sản xuất nào, và ngành phần mềm cũng không phải là ngoại lệ. Việc đảm bảo rằng chất lượng trong một sản phẩm là một vấn đề về quy trình, không phải là vấn đề về sự kiểm tra. Dĩ nhiên, việc kiểm nghiệm vẫn là điều cần thiết nhưng trạng thái hiện đại nhất là cố gắng giải quyết các vấn đề về bảo mật và chất lượng thông qua các quy trình xây dựng phần mềm thực tế, không phải chỉ là có một loạt các nhân viên kiểm tra sau khi nó đã được xây dựng. Phải nói rằng vẫn còn có vai trò của những người chuyên tập trung vào các vấn đề về chất lượng và bảo mật trong việc duy trì sổ đăng ký lỗi (một danh sách tất cả các lỗi) và giúp những người thích hợp trong nhóm nhận được thông tin chính xác liên quan đến việc xây dựng phần mềm an toàn.

### **Cấp phép và Ngừng cấp phép**

*Cấp phép* là quá trình chỉ định quyền hoặc thẩm quyền cho các đối tượng. Những người dùng có thể được cấp phép trong các nhóm, và các quy trình hoặc luồng máy tính có thể được cấp phép cho mức thẩm quyền cao hơn khi thực thi. *Hủy cấp phép* là việc loại bỏ quyền hạn hoặc thẩm quyền. Trong lĩnh vực bảo mật lập trình, thực tiễn là chỉ cung cấp một luồng lên đến cấp độ thực thi được nâng cao (ví dụ: root) trong thời gian cần có

quyền quản trị. Sau khi các bước đó trôi qua, luồng có thể được hủy cấp phép để trở lại mức truy cập thấp hơn. Sự kết hợp này làm giảm khoảng thời gian ứng dụng ở cấp độ thẩm quyền cao hơn, từ đó làm giảm nguy cơ rủi ro nếu chương trình bị chiếm quyền hoặc bị tấn công.

## **Phép đo Tính toàn vẹn**

Tính toàn vẹn được định nghĩa trong lĩnh vực bảo mật là sự xác định rằng dữ liệu không bị thay đổi trái phép. Trong môi trường phát triển và triển khai phần mềm, đây là một vấn đề rất quan trọng vì ngay cả những thay đổi nhỏ cũng có thể gây ra những vấn đề rất lớn và khó phát hiện. Việc duy trì quyền kiểm soát đối với cơ sở mã phần mềm (codebase) có nghĩa rằng có hai điều đang xảy ra. Đầu tiên, bạn phải có quyền kiểm soát các bản sao theo cách mà mọi người chỉ đang làm việc trên một cơ sở mã phần mềm hợp pháp. Không có gì làm hỏng một ngày nhanh hơn việc phát hiện ra phiên lập trình cả-ngày của bạn được thực hiện trên một bộ mã không được cập nhật - nói cách khác, bạn đã làm việc trên một bản sao sai. Tuy không thảm hại bằng việc sơn nhầm cho ngôi nhà (bạn không cần phải sơn lại), nhưng về bản chất, công trình đã bị thiệt hại. Khi mã được thay đổi liên tục từ nhiều tác giả, điều này không hề đơn giản như bạn tưởng tượng và một số hình thức kiểm soát phiên bản là điều bắt buộc. Thứ hai, bạn duy trì một nhật ký ghi lại các thay đổi và phương pháp xác định các phiên bản. Hệ thống kiểm soát phiên bản bạn đang sử dụng nên theo dõi các phiên bản, nhưng để xác định một cách rõ ràng một bộ mã phần mềm thì cần một công cụ khác. Một thuật toán băm tạo ra một giá trị băm duy nhất cho mỗi hạng mục duy nhất mà nó hoạt động và cơ sở mã phần mềm là các đối tượng kỹ thuật số. Việc duy trì một thư mục các giá trị băm biểu thị các phiên bản khác nhau của cơ sở mã phần mềm là cách thức các biện pháp kiểm soát tính toàn vẹn được chú thích trong mã. Nếu bạn có một phiên bản của mã, bạn có thể băm nó ra và tra cứu trong bảng phiên bản để xem bạn đang có phiên bản nào. Điều

này vượt trội hơn rất nhiều so với việc gắn nhãn trong mã với siêu dữ liệu vì các nhãn có thể được thay đổi, nhưng hàm băm được gắn với mã. Khi mã được phát hành để triển khai, nó thường được ký bằng kỹ thuật số và một lần nữa các giá trị băm đảm bảo cho người dùng rằng mã đã không bị thay đổi.

### Các Kỹ thuật Lập trình Bảo mật

Bảo mật phần mềm bắt đầu bằng mã phần mềm được bảo mật và không có lỗ hổng bảo mật. Thật không may, tất cả mã phần mềm đều có những điểm yếu và lỗ hổng bảo mật, vì vậy việc khởi tạo mã theo cách có khả năng phòng thủ hiệu quả để ngăn chặn việc khai thác các lỗ hổng có thể giúp duy trì được mức độ bảo mật mong muốn. Việc xử lý các cấu hình, lỗi và ngoại lệ và đầu vào một cách đúng đắn có thể hỗ trợ cho việc tạo một ứng dụng được bảo mật. Việc kiểm nghiệm ứng dụng trong suốt vòng đời của hệ thống có thể xác định hồ sơ rủi ro bảo mật thực tế của hệ thống.

Có rất nhiều yếu tố riêng lẻ trong vòng đời phát triển an toàn (SDL) có thể hỗ trợ cho một nhóm phát triển mã phần mềm được bảo mật. Các quy trình SDL chính xác, chẳng hạn như xác thực đầu vào, xử lý lỗi và ngoại lệ thích hợp, cũng như giảm thiểu việc chèn tập lệnh chéo-trang và giả mạo yêu cầu chéo-trang, có thể cải thiện tính bảo mật của mã phần mềm. Các yếu tố của quy trình như kiểm tra bảo mật, quản lý mờ (fuzzing) và quản lý vá lỗi cũng giúp đảm bảo các ứng dụng đáp ứng được cấu hình rủi ro mong muốn.

### Chuẩn hóa

*Chuẩn hóa* là một bước đầu tiên trong quá trình xác thực đầu vào. Cụ thể, đó là quá trình tạo ra biểu mẫu hợp chuẩn, hoặc biểu mẫu đơn giản nhất, của một chuỗi trước khi xử lý. Các chuỗi có thể được mã hóa bằng Unicode và các phương pháp mã hóa khác. Điều này khiến cho việc so

sánh từng-byte trở nên vô nghĩa khi cố gắng sàng lọc các chuỗi đầu vào của người dùng. Việc kiểm tra xem chuỗi có phải là "rose" hay không có thể khó khăn khi "A rose is a rose is a r%6fse". Quá trình chuẩn hóa chuyển đổi tất cả những thứ này (rose hoặc r%6sfe) thành "rose", nơi chúng có thể được sàng lọc như là đầu vào hợp lệ.

Các thư viện khác nhau tồn tại để hỗ trợ các nhà phát triển thực hiện phần xác thực đầu vào này. Các nhà phát triển nên luôn luôn chuẩn hóa đầu vào của họ trước khi thực hiện các bước xác thực để loại bỏ Unicode và các vấn đề mã hóa khác. Theo tiêu chuẩn Unicode, "Khi việc triển khai giữ cho các chuỗi ở dạng hợp chuẩn, họ có thể yên tâm rằng các chuỗi tương đương có một biểu diễn nhị phân duy nhất".

### A Rose is a rose is a r%6fse

*Biểu mẫu hợp chuẩn* đề cập đến hình thức đơn giản nhất và, bởi vì rất nhiều lược đồ mã hóa được sử dụng, có thể trở thành một vấn đề phức tạp. Các ký tự có thể được mã hóa bằng ASCII, Unicode, hex, UTF-8, và thậm chí là bằng sự kết hợp giữa các lược đồ mã hóa. Vì vậy, nếu như kẻ tấn công muốn làm xáo trộn một phản hồi thì một số thứ có thể xảy ra.

Bằng cách mã-hóa-URL các chuỗi URL, có thể có khả năng vượt qua các hệ thống bảo mật bộ lọc và các hệ thống phát hiện xâm nhập.

Ví dụ, URL

`http://www.myweb.com/cgi?file=/etc/passwd`

có thể trở thành:

`http://www.myweb.com/cgi?file=%2F%65%74%63%2F%70%61%73%73%77%64`

Mã-hóa-hai-lần có thể làm phức tạp thêm vấn đề. Do đó, vòng giải mã đầu tiên

scripts/..%25c../winnt

trở thành

scripts/..%5c../winnt (%25 = "%")

Và vòng mã hóa thứ hai

scripts/..%5c../winnt

trở thành

scripts/..\\..../winnt

Dòng cuối cùng rất đơn giản: biết rằng việc mã hóa có thể được sử dụng và lập kế hoạch cho việc này khi thiết kế cơ chế xác-thực-đầu-vào. Hãy kỳ vọng rằng truyền tải được mã hóa sẽ được sử dụng để vượt qua các cơ chế bảo mật.

## Các Thủ tục Lưu trữ

Các *thủ tục lưu trữ* là những phương pháp tương tác với các công cụ cơ sở dữ liệu. Các thủ tục được lưu trữ là những phương pháp truy cập dữ liệu được biên dịch sẵn theo kịch bản mang lại rất nhiều ưu điểm. Đầu tiên là tốc độ. Bởi vì chúng đã được biên dịch trước nên chúng có thể hoạt động hiệu quả hơn nhiều trong môi trường sản xuất. Nhưng vì chúng được lập kịch bản trước nên chúng cung cấp ít tính linh hoạt hơn nhiều so với các phương pháp khác, chẳng hạn như sử dụng truy vấn được tham số hóa hoặc xây dựng và thực thi các câu lệnh SQL trong một chương trình ứng dụng.



## MÁCH NƯỚC CHO KỲ THI

Một thủ tục lưu trữ là một nhóm bao gồm một hay nhiều câu lệnh được lưu trữ trong một cơ sở dữ liệu. Các thủ tục lưu trữ được sử dụng trong những ngôn ngữ lập trình như SQL, Java, C++ và C.

## Gây hoang mang/Ngụy trang

*Gây hoang mang* hay *ngụy trang* là sự che giấu ý nghĩa hiển nhiên khỏi tầm quan sát. Mặc dù tính che đậy không được coi là bảo mật đầy đủ trong hầu hết các trường hợp, nhưng việc thêm tính năng gây bối rối hoặc ngụy trang vào hệ thống để khiến kẻ tấn công khó hiểu và khó khai thác hơn cũng là một điều tốt. Việc đánh số các máy chủ email của bạn là email1, email2, email3, ... gợi ý cho kẻ tấn công biết không tên gọi cần khám phá. Việc loại bỏ hoặc ẩn những gợi ý này khiến cho công việc trở nên khó khăn hơn và cung cấp thêm một lớp bảo vệ khác.

Điều này hoạt động tốt đối với tên gọi của dữ liệu và các phần tử đã được tiếp xúc khác bắt buộc phải tiếp xúc với bên ngoài. Một trường hợp khi điều này không hoạt động tốt là trong việc xây dựng mã. Mã bị xáo trộn, hoặc mã khó hoặc thậm chí gần như không thể đọc được, là một quả bom hẹn giờ đang kêu tích tắc. Sẽ đến ngày ai đó cần đọc mã, tìm ra cách hoạt động của nó để có thể sửa đổi hoặc xác định lý do tại sao nó không hoạt động. Nếu các lập trình viên gặp những vấn đề khi đọc và hiểu mã, bao gồm cách nó hoạt động và những gì nó phải làm thì họ có thể đóng góp vào việc bảo trì nó như thế nào?

## Tái sử dụng Mã và Mã Chết

Việc phát triển phần mềm hiện đại bao gồm việc tái sử dụng rộng rãi các thành phần. Từ các thư viện thành phần đến các chức năng chung trên CompTIA Security+ - All in One - Exam Guide

nhiều thành phần đều dẫn đến cơ hội đáng kể để giảm chi phí phát triển thông qua việc tái sử dụng. Điều này cũng có thể đơn giản hóa một hệ thống thông qua việc tái sử dụng các phần tử đã biết. Mặt trái của việc tái sử dụng ồ ạt có liên quan đến môi trường độc canh, đó là nơi mà sự thất bại có ảnh hưởng lớn hơn vì tất cả những nơi mà nó có liên quan.

Trong giai đoạn thiết kế, các quyết định nên được đưa ra về mức độ tái sử dụng thích hợp. Đối với một số chức năng phức tạp, chẳng hạn như trong mã hóa, sử dụng lại là cách ưu tiên. Trong những trường hợp khác, khi nguồn gốc của một thành phần không thể được xác lập, rủi ro của việc sử dụng có thể lớn hơn cả lợi ích. Ngoài ra, việc bao gồm mã phần mềm trước đó, đôi khi được gọi là *mã kế thừa*, có thể làm giảm các nỗ lực phát triển và rủi ro.



## MÁCH NƯỚC CHO KỲ THI

Việc sử dụng mã kế thừa trong các dự án hiện tại không loại trừ mã đó khỏi các quá trình đánh giá bảo mật. Tất cả mã đều phải nhận được sự giám sát giống nhau, đặc biệt là mã kế thừa có thể đã được phát triển trước khi áp dụng các quy trình vòng đời phát triển phần mềm (SDLC).

*Mã chết* là mã phần mềm, mặc dù nó có thể được thực thi nhưng sẽ thu được các kết quả không bao giờ được sử dụng ở nơi khác trong chương trình. Có các tùy chọn trình biên dịch có thể loại bỏ mã chết, được gọi là *loại bỏ mã chết*, nhưng chúng phải được sử dụng một cách cẩn trọng. Giả sử bạn có một phần mã mà bạn đã đặt cụ thể để thiết lập giá trị bí mật cho tất cả các số 0. Logic sẽ như sau: tạo ra khóa bí mật, sử dụng khóa bí mật, đặt khóa bí mật về 0. Bạn đặt khóa bí mật thành 0 để xóa khóa khỏi bộ nhớ và giữ cho khóa không bị đánh cắp. Nhưng cùng với đó là thói quen loại bỏ mã chết. Nó nhận thấy rằng bạn đang đặt giá trị của

khóa bí mật = 0, nhưng sau đó bạn không bao giờ sử dụng nó nữa. Vì vậy, trình biên dịch, trong việc tối ưu hóa mã của bạn, sẽ loại bỏ bước bảo vệ của bạn.

### **Thực thi và xác minh phía Máy chủ so với Máy khách**

Trong môi trường máy khách/máy chủ hiện đại, dữ liệu có thể được kiểm tra xem có tuân thủ các yêu cầu về đầu vào/đầu ra trên máy chủ hoặc máy khách hay không. Có những lợi thế khi xác minh các phần tử dữ liệu trên máy khách trước khi gửi chúng đến máy chủ - cụ thể ở đây là tính hiệu quả. Việc tiến hành các kiểm tra trên máy khách sẽ lưu một chuyến đi khứ hồi và sự chậm trễ của nó, trước khi người dùng được cảnh báo về sự cố. Điều này có thể cải thiện tính tiện dụng của các giao diện phần mềm.

Máy khách không phải là nơi thích hợp để thực hiện bất kỳ quá trình kiểm tra giá trị hoặc kiểm tra bảo mật quan trọng nào. Những lý do cho điều này là công việc gấp đôi. Đầu tiên, máy khách có thể thay đổi bất kỳ thứ gì sau khi kiểm tra. Thứ hai, dữ liệu có thể bị thay đổi khi đang trong quá trình truyền tải hoặc tại một proxy trung gian. Đối với tất cả các hoạt động kiểm tra cần thiết, vì lý do công việc hoặc vì bảo mật, các bước xác thực nên được thực hiện ở phía máy chủ, nơi dữ liệu không bị thay đổi trái phép. Các kiểm tra xác thực đầu vào chỉ có thể được thực hiện một cách an toàn ở phía máy chủ.



**MÁCH NƯỚC CHO KỲ THI** Tất cả xác thực đầu vào nên được hoàn thành ở phía máy chủ của mỗi quan hệ máy khách-máy chủ, nơi nó không bị ảnh hưởng và thay đổi bởi bên ngoài.

## Quản lý Bộ nhớ

*Quản lý bộ nhớ* cấu thành từ các hành động được sử dụng để kiểm soát và điều phối bộ nhớ máy tính, gán bộ nhớ cho các biến số và thu hồi bộ nhớ khi nó không còn được sử dụng nữa. Các lỗi trong quản lý bộ nhớ có thể dẫn đến một chương trình bị rò rỉ bộ nhớ, và điều này có thể phát triển theo thời gian, tiêu tốn ngày càng nhiều tài nguyên. Thủ tục để dọn dẹp bộ nhớ đã được cấp phát trong một chương trình nhưng không còn cần thiết nữa được gọi là *thu dọn rác*. Trong ngôn ngữ lập trình C và C++, khi không có bộ thu dọn rác tự động, lập trình viên phải cấp phát và giải phóng bộ nhớ một cách rõ ràng. Một trong những ưu điểm của các ngôn ngữ lập trình mới hơn như Java, C#, Python và Ruby là chúng cung cấp khả năng quản lý bộ nhớ tự động với tính năng thu gom rác. Điều này có thể không hiệu quả bằng mã hóa cụ thể trong C, nhưng nó ít bị lỗi hơn một cách đáng kể.

## Sử dụng Bộ Phát triển Phần mềm và Thư viện Bên-thứ-ba

Việc lập trình ngày nay, ở một mức độ lớn, là một bài tập trong việc sử dụng các *thư-viện-của-bên-thứ-ba* và *bộ công cụ phát triển phần mềm* (SDK). Điều này là bởi vì một khi mã đã được gỡ lỗi và được chứng minh là sẽ hoạt động, việc viết lại nó nói chung không phải là cách sử dụng thời gian có giá trị. Ngoài ra, một số thủ tục tương đối phức tạp, chẳng hạn như mã hóa, có các bộ thư viện đã được kiểm chứng và chứng minh, giúp loại bỏ rất nhiều rủi ro khi lập trình các chức năng này.



## MÁCH NƯỚC CHO KỲ THI

Các nhà phát triển phần mềm sử dụng các bộ chương trình và công cụ phần mềm đã được đóng gói sẵn được gọi là các SDK (software development kit) để tạo ra các ứng dụng cho các nền tảng thị trường cụ thể.

## Phơi nhiễm Dữ liệu

*Phơi nhiễm dữ liệu* là sự mất kiểm soát đối với dữ liệu từ một hệ thống trong quá trình vận hành. Dữ liệu phải được bảo vệ trong quá trình lưu trữ, trong quá trình giao tiếp và thậm chí ngay cả trong quá trình sử dụng. Nhóm lập trình phải lập biểu đồ luồng dữ liệu đi qua hệ thống và đảm bảo nó được bảo vệ khỏi sự phơi nhiễm trong suốt quá trình. Dữ liệu có thể bị mất vào tay các bên trái phép (không đảm bảo tính bảo mật) và nguy hiểm không kém, có thể bị thay đổi bởi một bên trái phép (không đảm bảo tính toàn vẹn).



## MÁCH NƯỚC CHO KỲ THI

Danh sách các phần tử theo các kỹ thuật mã hóa an toàn rất dài và cụ thể trong các mục tiêu của kỳ thi CompTIA Security+. Điều quan trọng là hiểu được những sự khác biệt để bạn có thể nhận ra bối cảnh thích hợp nhất với câu hỏi.

## Dự án Bảo mật Ứng dụng Web Mở (OWASP)

*Dự án Bảo mật Ứng dụng Web Mở (OWASP)* là một tổ chức phi lợi nhuận chuyên về cải thiện bảo mật phần mềm ứng dụng dựa-trên-nền-web. Được biết đến nhiều nhất với danh sách mười lỗ hổng phần mềm hàng đầu liên quan đến các ứng dụng web, OWASP cũng có vô số hướng dẫn hữu ích trên trang web của mình tại địa chỉ [www.owasp.org](http://www.owasp.org). OWASP là một tài nguyên nên được các nhà lập trình ứng dụng web sử dụng một cách tích cực để ngăn chặn các lỗ hổng thường gặp trong các ứng dụng web. Trang web này ([www.owasp.org](http://www.owasp.org)) có rất nhiều tài nguyên để hỗ trợ các nhà phát triển sản xuất các ứng dụng tốt hơn và an toàn hơn.

## Tính đa dạng của Phần mềm

Phần mềm không phải là một sản phẩm đơn lẻ. Có rất nhiều hình thức khác nhau, và chúng có thể được đặc trưng bởi một loạt các yếu tố khác

nhau. Phần mềm có thể được phân loại theo các yếu tố chẵng hạn như nền tảng (máy tính cá nhân, máy chủ, thiết bị di động, thiết bị IoT, đám mây), ngôn ngữ lập trình, giao diện (web, API, nhắn tin, kết nối trực tiếp), mục đích và toàn bộ các yếu tố khác. Người ta có thể nói rằng mỗi dự án cuối cùng sẽ là duy nhất. Tuy nhiên, thực tế rằng việc ai đó có thể chỉ ra lý do tại sao phần mềm của họ khác biệt hoặc đặc biệt không làm giảm đi một thực tế rằng đó là một loạt các hướng dẫn để máy tính hoạt động trên đó, và dựa trên các quyết định thiết kế, quyết định mã hóa và quyết định về môi trường, nó có thể và sẽ có các lỗ hổng bảo mật có khả năng cho phép kẻ tấn công làm những việc mang lại những kết quả không mong muốn. Do đó, tất cả các phần mềm đều cần phải được bảo mật. Việc có được quy trình bảo mật thích hợp như một phần của quy trình phát triển là điều quan trọng để giảm thiểu các lỗ hổng bảo mật và quản lý các vấn đề bảo mật khi chúng được khám phá ra.

Một khía cạnh quan trọng khác của đa dạng phần mềm là vấn đề tránh độc canh. Do nhiều hệ thống trong một doanh nghiệp có các thành phần chung, chẵng hạn như hệ điều hành, các thư viện chính, v.v..., nên sẽ có khả năng là các lỗ hổng phổ biến sẽ gây ảnh hưởng đến nhiều thành phần. Hệ quả của việc các hệ thống phần mềm cùng chia sẻ các lỗ hổng phổ biến là tính nhạy cảm với phần mềm độc hại và các cuộc tấn công khác bằng các phương pháp phổ biến ngày càng tăng. Phương pháp chủ yếu để đánh bại rủi ro mang tính hệ thống này là thông qua sự *đa dạng phần mềm*, có được các thành phần khác nhau với các yếu tố phần mềm khác nhau.

## Các Trình biên dịch

Các *trình biên dịch* lấy các chương trình máy tính được viết bằng một ngôn ngữ và chuyển đổi chúng thành một bộ mã có thể hoạt động trên một thiết lập phần cứng cụ thể. Các trình biên dịch hiện đại có thể lấy

mã phần mềm cấp-cao, bất-khả-tri-nền-tảng và chuyển đổi nó thành mã ngôn ngữ máy thực sự có thể chạy trên một nền tảng nhất định. Trong quá trình thực hiện sự chuyển đổi này, trình biên dịch có thể quản lý các khía cạnh khác nhau của chương trình, chẳng hạn như bộ nhớ, hiệu quả của mã, v.v...

## Mã nhị phân

Cuối cùng thì, tất cả các hệ thống máy tính kỹ thuật số đều là những cỗ máy nhị phân. Máy nhị phân hoạt động ở một trong hai trạng thái: bật (1) hoặc tắt (0). Việc nhóm các tín hiệu này (các số 1 và số 0) lại với nhau thành các từ và các cấu trúc xử lý và bộ nhớ lớn hơn là những gì làm cho máy tính có khả năng thực hiện công việc của chúng. Nhưng một khía cạnh thú vị của tất cả những điều này là khả năng sinh sôi. Hai máy tính giống hệt nhau có thể chạy cùng một thứ gì đó, các tín hiệu và cấu trúc bộ nhớ sẽ giống hệt nhau, bởi vì đó là cách máy tính hoạt động. Điều này dẫn đến một hình thức đa dạng quan trọng khác: ngẫu nhiên hóa. Mặc dù tất cả bộ nhớ máy tính là tập hợp các số 1 và 0, nhưng cách các tín hiệu này được sắp xếp đều có ý nghĩa. Việc có hai máy, hoặc nhiều hơn, với bộ nhớ hoàn toàn giống hệt nhau lại cung cấp cho những kẻ tấn công một mục tiêu có khả năng sinh sôi. Điều này đã dẫn đến các biện pháp phòng thủ bao gồm bộ nhớ ngẫu nhiên, trong đó hình mẫu là cụ thể cho mỗi lần khởi động của máy và chỉ máy mới biết.

*Đa dạng nhị phân* là việc tạo ra các ảnh nhị phân hoạt động giống hệt nhau, nhưng với các cách diễn đạt cụ thể khác nhau. Các vị trí khác nhau cho các biến bộ nhớ, các hiệu số con trỏ khác nhau và các bộ trí khác nhau trong bộ nhớ máy tính đều có thể được thực hiện ngày nay mà vẫn bảo toàn hoàn toàn chức năng. Kiểu phòng thủ này khiến kẻ tấn công khó

vượt qua các biện pháp kiểm soát và đưa thứ gì đó vào bộ nhớ một cách trực tiếp.



**LƯU Ý** Khi đưa tính đa dạng nhị phân đến cực điểm, người ta có thể chạy một tập hợp các biến thể đồng thời trong môi trường thực thi đa biến (multivariant execution environment - MVEE). Sau đó, hệ thống thống nhất các đầu vào/đầu ra và giám sát các hoạt động, cho phép phát hiện khi nào các biến thể sẽ khác nhau về hành vi. Điều này chỉ ra những hành vi bất thường và cho phép hệ thống ứng phó và phục hồi từ luồng kết quả xấu.

### Tự động hóa/Tập lệnh theo kịch bản

Tự động hóa thông qua kịch bản và các phương tiện có thể lập trình khác có tính tiện ích rất lớn trong phát triển phần mềm. Việc sử dụng các phương pháp được-hỗ-trợ-bởi-công-nghệ này đã dẫn đến một lĩnh vực phát triển [phần mềm] được gọi là DevOps. DevOps là sự kết hợp giữa phát triển và vận hành - nói cách khác, là sự kết hợp các nhiệm vụ được thực hiện bởi các nhóm vận hành hệ thống và phát triển ứng dụng của một công ty. DevOps nhấn mạnh sự giao tiếp và cộng tác giữa các chuyên gia quản lý sản phẩm, phát triển phần mềm và vận hành để tạo điều kiện phát triển liên tục, tích hợp liên tục, phân phối liên tục và quy trình giám sát liên tục. DevOps có thể được coi là mô hình chống-lại-thác-nước bởi vì thay vì đi từ giai đoạn này sang giai đoạn khác, trong DevOps, khi những thay đổi nhỏ sẵn sàng để xảy ra, chúng sẽ xảy ra. Điều này dẫn đến nhiều thay đổi nhỏ gia tăng dần nhưng thời gian giữa các lần cập nhật sẽ ít hơn và cần ít thời gian hơn để sửa chữa hoặc thay đổi mới thứ. Bảo mật DevOps là việc bổ sung các bước bảo mật vào quy trình DevOps. Cũng giống như bạn có thể thêm các bước bảo mật vào mô hình thác nước

hoặc bất kỳ mô hình phát triển phần mềm nào khác, bạn cũng có thể thêm chúng vào DevOps, dẫn đến kết quả là DevOps được bảo mật.

### **Chuỗi Hành động được Tự động hóa**

Một trong những yếu tố quan trọng của DevOps là tự động hóa. DevOps dựa vào tự động hóa để đạt được nhiều hiệu quả. *Tự động hóa bảo mật* có thể thực hiện điều tương tự đối với bảo mật mà tự động hóa có trong DevOps. Việc tự động hóa các thủ tục và quy trình mở rộng cho phép cần ít tài nguyên hơn để bao phủ nhiều môi trường hơn theo cách hiệu quả và hiệu suất hơn. Tự động hóa loại bỏ chi phí lao động thủ công, đặc biệt là đối với nhân viên an ninh mạng có tay nghề cao. Thay vì thay thế nhân sự bằng các tập lệnh kịch bản, việc sử dụng tự động hóa cho phép nhân viên dành thời gian của họ để thực hiện công việc phân tích mang lại giá-trị-gia-tăng.



**MÁCH NƯỚC CHO KỲ THI** Các tác động của giám sát/xác nhận/tích hợp/cung cấp/triển khai liên tục có thể sẽ phụ thuộc vào chi tiết của câu hỏi, bối cảnh và câu hỏi cụ thể đang được hỏi. Để xác định khía cạnh nào là đúng, cần phải kiểm tra cẩn thận ngữ cảnh của câu hỏi. Hãy tìm hiểu sự khác biệt, không chỉ bối cảnh của “liên tục”.

### **Giám sát Liên tục**

*Giám sát liên tục* là thuật ngữ được sử dụng để mô tả các công nghệ và quy trình được sử dụng để cho phép phát hiện nhanh chóng các vấn đề về tuân thủ và rủi ro bảo mật. Không chỉ là một từ thông dụng, giám sát liên tục là một trong những công cụ quan trọng nhất hiện có để quản lý rủi ro. Tự động hóa và các tập lệnh kịch bản thường được sử dụng như một phần của khuôn khổ giám sát liên tục, vì chúng có thể cung cấp khả năng giám sát 24/7/365 các quy trình và điều kiện, đưa cảnh báo vào hệ

thống giám sát của tổ chức để được xem xét và hành động bởi nhân viên an ninh.

### **Xác minh Liên tục**

*Xác minh liên tục* là phần mở rộng của kiểm nghiệm để hỗ trợ cho quá trình phát triển phần mềm liên tục diễn ra trong DevOps. Khi mã phần mềm được thay đổi trong quy trình DevOps, mã mới phải được kiểm tra với cơ sở mã hiện có để đảm bảo về mặt chức năng và tính ổn định. Việc khiến cho quá trình này trở thành một phần của quá trình phát triển liên tục là điều cần thiết để giữ cho sự phát triển đi đúng quỹ đạo một cách kịp thời.

### **Tích hợp Liên tục**

*Tích hợp liên tục* là cách mà DevOps liên tục cập nhật và cải tiến cơ sở mã phần mềm sản xuất. Bằng cách sử dụng mức độ tự động hóa cao và mạng lưới an toàn của các quy trình dự phòng tự động, tích hợp liên tục cho phép kiểm tra và cập nhật ngay cả những thay đổi nhỏ mà không cần tốn nhiều chi phí. Điều này có nghĩa là thay vì một số bản cập nhật lớn, với nhiều phần tử cập nhật đa-mục-đích được tích hợp và nhiều tiềm năng - tất cả đều nằm gọn trong một gói lớn duy nhất, một loạt các tích hợp đơn-mục-đích nhỏ hơn sẽ được chạy. Do đó, khi thử nghiệm, bạn đã tách biệt các thay đổi thành một lượng nhỏ [thay đổi] có thể quản lý được, mà không cần đến ý nghĩa của nhiều tương tác tiềm năng. Điều này làm giảm các lỗi tương tác và các loại lỗi khác tiêu-tốn-nhiều-thời-gian để theo đuổi.

### **Cung cấp Liên tục**

*Cung cấp liên tục* là một phần mở rộng tự nhiên của tích hợp liên tục để bạn có thể phát hành những thay đổi mới một cách nhanh chóng cho sản xuất theo cách bền vững. Cung cấp liên tục dựa vào kiểm tra được tự động hóa và là một quy trình phát hành tự động cho phép phân phối các

bản cập nhật khi chúng hoàn tất, bất kỳ lúc nào, trái ngược với lịch phát hành cố định. Khi mã đã sẵn sàng để đưa vào [môi trường] sản xuất, việc cung cấp liên tục là quá trình tự động hóa của bước đó, nhưng vẫn nằm dưới sự kiểm soát của nhân viên vận hành cụ thể.

### Triển khai Liên tục

*Triển khai liên tục* là việc cung cấp liên tục theo chế độ thử nghiệm tự động. Nó tiến xa hơn một bước so với cung cấp liên tục ở chỗ việc phát hành là tự động. Với phương pháp này, mọi thay đổi vượt qua tất cả các giai đoạn trong đường ống sản xuất của bạn sẽ được phát hành vào [môi trường] sản xuất. Không có sự can thiệp của con người và khi tất cả các cửa được đáp ứng (nghĩa là, không có những thử nghiệm thất bại), việc triển khai liên tục sẽ tự động gửi mã đến [môi trường] sản xuất.



### MÁCH NƯỚC CHO KỲ THI

Phát triển liên tục tiến một bước xa hơn cung cấp liên tục – mọi thay đổi vượt qua được tất cả các giai đoạn của đường ống sản xuất của bạn được phát hành cho khách hàng một cách hoàn toàn tự động.

### Tính đàn hồi

*Tính đàn hồi* là đặc tính cho thấy một điều gì đó có khả năng thay đổi mà không bị phá vỡ. Một trong những điểm mạnh của điện toán đám mây là tính đàn hồi của nó. Người ta có thể bổ sung thêm hoặc loại bỏ tài nguyên vào hoặc từ môi trường đám mây gần như hoàn toàn tự động mà không gặp phải vấn đề gì. Tính đàn hồi trong phần mềm hoạt động theo cách thức tương tự - phần mềm có khả năng phục hồi như thế nào đối với những thay đổi trong môi trường của nó trong khi vẫn giữ được tính bảo mật. Để phần mềm có thể có tính đàn hồi, nó cần phải có khả năng hoạt động trong nhiều điều kiện khác nhau. Phần mềm kế thừa hoạt động

trong một luồng duy nhất, mặc dù dễ viết hơn, nhưng không có tính đàm hồi. Khi phần mềm đơn-luồng được sử dụng trong môi trường gồm các máy ảo, nhiều bộ xử lý và các môi trường đám mây, hiệu suất của nó bị giới hạn ở một luồng duy nhất. Phần mềm đa luồng có thể mở rộng quy mô và thích ứng tốt hơn, nhưng điều này cũng làm gia tăng độ phức tạp, kéo theo các vấn đề như điều kiện cạnh tranh. Để khả năng mở rộng trở nên ổn định và bền vững, phần mềm cần phải có tính đàm hồi.

### **Khả năng mở rộng**

*Khả năng mở rộng* là đặc trưng của hệ thống phần mềm để xử lý khôi lượng công việc lớn hơn dựa trên tài nguyên hiện tại của nó (*scale up*) hoặc dựa trên tài nguyên bổ sung (*scale out*) mà không bị gián đoạn. Khả năng mở rộng rất quan trọng trong các hệ thống web, cơ sở dữ liệu, công cụ ứng dụng và hệ thống đám mây. Khôi lượng công việc có thể khác nhau và các hệ thống đám mây/vùng chứa có thể bổ sung thêm năng lực xử lý và lưu trữ, nhưng phần mềm phải có khả năng giải quyết những thay đổi trong môi trường. Mặc dù điều này trông có vẻ hiển nhiên, nhưng điều quan trọng lại nằm trong các chi tiết. Vòng lặp thời gian có thể ảnh hưởng đến khả năng phần mềm chạy trên phần cứng nhanh hơn, vì hệ thống chỉ có thể chạy nhanh nhất bằng với liên kết chậm nhất của nó. Việc mở rộng quy mô cho nhiều máy sẽ dẫn đến các vấn đề về đồng bộ hóa và phối hợp. Tất cả những vấn đề này đều có thể được giải quyết, nhưng điều này phải xảy ra trong quá trình thiết kế và phát triển, không phải sau khi đã chuyển giao.

### **Kiểm soát phiên bản**

Các chương trình được phát triển, phát hành và sử dụng, sau đó những thay đổi là điều cần thiết, để thay đổi chức năng, sửa lỗi hoặc cải thiện hiệu suất. Điều này dẫn đến sự tồn tại nhiều phiên bản của chương trình.

*Kiểm soát phiên bản* cũng đơn giản như theo dõi phiên bản chương trình

nào đang được làm việc, cho dù là trong giai đoạn phát triển, thử nghiệm hay sản xuất. Việc tạo phiên bản có xu hướng sử dụng số nguyên đầu tiên để biểu thị các bản phát hành chính và sử dụng các số sau dấu thập phân để biểu thị những thay đổi nhỏ.

Việc có nhiều phiên bản sẽ tập trung vào vấn đề về quản lý thay đổi. Làm thế nào để một công ty quản lý các phiên bản hiện đang được sử dụng và cách họ làm thế nào để điều phối các thay đổi khi chúng được nhà sản xuất phát hành? Trong xuất bản phần mềm truyền thống, một phiên bản mới yêu cầu một bản cài đặt mới và việc thử nghiệm là khá quan trọng vì mức độ thay đổi có thể rất lớn và gây ra các vấn đề về tính tương thích, chức năng và thậm chí là tính đúng đắn. DevOps đã lật ngược tình thế này bằng cách đưa ra ý tưởng rằng các nhà phát triển và sản xuất làm việc cùng nhau và tạo ra một loạt các bản-phát-hành-vi-mô về bản chất để mọi vấn đề thực tế đều liên quan đến các thay đổi đơn lẻ và không bị sa lầy bởi các tương tác giữa nhiều thay đổi mô-đun.

Bất kể bạn đang xuất bản phần mềm truyền thống hay đang hoạt động trong thế giới DevOps, bạn vẫn cần một quy trình quản lý thay đổi để đảm bảo rằng mọi thay đổi trong quá trình sản xuất đều được cấp phép, kiểm tra một cách đúng đắn và khôi phục lại phiên bản trước đó nếu chúng thất bại, đồng thời bạn phải duy trì tính hiện hành và chính xác của tài liệu.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các khái niệm phát triển, triển khai và tự động hóa ứng dụng một cách an toàn. Chương được mở đầu bằng một cuộc thảo luận về môi trường, bao gồm các yếu tố phát triển, kiểm nghiệm, chia giai đoạn, sản xuất và đảm bảo chất lượng. Sau đó, nó kiểm tra việc cấp phép và hủy cấp phép cũng như quản lý tính toàn vẹn.

Chương này sau đó chuyển sang các kỹ thuật mã hóa an toàn. Chúng bao gồm chuẩn hóa, thủ tục lưu trữ, gây bối rối/ngụy trang, tái sử dụng lại mã phần mềm và mã chết. Phần này bao gồm một cuộc thảo luận về các yếu tố xác thực phía-máy-chủ so với phía-máy-khách và kết thúc với việc quản lý bộ nhớ, sử dụng thư viện của bên-thứ-ba và bộ phát triển phần mềm cũng như mức độ phơi nhiễm của dữ liệu.

Dự án Bảo mật Ứng dụng Web Mở (OWASP) và sự đa dạng phần mềm đã được thảo luận tiếp theo. Trong phần về sự đa dạng của phần mềm, các vấn đề về trình biên dịch và đa dạng nhị phân được đề cập. Sau đó, chương này chuyển sang các vấn đề từ thế giới DevOps hoặc tự động hóa và tập lệnh kịch bản được áp dụng cho phát triển phần mềm. Các chủ đề trong phần này bao gồm tự động hóa chuỗi hành động, giám sát liên tục, xác thực liên tục, tích hợp liên tục, phân phối liên tục và triển khai liên tục.

Chương này kết thúc với việc kiểm tra tính đàn hồi và khả năng mở rộng, tiếp theo sau đó là kiểm soát phiên bản.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Để phát triển phần mềm một cách an toàn nhằm ngăn chặn những kẻ tấn công chèn trực tiếp quá trình tấn công vào bộ nhớ máy tính và thao túng các tiến trình của ứng dụng, người ta nên sử dụng phương pháp nào?

  - A.** Tính đàn hồi
  - B.** Mã chết
  - C.** Chuẩn hóa
  - D.** Đa dạng phần mềm.
2. Những vấn đề trong giai đoạn nào sẽ chắc chắn ngừng quá trình triển khai liên tục nhưng không nhất thiết phải ngừng cung cấp liên tục?

  - A.** Tích hợp liên tục
  - B.** Giám sát liên tục
  - C.** Xác thực liên tục
  - D.** Phát triển liên tục.
3. Tại sao quản lý bộ nhớ lại là điều quan trọng trong phát triển phần mềm?

  - A.** Một chương trình có thể phát triển và tiêu tốn không gian của chương trình khác
  - B.** Bộ nhớ là đắt tiền
  - C.** Bộ nhớ có thể là vấn đề về tốc độ
  - D.** Tất cả đều sai.
4. Khi một chương trình được cài đặt và cần cấp quyền, việc này được gọi là gì?

- A.** Chia giai đoạn
  - B.** Cấp phép
  - C.** Tích hợp liên tục
  - D.** Kiểm soát phiên bản.
- 5.** Những tuyên bố nào dưới đây liên quan đến tính đàn hồi và khả năng mở rộng là đúng?
- A.** Khả năng mở rộng đòi hỏi phải có tính đàn hồi
  - B.** Tính đàn hồi liên quan đến việc cho phép phần mềm sử dụng nhiều bộ xử lý hơn để thực hiện nhiều công việc hơn
  - C.** Tính đàn hồi có nghĩa là được chuẩn bị để tận dụng lợi thế của khả năng mở rộng
  - D.** Tất cả đều đúng.
- 6.** Để bảo vệ phần mềm khỏi kỹ thuật đảo ngược của những kẻ tấn công, các nhà phát triển có thể sử dụng những điều nào dưới đây?
- A.** Mã chết
  - B.** Gây bối rối
  - C.** Đa dạng nhị phân
  - D.** Thủ tục lưu trữ.
- 7.** Để quản lý nhiều bản phát hành khác nhau của phần mềm theo thời gian, tổ chức sử dụng điều gì dưới đây?
- A.** Môi trường chia giai đoạn
  - B.** Các bước cấp phép và hủy cấp phép
  - C.** Kiểm soát phiên bản
  - D.** Tích hợp liên tục
- 8.** Những môi trường nào dưới đây được sử dụng để kiểm tra tính tương thích so với các môi trường được nhắm mục tiêu?
- A.** Sản xuất
  - B.** Kiểm nghiệm

- C. Đảm bảo chất lượng**
- D. Chia giai đoạn.**
- 9.** Thực tế là có rất nhiều phương pháp biểu diễn một đối tượng trong hệ thống máy tính có thể dẫn đến các vấn đề khi so sánh logic lad điều cần thiết. Những gì có thể được sử dụng để đảm bảo độ chính xác của các yếu tố so sánh?
- A. Chuẩn hóa**
- B. Các thủ tục lưu trữ**
- C. Các thư viện bên-thứ-ba**
- D. Các bộ công cụ phát triển phần mềm bên-thứ-ba.**
- 10.** Phương pháp chắc chắn duy nhất để đảm bảo đầu vào được xác thực trước khi sử dụng trên một máy chủ là gì?
- A. Sử dụng các thư viện và bộ công cụ phát triển phần mềm bên-thứ-ba**
- B. Xác thực phía-máy-chủ**
- C. Các thủ tục lưu trữ**
- D. Xác thực phía-máy-khách.**

## Đáp án

1. **D.** Đa dạng phần mềm dưới hình thức đa dạng nhị phân sẽ ngăn chặn các cuộc tấn công trực tiếp vào bộ nhớ chống lại các cấu trúc phần mềm đã được biết đến.
2. **C.** Xác thực liên tục là bắt buộc để đảm bảo phần mềm không-có-lỗi, và các lỗi sẽ ngừng việc phát triển liên tục.
3. **A.** Thất bại trong quản lý bộ nhớ có thể dẫn đến việc một chương trình gia tăng kích cỡ khi thực thi. Điều này có thể dẫn đến lỗi của riêng nó hoặc làm giảm tài nguyên bộ nhớ dành cho các chương trình khác.
4. **B.** Cấp phép là chỉ định quyền hạn hoặc thẩm quyền cho các đối tượng.
5. **D.** Tất cả các đáp án trên đều là câu trả lời đúng. Khả năng mở rộng đòi hỏi tính đàn hồi đối với quy mô, tính đàn hồi liên quan đến việc cho phép phần mềm sử dụng nhiều bộ xử lý hơn để thực hiện nhiều công việc hơn và tính đàn hồi có nghĩa là phát triển phần mềm được chuẩn bị để tận dụng khả năng mở rộng.
6. **B.** Gây bối rối là kỹ thuật che giấu các thuộc tính để ngăn chặn việc xem xét. Việc khiến cho mã phần mềm khó biên dịch ngược và không lưu trữ bất kỳ manh mối cụ thể nào trong mã nguồn có thể làm cho kỹ thuật đảo ngược trở thành một thách thức.
7. **C.** Kiểm soát phiên bản bao gồm các quy trình và thủ tục được sử dụng để quản lý các bản phát hành phần mềm khác nhau theo thời gian.
8. **D.** Môi trường chia giai đoạn có thể được sử dụng để quản lý các bản phát hành phần mềm so với các đích nhắm mục tiêu khác nhau để đảm bảo tính tương thích.
9. **A.** Chuẩn hóa là quá trình giảm các mục đến một dạng tiêu chuẩn trước khi so sánh để đảm bảo khớp logic phù hợp.

**10. B.** Xác thực phía-máy-chủ là phương pháp xác thực chắc chắn duy nhất cho các đầu vào đối với ứng dụng.

## Chương 12 Xác thực và Cấp phép

### Xác thực và Cấp phép

Trong chương này bạn sẽ

- Tìm hiểu cách xác định và triển khai các phương pháp xác thực, bao gồm các yếu tố và thuộc tính
- Tìm hiểu về các khái niệm và yêu cầu thiết kế sự cấp phép.

Một trong những nguyên lý cốt lõi của bảo mật máy tính là khái niệm rằng tất cả mọi hành động sẽ được kiểm soát thông qua một hệ thống phê duyệt, ví dụ, chỉ có những bên được cấp phép mới có thể thực hiện những hành động truy cập đến một tài nguyên, vận hành trên một tài nguyên, và lưu trữ một mục. Các hệ thống quản lý nhân dạng và quản lý truy cập là những cơ chế mà theo đó, điều này được thực hiện. Chương này xem xét những thành phần nền tảng đứng sau các hệ thống xác thực.

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 2.4 của kỳ thi CompTIA Security+: Tóm tắt những khái niệm thiết kế xác thực và cấp phép.

#### Các Phương pháp Xác thực

*Xác thực* là quá trình xác minh một nhân dạng đã được xác lập trước đó trong một hệ thống máy tính. Có rất nhiều phương pháp khác nhau để thực hiện chức năng này, mỗi phương pháp có những ưu điểm và nhược điểm riêng của nó, như được thảo luận chi tiết trong các phần sau đây.

## Các Dịch vụ Danh bạ

Một *danh bạ* là một cơ chế lưu trữ dữ liệu tương tự như với một cơ sở dữ liệu, nhưng nó có một số điểm khác biệt được thiết kế để cung cấp các dịch vụ truy-xuất-dữ-liệu hiệu quả so với các cơ chế cơ sở dữ liệu tiêu chuẩn. Một danh bạ được thiết kế và tối ưu hóa để việc đọc dữ liệu, cung cấp các hoạt động tìm kiếm và truy xuất cực kỳ nhanh chóng. Các loại thông tin được lưu trữ trong một danh bạ có xu hướng là dữ liệu thuộc tính mô tả. Danh bạ cung cấp chế độ xem tinh về dữ liệu có thể được thay đổi mà không cần giao dịch cập nhật phức tạp. Dữ liệu được mô tả phân cấp theo cấu trúc giống nhau và một giao diện mạng để đọc là điển hình. Các sử dụng phổ biến của thư mục bao gồm danh sách địa chỉ email, dữ liệu máy chủ miền và bản đồ tài nguyên của tài nguyên mạng. *Giao thức Truy cập Danh bạ Hạng nhẹ* (Lightweight Directory Access Protocol - LDAP) thường được sử dụng để xử lý quá trình xác thực và ủy quyền người dùng và kiểm soát quyền truy cập vào các đối tượng Active Directory (AD).

Để hỗ trợ cho khả năng tương tác, X.500 đã được tạo ra như một tiêu chuẩn dành cho các dịch vụ danh bạ. Phương pháp chính để truy cập một danh bạ X.500 là thông qua Giao thức Truy cập Danh bạ (Directory Access Protocol - DAP), một giao thức hạng nặng rất khó triển khai một cách hoàn toàn, đặc biệt là trên máy tính để bàn và các nền tảng hạn chế hơn. Kết quả đã dẫn đến LDAP, vốn có chức năng được sử dụng phổ biến nhất. LDAP có thể tương tác với các dịch vụ X.500 và quan trọng nhất là có thể được sử dụng qua TCP với nguồn tài nguyên máy tính ít hơn một cách đáng kể so với việc triển khai X.500 đầy đủ. LDAP cung cấp mọi chức năng mà hầu hết các danh bạ cần và dễ dàng và tiết kiệm hơn để triển khai, do đó, LDAP đã trở thành tiêu chuẩn Internet cho các dịch vụ danh bạ. Các tiêu chuẩn LDAP được quản lý bởi hai thực thể riêng biệt, tùy thuộc vào việc sử dụng: Liên minh Viễn thông Quốc tế (International

Telecommunication Union - ITU) quản lý tiêu chuẩn X.500 và LDAP được điều chỉnh cho việc sử dụng Internet bởi Lực lượng Đặc nhiệm Kỹ thuật Internet (Internet Engineering Task Force - IETF). Rất nhiều RFC áp dụng cho chức năng LDAP, nhưng một vài trong số RFC quan trọng nhất là RFC 4510 đến 4519.

Khi tích hợp với các hệ thống dựa-trên-đám-mây, bạn có thể thấy sẽ gặp khó khăn trong việc quản lý thông tin đăng nhập trên hai miền khác nhau. Các nhà cung cấp khác nhau đã sáng tạo ra những công nghệ dựa-trên-danh-bạ để giải quyết vấn đề này, chẳng hạn như AWS Directory Service dành cho Microsoft Active Directory, còn được gọi là AWS Managed Microsoft AD. Dịch vụ này cho phép tải trọng công việc nhận-biết-danh-bạ và tài nguyên AWS của bạn sử dụng Active Directory được quản lý trong Đám mây AWS. Vì AWS Managed Microsoft AD được xây dựng dựa trên Microsoft Active Directory thực tế, bạn có thể sử dụng các công cụ quản trị Active Directory tiêu chuẩn và tận dụng các tính năng Active Directory tích hợp sẵn, chẳng hạn như Group Policy và các tính năng đăng nhập một lần (SSO).



**MÁCH NƯỚC CHO KỲ THI** Một máy khách bắt đầu một phiên LDAP bằng cách kết nối tới một máy chủ LDAP, được gọi là Directory System Agent (DSA), theo mặc định trên cổng TCP và UDP 389 hoặc trên cổng 636 đối với LDAPS (LDAP qua SSL).

### Liên kết

*Liên kết*, hoặc *liên kết danh tính*, xác định các chính sách, giao thức và thực tiễn để quản lý danh tính trên các hệ thống và tổ chức. Mục tiêu cuối cùng của việc liên kết là cho phép người dùng truy cập liền mạch vào dữ liệu hoặc hệ thống trên các miền. Liên kết được kích hoạt thông

qua việc sử dụng các tiêu chuẩn ngành như Ngôn ngữ Đánh dấu Xác nhận Bảo mật (Security Assertion Markup Language - SAML), được thảo luận trong Chương 24, "Triển khai Xác thực và Cấp phép".



**MÁCH NƯỚC CHO KỲ THI** Các hệ thống quản lý truy cập danh tính đã được liên kết cho phép người dùng xác thực và truy cập vào nguồn tài nguyên trên nhiều doanh nghiệp bằng cách sử dụng một thông tin xác thực duy nhất. Tuy nhiên, đừng nhầm điều này với đăng nhập một lần (SSO), vốn cho phép người dùng truy cập vào nhiều nguồn tài nguyên trong một tổ chức hoặc doanh nghiệp duy nhất.

### **Chứng thực**

*Chứng thực* là việc cung cấp chứng cứ hoặc bằng chứng về một số điều thực tế. Đối với trường hợp xác thực, việc chứng thực có thể được thực hiện bởi một dịch vụ kiểm tra thông tin đăng nhập được nhập vào và nếu chúng chính xác và khớp với các giá trị cần thiết, dịch vụ có thể chứng thực rằng thông tin đã nhập là hợp lệ hoặc chính xác. Chứng thực được sử dụng trong toàn bộ an ninh mạng bất cứ khi nào bên thứ ba hoặc một thực thể xác minh một đối tượng là hợp lệ hoặc một hạng mục là đúng về giá trị.

### **Công nghệ**

Có rất nhiều cách để thực hiện việc xác thực, và rất nhiều công nghệ có thể được sử dụng để hỗ trợ cho những nỗ lực này.

### **Mật khẩu Một-Lần theo-Thời-gian (Time-based One-Time Password – TOTP)**

Thuật toán *Mật khẩu Một-Lần theo-Thời-gian (TOTP)* là một triển khai cụ thể của một HOTP (sẽ được thảo luận ngay sau đây) sử dụng một khóa

bí mật với dấu thời gian hiện hành để tạo ra một mật khẩu một-lần (OTP). Nó được mô tả trong RFC 6238 (tháng Năm năm 2011).

## **Mật khẩu Một-Lần theo-HMAC (HMAC-based One-Time Password – HOTP)**

*Mật khẩu Một-Lần theo-HMAC* là một thuật toán có thể được sử dụng để để xác thực một người dùng trong một hệ thống bằng cách sử dụng một máy chủ xác thực (HMAC là viết tắt của mã xác thực thông điệp theo-hàm-băm - hash-based message authentication code). Nó được định nghĩa trong RFC 4226 (tháng Mười hai năm 2005).



**MÁCH NƯỚC CHO KỲ THI** Các mật khẩu HOTP có thể vẫn có hiệu lực và hoạt động trong một khoảng thời gian chưa xác định. Các mật khẩu TOTP được xem là bảo mật hơn bởi vì chúng chỉ có hiệu lực trong một khoảng thời gian ngắn và thường xuyên thay đổi.

## **Dịch vụ Tin nhắn Ngắn (Short Message Service – SMS)**

Việc sử dụng *Dịch vụ Tin nhắn Ngắn (SMS)*, hoặc tin nhắn văn bản, trên một điện thoại di động cung cấp một yếu tố xác thực thứ hai được gửi đến cho một số [điện thoại] đã được xác định trước. Tin nhắn đã được gửi cung cấp một mã số mà người dùng sẽ nhập vào hệ thống. Mã thường sẽ có hiệu lực trong một khoảng thời gian, như được minh họa trong Hình 12-1. Đây là một cách xác minh rằng thông tin đăng nhập đầu tiên, thường là một mật khẩu, đã được nhập bởi cá nhân đã định – giả định rằng họ có quyền kiểm soát điện thoại di động. Đây là một ví dụ thực tế về xác thực đa yếu tố, sẽ được thảo luận sau trong chương này.



**Hình 12-1** Ví dụ về mã xác thực SMS

### **Khóa Token**

*Khóa token* là những thiết bị vật lý chứa một bộ mã thông báo kỹ thuật số được sử dụng để nhận diện một người dùng. Đây là phần tử “thứ gì đó bạn đang có” trong một lược đồ xác thực đa yếu tố. Hình thức của token thực tế có thể thay đổi từ thẻ thông minh, bàn phím fob [*chưa biết là gì*], cho đến một thiết bị USB. Thẻ lân cận (proximity card) được sử dụng trong hệ thống truy cập vật lý là thiết bị mang-mã-thông-báo.

Như trong tất cả các yếu tố “thứ gì đó bạn đang có”, mã thông báo là bằng chứng về loại sự kiện sở hữu và để ngăn việc sử dụng chúng nếu bị mất, chúng được hỗ trợ bằng mã PIN. Các mã thông báo khác nhau có thể mang các dạng khóa khác nhau. Các khóa có thể là động, thay đổi theo thời gian hoặc tĩnh. Mã thông báo động tăng cường bảo mật trong đó giá trị thay đổi theo thời gian và không thể bị ghi nhận và phát lại. Ví dụ về mã thông báo thương mại được hiển thị trong Hình 12-2.



**Hình 12-2** Bộ xác thực token của Blizzard Entertainment

## Mã Tĩnh

*Mã tĩnh* đúng như tên gọi của nó - mã không thay đổi hoặc có bản chất tĩnh. Có rất nhiều trường hợp sử dụng mà mã tĩnh này điều này là cần thiết, chẳng hạn như các thiết bị không có sự can thiệp của người dùng. Các thiết bị không có sự can thiệp của người dùng được triển khai một cách rộng rãi trong rất nhiều hệ thống. Một ví dụ sẽ là đồng hồ đo điện thông minh, một thiết bị cần giao tiếp với các hệ thống khác và xác thực danh tính của nó. Việc sử dụng mã tĩnh có một điểm yếu là nếu bị xâm nhập, các khóa sẽ không còn hiệu lực. Tiêu chuẩn là sử dụng bảo vệ bằng mật mã đối với tất cả quá trình truyền các mã tĩnh, khiến cho mã trở nên không thể đọc được ngay cả khi dữ liệu kênh liên lạc bị sao chép lại.

## Các Ứng dụng Xác thực

Bạn cần một yếu tố thứ hai để xác thực? Chúng tôi có một ứng dụng cho việc đó. Đây không chỉ là một trò đùa, mà là một phương pháp xác thực ngày càng phổ biến hoạt động bằng cách xác minh rằng một người dùng có một thiết bị di động nhất định mà họ đang sở hữu. *Ứng dụng xác thực* hoạt động bằng cách chấp nhận thông tin nhập vào của người dùng, và nếu thông tin người dùng nhập là chính xác, ứng dụng đó có thể chuyển thông tin đăng nhập thích hợp đến hệ thống yêu cầu xác thực. Điều này

có thể ở dạng giá trị kỹ thuật số được lưu trữ hoặc mã dùng một-lần để đáp ứng một thử thách. Các ứng dụng xác thực tồn tại trên nhiều nền tảng - từ Android đến iOS, Linux và Windows - và có rất nhiều nhà cung cấp cho mỗi nền tảng. Việc sử dụng ứng dụng trên thiết bị là yếu tố xác thực thứ hai và là một phần của lược đồ xác thực đa yếu tố.

### **Thông báo Đẩy (Push Notification)**

Xác thực *thông báo đẩy* hỗ trợ xác thực người dùng bằng cách đẩy thông báo trực tiếp đến một ứng dụng trên thiết bị của người dùng. Người dùng nhận được cảnh báo rằng một nỗ lực xác thực đang diễn ra và họ có thể phê duyệt hoặc từ chối quyền truy cập thông qua giao diện người dùng trên ứng dụng. Bản thân thông báo đẩy không phải là một bí mật, nó chỉ là một phương tiện mà người dùng có thể xác thực và phê duyệt quyền truy cập. Đây là một giao tiếp ngoài-băng-tần và biểu thị cho một kênh giao tiếp thứ hai, do đó, khiến cho việc tấn công tài khoản trở nên khó khăn hơn một cách đáng kể.

### **Gọi Điện thoại**

Một hình thức khác của xác thực người dùng có một tương tác với hệ thống thông qua một cuộc gọi điện thoại. *Cuộc gọi điện thoại* xác thực được gửi từ một hệ thống xác thực đến một số điện thoại được chỉ định, để sau đó có thể xác minh rằng người dùng đang sở hữu thiết bị di động thực sự.



**MÁCH NƯỚC CHO KỲ THI** Token đại diện cho điều gì đó bạn có liên quan đến xác thực cũng như các thiết bị có thể lưu trữ nhiều thông tin hơn những gì mà người dùng có thể ghi nhớ, điều này khiến cho chúng trở nên rất có giá trị trong kiểm soát truy cập. Các chi tiết trong tình

huống đứng trước một câu hỏi sẽ cung cấp các tiêu chí cần thiết để chọn phương pháp mã thông báo tốt nhất cho câu hỏi.

### Xác thực Thẻ Thông minh

*Thẻ thông minh* (còn được gọi là *thẻ mạch được tích hợp [ICC]* hoặc *thẻ chip*) là một thẻ có kích-thước-bằng thẻ tín dụng với các mạch tích hợp đã nhúng được sử dụng để cung cấp xác thực bảo mật nhận dạng. Thẻ thông minh có thể tăng cường bảo mật vật lý vì chúng có thể mang theo các mã thông báo mã hóa quá dài để nhớ và không gian quá lớn để đoán. Ngoài ra, do cách thức thẻ thông minh được sử dụng và hoạt động, việc sao chép số không phải là một lựa chọn có tính thực tế. Thẻ thông minh có thể được sử dụng trong nhiều tình huống khác khi mà bạn muốn kết hợp thứ mà bạn đã biết (một mã PIN hoặc mật khẩu) với thứ gì đó bạn đang có (và không thể bị nhân bản, chẳng hạn như một thẻ thông minh). Nhiều máy tính xách tay kiểu-công-ty tiêu chuẩn với đầu đọc thẻ thông minh được cài đặt và việc sử dụng chúng được tích hợp vào hệ thống truy cập người dùng Windows.

### Sinh trắc học

Các yếu tố *sinh trắc học* là phép đo các yếu tố sinh học nhất định để nhận diện một cá nhân cụ thể so với những cá nhân khác. Những yếu tố này dựa trên những bộ phận của cơ thể con người là độc đáo. Yếu tố sinh học độc đáo được biết đến nhiều nhất là dấu vân tay. Trong vài năm nay, đầu đọc dấu vân tay đã được sử dụng trên máy tính xách tay và các thiết bị di động khác, trên bàn phím và các thiết bị USB độc-lập.

Tuy nhiên, rất nhiều yếu tố sinh học khác có thể được sử dụng, chẳng hạn như võng mạc hoặc mống mắt của mắt, hình dạng của bàn tay và hình dạng của khuôn mặt. Khi chúng được sử dụng để xác thực, sẽ có một quy trình bao gồm hai-phần: đăng ký và sau đó xác thực. Trong quá trình đăng ký, một máy tính sẽ lấy hình ảnh của yếu tố sinh học và chuyển

nó thành một giá trị bằng số, được gọi là mẫu. Khi người dùng cỗ găng xác thực, tính năng sinh trắc học sẽ được quét bởi đầu đọc và máy tính sẽ tính toán một giá trị theo cùng kiểu với mẫu và sau đó so sánh giá trị số đang được đọc với giá trị được lưu trữ trong cơ sở dữ liệu. Nếu chúng khớp nhau, quyền truy cập được cho phép. Vì các yếu tố vật lý này là duy nhất nên về mặt lý thuyết, chỉ có những người được ủy quyền thực sự mới được phép truy cập.

Tuy nhiên, trong thế giới thực, lý thuyết đằng sau sinh trắc học đã bị phá vỡ. Các token với mã kỹ thuật số hoạt động rất tốt vì mọi thứ vẫn nằm trong lĩnh vực kỹ thuật số. Một máy tính kiểm tra mã của bạn - chẳng hạn như 123, với cơ sở dữ liệu, nếu máy tính tìm thấy 123 và số đó có quyền truy cập, máy tính sẽ mở cửa. Tuy nhiên, sinh trắc học lấy một tín hiệu tương tự, chẳng hạn như dấu vân tay hoặc khuôn mặt và cỗ găng số hóa nó, sau đó nó được khớp với các chữ số trong cơ sở dữ liệu. Vấn đề với tín hiệu tương tự là nó có thể không được mã hóa theo cùng một cách chính xác trong hai lần. Ví dụ, nếu bạn đến làm việc với một miếng băng dán ở cổ tay, liệu sinh trắc học dựa-trên-khuôn-mặt sẽ cấp cho bạn quyền truy cập hay từ chối nó? Do điều này, các mẫu phức tạp hơn theo cách có thể có xác suất trùng khớp hoặc đo độ gần gũi.

## Vân tay

Một máy quét *vân tay* đo mẫu vân tay duy nhất của một người và chuyển hình mẫu đó thành giá trị số hoặc mẫu, như đã được thảo luận trong phần trước. Đầu đọc vân tay có thể được cải tiến để đảm bảo rằng mẫu là mẫu sống - một mẫu có máu lưu thông hoặc hoạt động sinh học có thể nhận diện khác - để ngăn chặn việc giả mạo đơn giản với khuôn Play-Doh của bản in. Máy quét vân tay khá rẻ tiền và được sử dụng rộng rãi trong các thiết bị di động. Một trong những thách thức của máy quét vân tay là chúng không hoạt động nếu người dùng đang đeo găng tay (ví dụ, găng

tay y tế) hoặc đã bị mòn dấu vân tay khi lao động chân tay, như nhiều người tham gia vào thương mại sheetrock [*nguyên văn: sheetrock trade - chưa hiểu là gì*] thực hiện thông qua công việc bình thường.

### **Võng mạc**

Máy quét võng mạc kiểm tra các mô hình mạch máu ở phía đáy mắt. Được cho là duy nhất và không thay đổi, *võng mạc* là một yếu tố sinh trắc học có thể phát hiện dễ dàng. Tính năng quét võng mạc không được nhiều người dùng chấp nhận vì nó liên quan đến việc quét tia laser vào bên trong nhãn cầu của người dùng, điều này làm nảy sinh một số vấn đề tâm lý đối với một số người dùng cảnh giác với việc để tia laser quét vào bên trong mắt của họ. Việc phát hiện này yêu cầu người dùng phải ở ngay trước thiết bị để thiết bị hoạt động. Nó cũng đắt hơn vì độ chính xác của máy dò và sự tham gia của tia laser và tầm nhìn của người dùng.

### **Mõng mắt**

Máy quét *mõng mắt* hoạt động theo cách tương tự như máy quét võng mạc ở chỗ nó sử dụng hình ảnh của một phép đo sinh học độc đáo (trong trường hợp này là sắc tố liên quan đến mõng mắt của mắt). Điều này có thể được chụp ảnh và đo từ xa, loại bỏ trở ngại tâm lý khi đặt mắt của một người gần máy quét. Nhược điểm của việc có thể chụp quét mõng mắt ở khoảng cách xa là việc này rất dễ thực hiện mà người đó không biết và thậm chí có thể chế tạo kính áp tròng để bắt chước một mẫu. Ngoài ra còn có một số vấn đề khác liên quan đến tình trạng y tế như mang thai và một số bệnh có thể được phát hiện bằng những thay đổi trong mõng mắt của một người và nếu tiết lộ, sẽ là một hành vi vi phạm quyền riêng tư.

### **Khuôn mặt**

Nhận dạng *khuôn mặt* chủ yếu là công cụ khoa học viễn tưởng cho đến khi nó được tích hợp vào các điện thoại di động khác nhau. Một cảm biến

nhận dạng khi bạn di chuyển điện thoại vào vị trí có thể nhìn thấy khuôn mặt của mình, cùng với trạng thái không đăng nhập, sẽ bật camera hướng-về-phía-trước-mặt, khiến hệ thống tìm kiếm chủ sở hữu đã được đăng ký của nó. Hệ thống này đã được chứng minh là có khả năng phân biệt khá cao và hoạt động khá tốt, và chỉ có một nhược điểm: người khác có thể di chuyển điện thoại trước mặt người dùng đã được đăng ký và nó có thể sẽ mở khóa. Về bản chất, một người dùng khác có thể kích hoạt cơ chế mở khóa mà người dùng không hề hay biết. Một hạn chế nhỏ khác là đối với các giao dịch nhất định, chẳng hạn như nhận dạng tích cực cho các giao dịch tài chính, vị trí của điện thoại trên vị trí NFC, cùng với khuôn mặt của người dùng cần phải ở một hướng nhất định đối với điện thoại, dẫn đến một số vị trí khó xử. Nói cách khác, việc phải đặt khuôn mặt của bạn vào một vị trí thích hợp trên điện thoại để nhận dạng bạn trong khi vẫn giữ điện thoại dựa vào đầu đọc thẻ tín dụng NFC có chiều cao đối diện có thể sẽ gây ra lúng túng.

### **Giọng nói**

Nhận dạng *giọng nói* là việc sử dụng các chất âm đặc đáo và các mẫu giọng nói để nhận diện một người. Từ lâu đã là chủ đề của phim khoa học viễn tưởng, yếu tố sinh trắc học này là một trong những công cụ khó nhất để phát triển thành một cơ chế đáng tin cậy, chủ yếu là do các vấn đề về tỷ lệ chấp nhận sai và tỷ lệ từ chối, sẽ được thảo luận một chút ở phần sau của chương.

### **Tĩnh mạch**

Một yếu tố sinh trắc học khác là sử dụng các mẫu *tĩnh mạch* để nhận diện người dùng. Con người có một hệ thống mạch máu chung, nhưng các phần tử riêng lẻ có thể khác nhau về kích thước và cấu trúc vi mô, và những mô hình hạt-mịn này được cho là duy nhất. Cảm biến có thể đo lường các mẫu này và sử dụng chúng để xác định người dùng. Ba vị trí mô hình

mạch máu phổ biến được sử dụng bao gồm: lòng bàn tay, ngón tay và các tĩnh mạch trong võng mạc. Phép đo này được thực hiện thông qua phân tích quang phổ của mô, sử dụng các tần số phát hiện lượng hemoglobin trong máu. Đây là các phép đo không xâm lấn, nhưng chúng yêu cầu ở gần mẫu vật của người dùng được đo.

### **Phân tích Dáng đi**

*Phân tích dáng đi* là phép đo kiểu dáng được thể hiện bởi một người khi họ bước đi. Việc phân tích dáng đi, chiều dài, tốc độ và tỷ lệ chuyển động của các điểm cụ thể cung cấp một chữ ký duy nhất có thể được ghi lại và so sánh với các mẫu trước đó. Thậm chí ngay cả khi không được sử dụng để xác thực, vì mẫu trước đó được yêu cầu, phân tích dáng đi có thể được sử dụng để xác định nghi phạm trong một nhóm người khác, cho phép theo dõi các cá nhân trong một đám đông. Xét từ góc độ kiểm soát truy cập, trong những tình huống bảo mật cao, một camera có thể ghi lại dáng đi của nhân viên đến và so sánh với các giá trị đã biết, cung cấp yếu tố bổ sung từ xa và sớm để xác định danh tính.

### **Tỷ lệ Hiệu lực**

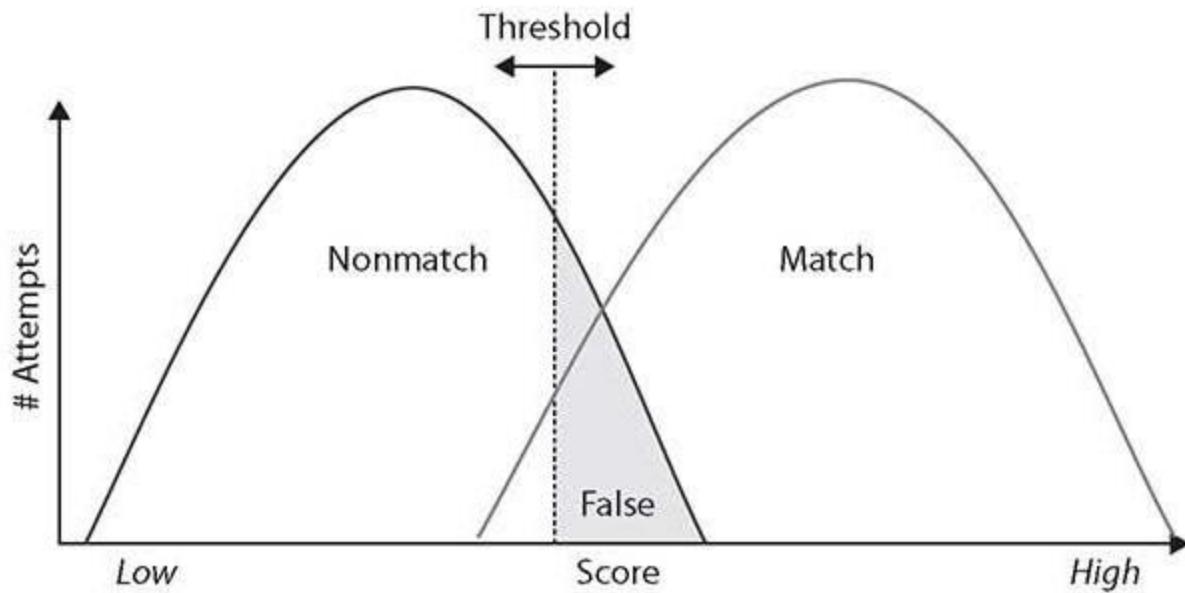
Các phép đo sinh trắc học đều có một mức độ không chắc chắn, và do đó hiệu quả của các giải pháp sinh trắc học đã trở thành một vấn đề kể từ khi chúng được phát triển lần đầu tiên. Khi mỗi thế hệ cảm biến cải thiện độ chính xác của các phép đo, các sai số đã được giảm xuống mức giờ đây thể quản lý được. Để sinh trắc học có hiệu quả, chúng phải có cả tỷ lệ dương tính giả thấp và tỷ lệ âm tính giả thấp. Các thuật ngữ về *tỷ lệ chấp nhận sai* (*false acceptance rate - FAR*) và *tỷ lệ từ chối sai* (*false rejection rate - FRR*) mô tả khả năng một người dùng không hợp lệ sẽ được chấp nhận sai hoặc một người dùng hợp lệ sẽ bị từ chối sai, tương ứng như được đề cập chi tiết trong các phần tiếp theo. Hai thước đo này là khác nhau và trong khi tỷ lệ từ chối sai thấp là quan trọng đối với tính

tiện dụng, thì tỷ lệ chấp nhận sai thấp lại quan trọng hơn xét từ góc độ bảo mật. Người dùng phải lặp lại cỗ gắng xác thực là điều bất tiện, nhưng việc xác thực xảy ra cho người dùng trái phép còn tệ hơn.

Liên minh FIDO, một tổ chức chứng nhận và tiêu chuẩn xác thực hàng đầu, có các thông số kỹ thuật về tỷ lệ lỗi. FRR phải dưới 3% (không quá ba lỗi trong 100 lần thử) và FAR phải dưới 0,01% (không quá một lỗi trong 10.000 lần thử). Như trong tất cả các tình huống phòng-thủ-có-chiều-sâu, backstop là một chức năng khóa, nơi các thiết bị sẽ khóa sau một số lần thử thất bại nhất định. Điều này khiến cho FAR trở nên an toàn hơn chỉ là con số tỷ lệ phần trăm đơn thuần.

### **Chấp thuận Sai**

Tỷ lệ chấp nhận sai (FAR) xác định mức độ dương tính giả được cho phép trong hệ thống. *Chấp thuận sai* (hoặc dương tính giả) được thể hiện bằng vùng màu xám trong Hình 12-3. Trong khu vực này, hai đường cong trùng nhau và quyết định đã được đưa ra rằng trong ngưỡng này (hoặc tốt hơn), một tín hiệu chấp nhận sẽ được đưa ra. Do đó, nếu bạn không phải là đối sánh, nhưng giá trị đo được của bạn nằm ở đầu trên của đường cong không khớp (trong vùng được tô màu xám), bạn sẽ được coi là đối sánh và do đó trở thành dương tính giả. Tỷ lệ chấp nhận sai được biểu thị bằng xác suất hệ thống xác định sai khớp giữa đầu vào sinh trắc học và giá trị mẫu được lưu trữ.



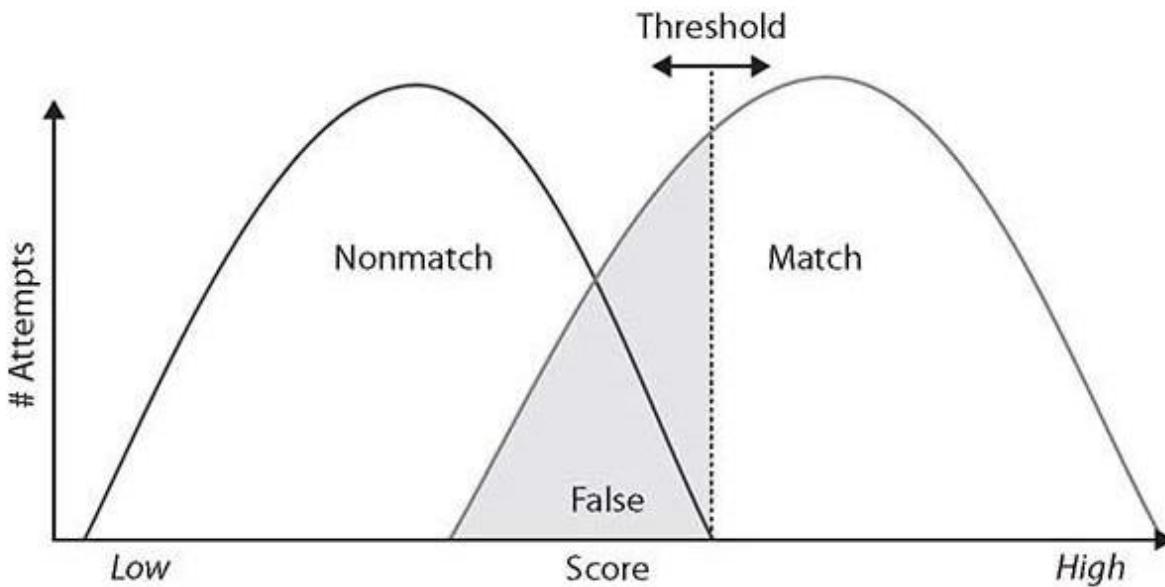
**Hình 12-3** Tỷ lệ chấp thuận sai

Khi chọn giá trị ngưỡng, nhà thiết kế phải nhận thức được hai yếu tố. Một là từ chối mẫu sinh trắc học hợp pháp - khu vực trên đường cong khớp bên dưới giá trị ngưỡng. Thứ hai là sự chấp nhận dương tính giả. Càng nhiều đường cong chồng lên nhau, vẫn đề càng lớn, bởi vì một khi ngưỡng được chọn, con số đó sẽ xác định FAR. Việc đặt ngưỡng cao hơn sẽ làm giảm dương tính giả nhưng tăng âm tính giả hoặc tỷ lệ từ chối. Điều này sẽ làm tăng tỷ lệ từ chối sai, sẽ được thảo luận trong phần tiếp theo.

### Từ chối Sai

Tỷ lệ từ chối sai (FRR) xác định mức độ âm tính giả hoặc từ chối sai sẽ được phép trong hệ thống. Sự từ chối sai được thể hiện bằng vùng tô màu xám trong Hình 12-4. Trong phần này, các đường cong chồng lên nhau và quyết định đã được đưa ra rằng ở ngưỡng này (hoặc thấp hơn), một tín hiệu từ chối sẽ được đưa ra. Vì vậy, nếu bạn đang ở cuối phía dưới của đường cong đối sánh (trong vùng tô màu xám), bạn sẽ bị từ chối, ngay cả khi bạn đã khớp. Tỷ lệ từ chối sai được biểu thị bằng

xác suất hệ thống từ chối sai một đối sánh hợp pháp giữa đầu vào sinh trắc học và giá trị mẫu được lưu trữ.

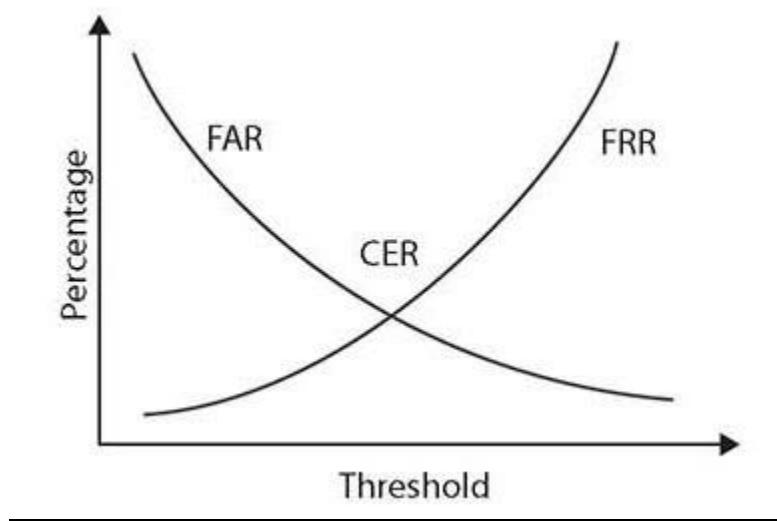


**Hình 12-4** Tỷ lệ từ chối sai

Khi so sánh FAR và FRR, người ta nhận thấy rằng trong hầu hết các trường hợp, bất cứ khi nào các đường cong trùng nhau, chúng đều có liên quan với nhau. Điều này sẽ dẫn đến vấn đề về tỷ lệ lỗi chéo. Cả FAR và FRR đều được thiết lập bằng cách chọn giá trị ngưỡng. Điều này được thực hiện khi hệ thống được thiết lập và phản ánh việc lựa chọn tỷ lệ lỗi nào là quan trọng hơn. Nếu bạn muốn làm cho tỷ lệ dương tính giả khó xảy ra hơn, bạn sẽ gây ra nhiều lần cấp phép thất bại cho những người dùng hợp pháp vì họ sẽ được hệ thống nhìn thấy như đang trên đường cong khác. Nếu bạn muốn đảm bảo tất cả người dùng hợp pháp không gặp sự cố trong quá trình quét, thì một số người dùng trái phép sẽ được chấp nhận (dương tính giả) vì họ sẽ được hệ thống hiểu là đang ở sai đường cong, dựa trên nơi ngưỡng được thiết lập.

## Tỷ lệ Lỗi Chéo

Tỷ lệ lỗi chéo (CER) là tỷ lệ lỗi chấp nhận và từ chối bằng nhau. Đây là trạng thái mong muốn để hoạt động hiệu quả nhất và nó có thể được quản lý bằng cách thao tác giá trị ngưỡng được sử dụng để khớp các mẫu. Trong thực tế, các giá trị có thể không hoàn toàn giống nhau, nhưng chúng thường sẽ gần nhau. Hình 12-5 thể hiện mối quan hệ giữa FAR, FRR và CER.



**Hình 12-5** So sánh FRR, FAR và CER



**MÁCH NƯỚC CHO KỲ THI**

Hãy nhớ rằng tỷ lệ lỗi chéo (CER) là tỷ lệ phần trăm mà tại đó, tỷ lệ chấp thuận sai (FAR) và tỷ lệ từ chối sai (FRR) là bằng nhau.

## Các Yếu tố Xác thực Nhiều lớp (MFA) và các Thuộc tính

Xác thực đa yếu tố (*multifactor authentication*) (hoặc xác thực nhiều yếu tố - *multiple-factor authentication*) chỉ đơn giản là sự kết hợp của hai hoặc nhiều loại xác thực với nhau. Năm thể loại xác thực rộng rãi có thể được sử dụng: bạn là ai (ví dụ, sinh trắc học), bạn có gì (ví dụ, mã thông

báo), bạn biết những gì (mật khẩu và thông tin khác), bạn đang ở đâu (vị trí) và bạn làm gì (hoạt động thể chất). Xác thực hai-yếu-tổ kết hợp bất kỳ hai yếu tố nào trong số này trước khi cấp quyền truy cập. Một ví dụ sẽ là đầu đọc thẻ sau đó bật máy quét vân tay - nếu vân tay của bạn khớp với vân tay trong hồ sơ của thẻ thì bạn sẽ được cấp quyền truy cập. Xác thực ba-yếu-tổ sẽ kết hợp ba loại, chẳng hạn như đầu đọc thẻ thông minh yêu cầu mã PIN trước khi bật máy quét vân tay. Nếu cả ba yếu tố, bao gồm thẻ (vật lý), mã PIN (kiến thức) và quét (sinh trắc học), tương ứng với một người dùng hợp lệ trong cơ sở dữ liệu máy tính thì quyền truy cập sẽ được cấp.



## MÁCH NƯỚC CHO KỲ THI

Xác thực hai-yếu-tổ kết hợp hai trong số bất kỳ phương pháp [xác thực] nào, khớp các mẫu vật chẵng hạn như một token với một sinh trắc học. Xác thực ba-yếu-tổ kết hợp ba trong số các phương pháp [xác thực], chẵng hạn như mã số, sinh trắc học và token.

Các phương pháp xác thực đa yếu tố giúp tăng cường bảo mật đáng kể bằng cách khiến cho những kẻ tấn công rất khó lấy được tất cả các tài liệu chính xác để được xác thực. Chúng [các phương pháp xác thực đa yếu tố] cũng bảo vệ chống lại nguy cơ bị đánh cắp mã thông báo, vì kẻ tấn công phải có sinh trắc học, mật khẩu chính xác hoặc cả hai. Quan trọng hơn, xác thực đa yếu tố nâng cao tính bảo mật của hệ thống sinh trắc học bằng cách bảo vệ chống lại sinh trắc học giả mạo. Sự thay đổi của mã thông báo khiến cho sinh trắc học trở nên vô dụng trừ khi kẻ tấn công có thể đánh cắp được mã thông báo mới. Nó cũng làm giảm dương tính giả bằng cách cố gắng đổi sánh sinh trắc học đã được cung cấp với sinh trắc học được liên kết với mã thông báo đã được cung cấp. Điều này ngăn ngừa việc máy tính tìm kiếm kết quả phù hợp bằng cách sử dụng

toàn bộ cơ sở dữ liệu sinh trắc học. Sử dụng nhiều yếu tố là một trong những cách tốt nhất để đảm bảo xác thực và kiểm soát truy cập thích hợp.

## Các Yếu tố

Các *yếu tố* là những phần tử cụ thể để tạo nên một mục chứng minh. Những mục này có thể được nhóm thành ba lớp: thứ mà bạn biết (mật khẩu), thứ mà bạn có (mã thông báo) và bạn đang là ai (sinh trắc học). Mỗi loại đều có ưu điểm và nhược điểm, như được thảo luận trong các phần tiếp theo.

## Thứ mà bạn biết

Ví dụ phổ biến nhất về *thứ mà bạn biết* là một mật khẩu. Một trong số những thách thức với việc sử dụng “thứ mà bạn biết” như một yếu tố xác thực là rằng nó có thể được “chia sẻ” (hoặc nhân bản) và bạn không hề hay biết. Một mối quan tâm khác với việc sử dụng “thứ mà bạn biết” là rằng bởi vì có rất nhiều yếu tố khác nhau mà người dùng thông thường cần phải nhớ, họ làm những việc để hỗ trợ bộ nhớ [của họ], chẳng hạn như việc lặp lại mật khẩu, thực hiện những thay đổi nhỏ đối với mật khẩu, chẳng hạn như tăng số từ password1 đến password2 và viết chúng ra. Đây là tất cả những phương pháp phổ biến được sử dụng để đối phó với tình trạng mật khẩu lộn xộn, tuy nhiên chúng đều gây ra các lỗ hổng mới.

Một hình thức xác thực khác mà bạn biết là xác thực dựa-trên-danh-tính. Trong xác thực dựa-trên-danh-tính, bạn liên hệ với ai đó để được cấp quyền truy cập và họ phản hồi bằng một loạt các câu hỏi thử thách. Đôi khi các câu hỏi dựa trên thông tin đã được gửi trước đó, và đôi khi các câu hỏi dựa trên những thông tin đã được công bố công khai, chẳng hạn như địa chỉ, số điện thoại, ô tô đã mua/được cấp phép trước đó, v.v... Một lần nữa, người trả lời thích hợp sẽ biết những câu trả lời này, trong khi kẻ mạo danh thì không. Các bài kiểm tra này được tính thời gian, và

nếu người trả lời mất quá nhiều thời gian (ví dụ, dành thời gian để thực hiện tra cứu), họ sẽ thất bại.

## Thứ mà bạn có

*Thứ mà bạn có* đề cập một cách cụ thể đến mã thông báo bảo mật và các vật phẩm khác mà người dùng có thể sở hữu về mặt vật lý. Một trong những thách thức khi sử dụng “thứ mà bạn có” làm yếu tố xác thực là bạn phải mang nó theo bất cứ khi nào bạn muốn được xác thực và điều này có thể gây ra vấn đề. Nó cũng dựa trên các tương tác có thể không sẵn có đối với một số hệ thống, chẳng hạn như thiết bị di động, mặc dù các tương tác, chẳng hạn như trình tạo ra mật-khẩu-một-lần (OTP), là độc lập với thiết bị. Trình tạo OTP tạo ra mật khẩu mới theo yêu cầu, dựa trên một trình tự chỉ được biết bởi trình tạo OTP và phần tử OTP trên hệ thống chấp nhận mật khẩu.

Một trong những thách thức đối với “thứ mà bạn có” là khái niệm “thứ bạn đã đánh mất”, chẳng hạn như những thứ bạn để trong cặp, ở nhà, v.v... Cũng giống như việc bạn để lại vòng chìa khóa cùng với chìa khóa văn phòng của bạn có thể buộc phải quay trở lại nhà để lấy nó, do đó, bạn có thể để lại khóa bảo mật hoặc yếu tố bảo mật khác mà bản chất là “thứ mà bạn có”. Và nếu thứ gì đó bạn có trở thành thứ bạn đã bị đánh cắp thì hệ lụy là khá rõ ràng - bạn không có quyền truy cập và bạn phải xác định lại chính mình để có quyền truy cập trở lại.

## Bạn đang là ai

*Bạn đang là ai* đặc biệt đề cập đến các yếu tố sinh trắc học. Một trong những thách thức với việc sử dụng tạo tác “bạn đang là ai” làm yếu tố xác thực là chúng thường khó thay đổi, một khi đã được chỉ định, chúng hầu như chắc chắn trở nên bất biến, vì bạn có thể thay đổi các ngón tay, nhưng chỉ một số lần giới hạn, và sau đó bạn hết thay đổi. Một thách thức khác với sinh trắc học là có thể tồn tại các vấn đề về văn hóa hoặc

các vấn đề khác liên quan đến việc đo lường những gì mà một người có thể đang có. Ví dụ, mọi người ở một số nền văn hóa phản đối việc chụp ảnh của họ. Một ví dụ khác là những người lao động thể chất trong một số ngành có xu hướng bị thiếu dấu vân tay có thể quét được vì chúng đã bị mòn. Một số yếu tố sinh trắc học không thể sử dụng được trong một số môi trường nhất định, ví dụ, trong trường hợp nhân viên y tế hoặc công nhân làm việc trong môi trường phòng-sạch (clean-room), đồ bảo hộ lao động cá nhân của họ sẽ hạn chế việc sử dụng đầu đọc dấu vân tay và các thiết bị sinh trắc học tiềm năng khác.

## Các Thuộc tính

*Thuộc tính* là tập hợp các tạo tác, giống như các yếu tố đã trình bày trước đó, nhưng thay vì chỉ tập trung vào mục xác thực, chúng sẽ tập trung vào các yếu tố được liên kết với người dùng. Các thuộc tính phổ biến bao gồm vị trí của người dùng, khả năng của họ để thực hiện một nhiệm vụ hoặc điều gì đó về chính bản thân người dùng. Các thuộc tính sẽ này được thảo luận trong những phần sau.

## Bạn đang ở đâu

Một trong những yếu tố xác thực phân biệt đối xử là vị trí của bạn hoặc nơi bạn đang ở. Khi một thiết bị di động được sử dụng, GPS có thể xác định vị trí hiện tại của thiết bị. Khi bạn đăng nhập vào kết nối máy tính để bàn có dây, cục bộ, nó cho thấy bạn đang ở trong tòa nhà. Cả hai điều này có thể được so sánh với hồ sơ để xem liệu bạn có thực sự ở đó hay không ở đó. Nếu bạn bị đánh dấu vào tòa nhà của mình và tại bàn làm việc trên máy tính có dây, thì kết nối thứ hai với một vị trí khác sẽ bị nghi ngờ, vì bạn chỉ có thể ở một nơi tại một thời điểm.

Với cấu trúc địa lý (xem Chương 21, “Giải pháp di động an toàn” để biết thêm chi tiết), vị trí trở thành một điều quan trọng đối với các dịch vụ tiếp thị đẩy nội dung đến các thiết bị khi ở các vị trí cụ thể. Dịch vụ định

vị trên thiết bị di động, cùng với tính năng định vị địa lý, có thể cảnh báo cho người khác khi bạn đang ở trong một khu vực cụ thể — không phải xác thực cụ thể, nhưng dẫn đến khu vực đó.

### **Điều gì đó mà Bạn Có thể Thực hiện**

*Điều gì đó mà bạn có thể thực hiện* đặc biệt đề cập đến một hành động vật lý mà bạn có thể thực hiện một cách duy nhất. Một ví dụ về điều này là một chữ ký, chuyển động của ngón bút và kết quả đầu ra hai-chiều là rất khó để người khác có thể bắt chước được. Điều này khiến cho nó trở nên hữu ích đối với xác thực, nhưng những thách thức vẫn tồn tại trong việc thu thập dữ liệu, vì các bàn chữ ký không phải là các thiết bị ngoại vi phổ biến trên các máy tính. Phân tích đáng đi, đã được trình bày trước đó, là một ví dụ khác của thuộc tính này. Điều gì đó mà bạn có thể thực hiện là một trong những mẫu vật khó nắm bắt hơn nếu không có phần cứng chuyên dụng, khiến nó trở nên ít phổ biến hơn như một phương pháp xác thực.

### **Thứ gì đó mà Bạn Có thể Trưng ra**

*Thứ gì đó mà bạn có thể trưng ra* là một trường hợp đặc biệt của sinh trắc học. Một ví dụ sẽ là phản ứng của sóng não khi nhìn thấy một bức tranh. Một ví dụ khác là kết quả của một bài kiểm tra bằng máy phát hiện nói dối. Khái niệm này là trình bày một yếu tố kích hoạt và đo lường một ứng phó không thể bị làm giả. Khi các cảm biến được cải tiến, việc theo dõi chuyển động của mắt và cảm nhận các khía cạnh khác của phản ứng sẽ trở thành các dạng có thể được sử dụng để hỗ trợ xác thực.

### **Ai đó mà Bạn Biết**

Cũng giống như mật khẩu liên quan đến việc sở hữu kiến thức, *ai đó mà bạn biết* liên quan đến một trí nhớ cụ thể, nhưng trong trường hợp này là một cá nhân. Đây là thuộc tính cổ điển “có ai đó sẽ xác nhận cho bạn”.

Về mặt điện tử, điều này có thể được thực hiện thông qua một chuỗi mô hình tin cậy và nó thường được sử dụng trong quá khứ do kết quả của việc mọi người ký vào khóa của nhau, cho thấy sự tin tưởng.



**MÁCH NƯỚC CHO KỲ THI** Hãy trở nên có khả năng phân biệt giữa ba yếu tố để xác thực (điều gì đó bạn biết, có và bạn là ai) cũng như bốn thuộc tính (bạn đang ở đâu, điều gì đó bạn có thể làm và trưng ra, và người nào đó mà bạn biết). Đây là những điều dễ dàng được kiểm tra trong kỳ thi. Hãy chắc chắn nhận ra được các ví dụ cho từng yếu tố khớp với một câu hỏi dạng-kịch-bản-tình-huống.

### Xác thực, Cấp phép và Tính toán (AAA)

Xác thực là quá trình xác minh và nhận diện được xác lập trước đó trong một hệ thống máy tính. Có một loạt các phương pháp khác nhau để thực hiện chức năng này, mỗi phương pháp có những ưu và nhược điểm khác nhau. Các phương pháp xác thực và những ưu và nhược điểm của chúng đã được mô tả trong toàn bộ chương.

Cấp phép là quá trình cho phép hoặc từ chối quyền truy cập vào một nguồn tài nguyên cụ thể. Khi nhân dạng đã được xác nhận thông qua quá trình xác thực, những hành động cụ thể có thể được cấp phép hoặc bị từ chối. Có rất nhiều kiểu lược đồ cấp phép được sử dụng, nhưng mục đích là như nhau: xác định xem liệu một người dùng nhất định, người đã được xác định là có những quyền hạn đối với một đối tượng hoặc nguồn tài nguyên cụ thể đang được yêu cầu hay không. Chức năng này thường là một phần của hệ điều hành và trong suốt đối với người dùng.

Tính toán là quá trình quy định việc sử dụng tài nguyên bằng cách tính toán nhằm mục đích theo dõi mức sử dụng tài nguyên. Đây là chức năng tính toán cơ bản vẫn đang được sử dụng bởi một số doanh nghiệp.

Việc phân tách các nhiệm vụ, từ nhận dạng đến xác thực đến cấp phép, đều có một số ưu điểm. Rất nhiều phương pháp có thể được sử dụng để thực hiện từng tác vụ, và trên nhiều hệ thống, một số phương pháp đồng thời cho hiện diện từng tác vụ. Việc tách các nhiệm vụ này thành các phần tử riêng lẻ cho phép các tổ hợp triển khai hoạt động cùng với nhau. Bất kỳ hệ thống hoặc tài nguyên nào, có thể là phần cứng (bộ định tuyến hoặc máy trạm) hoặc một thành phần phần mềm (hệ thống cơ sở dữ liệu), đang yêu cầu cấp phép đều có thể sử dụng cấp phép của riêng nó sau khi quá trình xác thực đã xảy ra. Điều này khiến cho việc áp dụng các nguyên tắc này một cách hiệu quả và nhất quán.



**MÁCH NƯỚC CHO KỲ THI** Xác thực là quá trình xác minh một nhân dạng. Cấp phép là quá trình chấp thuận hoặc từ chối quyền truy cập vào các nguồn tài nguyên. Tính toán là quá trình tiếp tục theo dõi các nguồn tài nguyên mà một người dùng đang truy cập. Cùng với nhau, chúng tạo thành khuôn khổ AAA để xác định bảo mật truy cập.

### Các yêu cầu Đám mây so với Tại-chỗ

Xác thực đối với đám mây so với các yêu cầu tại-chỗ về cơ bản là việc kiểm tra lại toàn bộ vấn đề về nhận dạng và xác thực một lần nữa. Khi xác lập hệ thống đám mây hoặc tại-chỗ, bạn sử dụng danh tính và xác thực làm nền tảng cho nỗ lực bảo mật của mình. Cho dù bạn sử dụng phương pháp Active Directory hay hệ thống khác để quản lý danh tính tại-chỗ, khi bạn thiết lập một hệ thống dựa-trên-đám-mây, các tùy chọn cần được đánh giá hoàn toàn và các lựa chọn phù hợp được đưa ra dựa

trên việc sử dụng đám mây trong doanh nghiệp. Các phương pháp đơn giản bao gồm một hệ thống độc lập hoàn toàn mới, mặc dù điều này làm gia tăng chi phí và giảm tính tiện dụng khi số lượng người dùng tăng lên. Các giải pháp như xác thực được liên kết và đăng nhập một lần hiện diện và việc xác định đúng các quy trình xác thực nên dựa vào mức độ quan trọng của dữ liệu và ai cần quyền truy cập.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các khái niệm thiết kế liên quan đến quá trình xác thực và cấp phép. Chương này mở đầu bằng việc kiểm tra các phương pháp xác thực, bao gồm các dịch vụ danh bạ, liên kết, chứng thực và các công nghệ. Các công nghệ mà chúng ta đã kiểm tra bao gồm mật-khẩu-một-lần theo-thời-gian, mật-khẩu-một-lần dựa-trên-HMAC, Dịch vụ Tin nhắn Ngắn, khóa mã thông báo (token), mã tĩnh, các ứng dụng xác thực, thông báo đẩy và cuộc gọi điện thoại. Phần đầu tiên kết thúc với một cuộc thảo luận về xác thực dựa-trên-thẻ thông minh.

Cuộc thảo luận về sinh trắc học bao gồm cả các yếu tố và cách sử dụng. Bạn đã tìm hiểu về một số công nghệ sinh trắc học khác nhau: quét vân tay, quét võng mạc, quét mống mắt, nhận dạng khuôn mặt, nhận dạng giọng nói, mẫu tĩnh mạch và phân tích dáng đi. Các phương pháp và phân tích được đề cập bao gồm tỷ lệ hiệu quả: tỷ lệ chấp nhận sai, tỷ lệ từ chối sai và tỷ lệ lỗi chéo.

Chương được tiếp tục với việc kiểm tra các yếu tố và thuộc tính xác thực đa yếu tố. Ba yếu tố được trình bày là thứ mà bạn biết, thứ mà bạn có và thứ chỉ ra bạn là ai. Bốn thuộc tính tiếp theo: bạn là ai, bạn có thể làm gì, bạn thể hiện điều gì đó và ai đó mà bạn biết. Chương này kết thúc với việc kiểm tra xác thực, cấp phép và tính toán cũng như các yêu cầu về đám mê so với tại chỗ.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Trong một chuyến viếng thăm một trung tâm dữ liệu, nơi tổ chức của bạn đang lưu một số các máy chủ ngoại biên, bạn nhìn thấy một cánh cửa với một bảng điều khiển trông-khá-kỳ-lạ bên cạnh nó. Bạn nhìn thấy mọi người tiếp cận nó và đặt mắt của họ vào trong một đầu đọc có mái che. Một vài giây sau khi họ thực hiện việc này, cánh cửa mở ra. Kiểu máy quét sinh trắc học này có thể là gì?

  - A. Máy quét nhận dạng giọng nói
  - B. Máy quét võng mạc
  - C. Máy quét vân tay
  - D. Máy quét nhận dạng khuôn mặt.
2. Bạn đã dành tuần trước để điều chỉnh giải pháp quét-vân-tay cho tổ chức của mình. Bất chấp những nỗ lực hết mình của bạn, khoảng 1 trong 50 lần thử sẽ thất bại, ngay cả khi người dùng đang sử dụng đúng ngón tay và dấu vân tay của họ đang có trong hệ thống. Người giám sát của bạn nói rằng 1 trong 50 là "đủ tốt" và yêu cầu bạn chuyển sang dự án tiếp theo. Người giám sát của bạn vừa xác định điều nào sau đây cho hệ thống quét vân tay của bạn?

  - A. Tỷ lệ từ chối sai
  - B. Tỷ lệ chấp nhận sai
  - C. Ngưỡng quan trọng
  - D. Tiêu chí chấp nhận lỗi.

3. Thuật toán nào sau đây sử dụng khóa bí mật có dấu thời gian hiện tại để tạo ra mật khẩu một-lần?
  - A. Mã Xác thực Thông điệp dựa-trên-Băm
  - B. Mật khẩu Cấp phép Thông điệp Băm-theo-Ngày-tháng
  - C. Mật khẩu Một-Lần theo-Thời gian
  - D. Đăng nhập một-lần.
4. Liên quan đến xác thực, mã thông báo truy cập thuộc loại yếu tố nào?
  - A. Một cái gì đó bạn là
  - B. Một thứ gì đó mà bạn đang có
  - C. Một thứ gì đó mà bạn biết
  - D. Một thứ gì đó mà bạn thấy.
5. Hình thức nào sau đây *không phải* là dạng token phần cứng phổ biến?
  - A. Thẻ tiêm cận
  - B. Thẻ truy cập phổ biến
  - C. USB token
  - D. Quét mống mắt.
6. Trong khi gửi tiền mặt từ một cuộc gây quỹ từ thiện tại một ngân hàng địa phương, bạn nhận thấy nhân viên ngân hàng đang giơ những thẻ lên bên cạnh một bảng điều khiển ở gần cửa ra vào. Đèn trên bảng chuyển sang màu xanh lục và nhân viên có thể mở cửa. Đèn trên bảng điều khiển đó lúc bình thường có màu đỏ. Ngân hàng này đang sử dụng loại hình kiểm soát cửa điện tử nào?
  - A. Máy quét mống mắt
  - B. Token phần cứng
  - C. Thẻ tiêm cận
  - D. Token khóa đối xứng.

7. Đồng nghiệp của bạn đang kể cho bạn một câu chuyện mà cô ấy đã nghe về cách đánh lừa máy quét dấu vân tay bằng cách sử dụng kẹo cao su. Cô ấy nghe nói rằng nếu bạn ăn một thanh kẹo dẻo vào ngón tay của người dùng đã được cấp phép, thì bạn có thể sử dụng thanh kẹo gấu dẻo đó làm dấu vân tay của họ để đánh lừa máy quét dấu vân tay. Nếu điều này hoạt động, kết quả là một ví dụ về điều nào sau đây?
- A. Âm tính giả  
B. Dương tính giả  
C. Dương tính chéo  
D. Âm tính chéo.
8. Để đảm bảo khách hàng nhập những thông tin đăng nhập vào trang web của bạn là hợp lệ và không phải ai đó có được thông tin đăng nhập bị đánh cắp, nhóm của bạn được giao nhiệm vụ thiết kế xác thực đa yếu tố. Lựa chọn nào sau đây sẽ không phải là lựa chọn tốt?
- A. Mã tĩnh  
B. Cuộc điện thoại  
C. Ứng dụng xác thực  
D. Dịch vụ Tin nhắn Ngắn.
9. Khi bạn đang thiết kế và điều chỉnh hệ thống sinh trắc học, điểm mà cả tỷ lệ lỗi chấp nhận và từ chối bằng nhau được gọi là điểm nào dưới đây?
- A. Tỷ lệ chấp nhận chéo  
B. Tỷ lệ chồng chéo chấp-nhận-từ-chối  
C. Tỷ lệ lỗi chéo  
D. Tỷ lệ chấp nhận chồng chéo
10. Thuật ngữ nào sau đây *không phải* là thuật ngữ được sử dụng trong xác thực đa yếu tố?

- A.** Ai đó mà bạn biết
- B.** Bạn đang ở đâu đó
- C.** Một thứ gì đó mà bạn đang có
- D.** Một thứ gì đó bạn đang nhìn thấy.

## Đáp án

1. **B.** Đây rất có thể là một máy quét võng mạc. Máy quét võng mạc kiểm tra các mô hình mạch máu ở đáy mắt. Việc quét võng mạc phải được thực hiện ở khoảng cách gần, người dùng phải ở ngay trên thiết bị để nó hoạt động.
2. **A.** Người giám sát của bạn vừa xác định tỷ lệ từ chối sai (FRR) cho hệ thống của bạn. FRR là mức âm tính giả, hoặc từ chối sai sẽ được chấp nhận trong hệ thống. Trong trường hợp này, người giám sát của bạn sẵn sàng chấp nhận một lần từ chối sai cho mỗi 50 lần thử.
3. **C.** Thuật toán Mật khẩu Một-Lần theo-Thời-gian (TOTP) là một triển khai cụ thể của HOTP sử dụng khóa bí mật có kèm dấu thời gian hiện tại để tạo ra mật khẩu dùng một lần. Hãy lưu ý rằng dấu thời gian là một đầu mối quan trọng trong câu hỏi.
4. **B.** Mã thông báo (token) truy cập là một đối tượng vật lý xác định các quyền truy cập cụ thể và khi xác thực, nó nằm trong danh mục yếu tố "thứ mà bạn có".
5. **D.** Quét mống mắt sẽ được coi là một kỹ thuật sinh trắc học và không phải là một mã thông báo phần cứng. Mã thông báo phần cứng là một vật phẩm vật lý mà người dùng phải sở hữu để truy cập vào tài khoản của họ hoặc các tài nguyên nhất định.
6. **C.** Các nhân viên ngân hàng đang sử dụng thẻ tiêm cận, là loại thẻ ra vào không tiếp xúc cung cấp thông tin cho hệ thống kiểm soát một cửa điện tử. Thẻ tiêm cận chỉ cần đủ gần để máy quét hoạt động - chúng không cần thực sự chạm vào máy quét.
7. **B.** Đây là một ví dụ về dương tính giả. Dương tính giả xảy ra khi quét sinh trắc học và cho phép người không được cấp phép có được quyền truy cập.

8. **A.** Mã tĩnh **có** thể được ghi lại và phát lại và không phù hợp với các hệ thống có người dùng đang hoạt động.
9. **C.** Tỷ lệ lỗi chéo (CER) là tỷ lệ mà tại đó tỷ lệ lỗi chấp nhận và lỗi từ chối là bằng nhau. Đây là trạng thái mong muốn để hệ thống sinh trắc học hoạt động hiệu quả nhất và nó có thể được quản lý bằng cách điều chỉnh giá trị ngưỡng được sử dụng để đối sánh.
10. **D.** Thứ gì đó mà bạn nhìn thấy không phải là yếu tố (thứ bạn biết, thứ bạn có hoặc bạn đang là ai) cũng không phải là thuộc tính (bạn đang ở đâu, điều gì đó bạn có thể thực hiện, điều gì đó bạn trưng ra, hoặc người mà bạn biết).

## Chương 13 Khả năng Phục hồi An ninh mạng

### Khả năng Phục hồi An ninh mạng

Trong chương này bạn sẽ

- Xem xét các thành phần để tạo ra tính dự phòng,
- Tìm hiểu các kiểu sao lưu và những vai trò của chúng trong khả năng phục hồi.

Các hệ thống được thiết kế để hoạt động vì một mục đích nào đó, và chúng ta sử dụng thuật ngữ *rủi ro* để mô tả những kết quả tác động khi các vấn đề về sự sụt giảm hiệu suất từ một trạng thái tối ưu. Vì nhiều lý do, việc mong đợi rằng một hệ thống luôn luôn hoạt động hoàn hảo, nói chung luôn là điều bất hợp lý. Chúng ta có thể thiết lập các biện pháp bảo vệ để giảm thiểu các vấn đề xảy ra khi một hệ thống bị sụt giảm, nhưng nó vẫn đặt ra câu hỏi về cách thức làm thế nào để một hệ thống quay trở lại hoạt động với hiệu suất đầy đủ. Đây là lúc khả năng phục hồi xuất hiện. Một hệ thống có khả năng phục hồi là hệ thống có thể trở lại điều kiện hoạt động thích hợp sau khi gặp phải sự cố. Và trong môi trường ngày càng thù địch ngày nay, đây là một thước đo an ninh quan trọng.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu kỳ thi 2.5 CompTIA Security+: Đặt ra một tình huống, triển khai khả năng phục hồi an ninh mạng.

## Dự phòng

*Dự phòng* là việc sử dụng nhiều thành phần độc lập để thực hiện một chức năng quan trọng, để từ đó nếu một thành phần bị lỗi, sẽ có một thành phần khác thực hiện công việc thay cho thành phần đã bị lỗi. Khi phát triển một chiến lược phục hồi cho việc đảm bảo rằng một tổ chức có được những gì nó cần để tiếp tục hoạt động, thậm chí ngay cả khi phần cứng hoặc phần mềm bị lỗi hoặc nếu bảo mật bị vi phạm, bạn nên cân nhắc các biện pháp khác liên quan đến dự phòng và phần cứng thay thế. Một số cách áp dụng phổ biến về dự phòng bao gồm việc sử dụng các máy chủ dự phòng, các kết nối dự phòng, và các ISP dự phòng. Nhu cầu đối với các máy chủ và kết nối dự phòng có thể tương đối rõ ràng, nhưng các ISP dự phòng có thể sẽ không như vậy, ít nhất là tại thời điểm ban đầu. Rất nhiều ISP đã có nhiều truy cập vào Internet của riêng họ, nhưng bằng cách có thêm các kết nối ISP bổ sung, một tổ chức có thể làm giảm nguy cơ từ việc gián đoạn của một ISP sẽ có tác động tiêu cực đến tổ chức. Việc đảm bảo truy cập Internet của nhân viên hoặc truy cập vào trang thương mại điện tử của tổ chức cho khách hàng không bị gián đoạn đang ngày càng trở nên quan trọng.

Nhiều tổ chức nhận thấy không nhất thiết phải duy trì một nguồn cung cấp các phụ tùng thay thế. Rốt cuộc, với giá của thiết bị lưu trữ đang giảm dần và tốc độ của bộ vi xử lý ngày càng gia tăng, tại sao phải thay thế một bộ phận bị hỏng bằng công nghệ cũ hơn? Tuy nhiên, một nguồn cung cấp phụ tùng thay thế sẵn sàng có thể giúp cho quá trình đưa hệ thống hoạt động trở lại trạng thái hoạt động trở lại dễ dàng hơn. Việc thay thế phần cứng và phần mềm bằng các phiên bản mới hơn đôi khi có thể dẫn đến các vấn đề về khả năng tương thích. Một phiên bản cũ hơn của một số phần mềm quan trọng có thể không hoạt động với phần cứng mới hơn, vốn có thể có nhiều năng lực hơn theo nhiều cách khác nhau. Việc dự phòng các phần cứng (hoặc phần mềm) tối quan trọng cho các

chức năng tối quan trọng trong tổ chức có thể tạo điều kiện thuận lợi một cách đáng kể cho việc duy trì tính liên tục của hoạt động kinh doanh trong trường hợp có lỗi phần mềm hoặc phần cứng.



**MÁCH NƯỚC CHO KỲ THI** Dự phòng là một yếu tố quan trọng trong cả tính bảo mật lẫn độ tin cậy. Hãy đảm bảo rằng bạn hiểu được nhiều khu vực khác nhau có thể được hưởng lợi từ các thành phần dự phòng.

### **Phân tán Địa lý**

Một yếu tố quan trọng có ảnh hưởng đến chi phí của chiến lược sao lưu là chi phí của việc lưu trữ các bản sao lưu. Một chiến lược đơn giản có thể là lưu trữ tất cả các bản sao lưu của bạn lại cùng nhau để thực hiện các hành động khôi phục nhanh chóng và dễ dàng. Tuy nhiên, đây không phải là một ý kiến hay. Giả sử rằng sự kiện thảm khốc cần khôi phục lại dữ liệu đã-sao-lưu là một vụ hỏa hoạn đã phá hủy hệ thống máy tính mà dữ liệu được xử lý trên đó. Trong trường hợp này, bất kỳ bản sao lưu nào được lưu trữ trong cùng một cơ sở cũng có thể bị mất đi trong cùng một vụ cháy.

Giải pháp là giữ các bản sao lưu ở các vị trí riêng biệt. Bản sao gần nhất có thể được lưu trữ cục bộ, vì nó có nhiều khả năng được cần đến nhất, trong khi các bản sao khác có thể được lưu giữ ở các địa điểm khác. Tùy thuộc vào mức độ bảo mật mà tổ chức của bạn mong muốn, bản thân địa điểm lưu trữ có thể được củng cố để chống lại các mối đe dọa có thể xảy ra trong khu vực của bạn (chẳng hạn như lốc xoáy hoặc lũ lụt). Một tiến bộ gần đây hơn là các dịch vụ sao lưu trực tuyến. Một số công ty bên thứ ba cung cấp kết nối tốc-độ-cao để lưu trữ dữ liệu trong một cơ sở riêng biệt. Việc truyền dữ liệu sao lưu qua kết nối mạng làm giảm bớt một số vấn đề khác đối với chuyển động vật lý của các phương tiện lưu

trữ truyền thống hơn, chẳng hạn như sự cẩn thận trong quá trình vận chuyển (chẳng hạn như băng từ không hoạt động tốt dưới ánh sáng mặt trời trực tiếp) hoặc thời gian để vận chuyển băng từ.

## Ổ đĩa

Các ổ đĩa là cơ chế lưu trữ chính trong một hệ thống, bất kể được cấu thành từ các ổ đĩa cứng vật lý với các đĩa quay hoặc các thiết bị nhớ thể-rắn. Thuật ngữ *đĩa* đề cập đến các đĩa quay trong truyền thống, nhưng ngày càng có nhiều quá trình lưu trữ được xử lý bởi bộ nhớ thể-rắn. Ngoài ra, những cấu trúc đĩa luận lý có thể được ánh xạ qua nhiều phần tử lưu trữ vật lý.

## Các Mức Mảng Dự phòng Đĩa Rẻ tiền (Redundant Array of Inexpensive Disks – RAID)

Một phương pháp tiếp cận phổ biến để gia tăng độ tin cậy trong việc lưu trữ trên đĩa cứng là sử dụng một *mảng dự phòng các đĩa cứng rẻ tiền (RAID)*. RAID lấy những dữ liệu thường được lưu trữ trên một đĩa duy nhất và trải rộng nó ra giữa một số đĩa khác. Nếu bất kỳ đĩa đơn nào bị mất (hỏng), dữ liệu có thể được khôi phục từ các đĩa khác, nơi dữ liệu cũng đang lưu trú. Với giá bán các đĩa lưu trữ ngày càng giảm, phương pháp tiếp cận này ngày càng trở nên phổ biến đến mức nhiều người dùng cá nhân thậm chí còn trang bị mảng RAID cho hệ thống tại gia đình của họ. RAID cũng có thể làm tăng tốc độ khôi phục dữ liệu vì nhiều ổ đĩa có thể bận truy xuất dữ liệu được yêu cầu cùng một lúc thay vì chỉ dựa vào một ổ đĩa để thực hiện công việc.

Một số phương pháp tiếp cận RAID khác nhau có thể được xem xét, bao gồm:

- **RAID 0** (đĩa tạo thành dải) chỉ đơn giản là trải rộng dữ liệu, vốn sẽ được lưu trữ trên một đĩa, qua một vài ổ đĩa khác. Việc này làm

giảm thời gian tiêu tốn để truy xuất dữ liệu bởi vì dữ liệu được đọc từ nhiều ổ đĩa tại cùng một thời điểm, nhưng lại không cải thiện được độ tin cậy vì chỉ cần một đĩa bị mất (hư hỏng) cũng sẽ dẫn đến việc mất toàn bộ dữ liệu (vì các phần của các tập tin được trải rộng ra giữa các đĩa khác nhau). Với RAID 0, dữ liệu được chia nhỏ trên toàn bộ các đĩa mà không có dự phòng.

- **RAID 1** (đĩa phản chiếu) đối ngược với RAID 0. RAID 1 sao chép dữ liệu từ một đĩa sang một hoặc nhiều đĩa khác. Nếu bất kỳ một đĩa nào bị mất (hư hỏng), dữ liệu cũng sẽ không bị mất vì nó cũng được sao chép trên (các) đĩa khác. Phương pháp này có thể được sử dụng để cải thiện độ tin cậy và tốc độ truy xuất, nhưng nó tương đối đắt tiền khi so sánh với những kỹ thuật RAID khác.
- **RAID 2** (mã sửa-lỗi cấp-degree-bit) thường không được sử dụng, vì nó chia dài dữ liệu qua nhiều ổ đĩa ở cấp độ từng bit, ngược lại với cấp độ khối (block). Nó được thiết kế để có khả năng khôi phục lại bất kỳ một đĩa đơn lẻ nào bị mất (hư hỏng) thông qua việc sử dụng các kỹ thuật sửa-lỗi.
- **RAID 3** (phân-dài-byte với sửa lỗi) trải rộng dữ liệu trên nhiều đĩa ở cấp độ byte với một đĩa được dành riêng cho các bit chẵn lẻ. Kỹ thuật này thường không được triển khai vì các hoạt động nhập/xuất không thể bị chồng chéo do nhu cầu tất cả phải đều truy cập vào cùng một đĩa (đĩa có các bit chẵn lẻ).
- **RAID 4** (ổ đĩa chẵn lẻ chuyên dụng) trải rộng dữ liệu trên nhiều đĩa nhưng thành các dải lớn hơn so với RAID 3 và sử dụng một ổ đĩa duy nhất để kiểm tra lỗi dựa trên chẵn lẻ. RAID 4 có nhược điểm là không cải thiện tốc độ truy xuất dữ liệu vì tất cả các truy xuất vẫn cần phải truy cập vào ổ đĩa chẵn lẻ.
- **RAID 5** (phân-dài-khối với kiểm tra lỗi) là một phương pháp thường được sử dụng để làm phân dải dữ liệu ở cấp độ khối và trải rộng dữ

liệu chẵn lẻ trên các ổ đĩa. Điều này đem lại cả độ tin cậy lẫn sự gia tăng hiệu suất về tốc độ. Hình thức [RAID] này yêu cầu tối thiểu phải có ba ổ đĩa.

RAID 0 đến 5 là các kỹ thuật ban đầu, với RAID 5 là phương pháp phổ biến nhất được sử dụng, vì nó cung cấp cả sự cải tiến độ tin cậy lẫn tốc độ. Các phương pháp bổ sung cũng đã được triển khai, chẳng hạn như sao chép dữ liệu chẵn lẻ trên các đĩa (RAID 6) và một dải phản chiếu (RAID 10). Một số cấp độ có thể được kết hợp để tạo ra cấp độ RAID bao gồm hai chữ số. Do đó, RAID 10 là sự kết hợp của cấp độ 1 (phản chiếu) và 0 (phân dải), đó là lý do tại sao nó cũng đôi khi được xác định là RAID 1 + 0. Phản chiếu là việc ghi dữ liệu vào hai hoặc nhiều ổ đĩa cứng (HDD) tại cùng một thời điểm - nếu một đĩa bị lỗi, hình ảnh đã được phản chiếu sẽ bảo toàn dữ liệu từ đĩa bị lỗi. Việc phân dải sẽ chia nhỏ dữ liệu thành các "phần (chunks)" được ghi liên tiếp vào các ổ đĩa khác nhau.



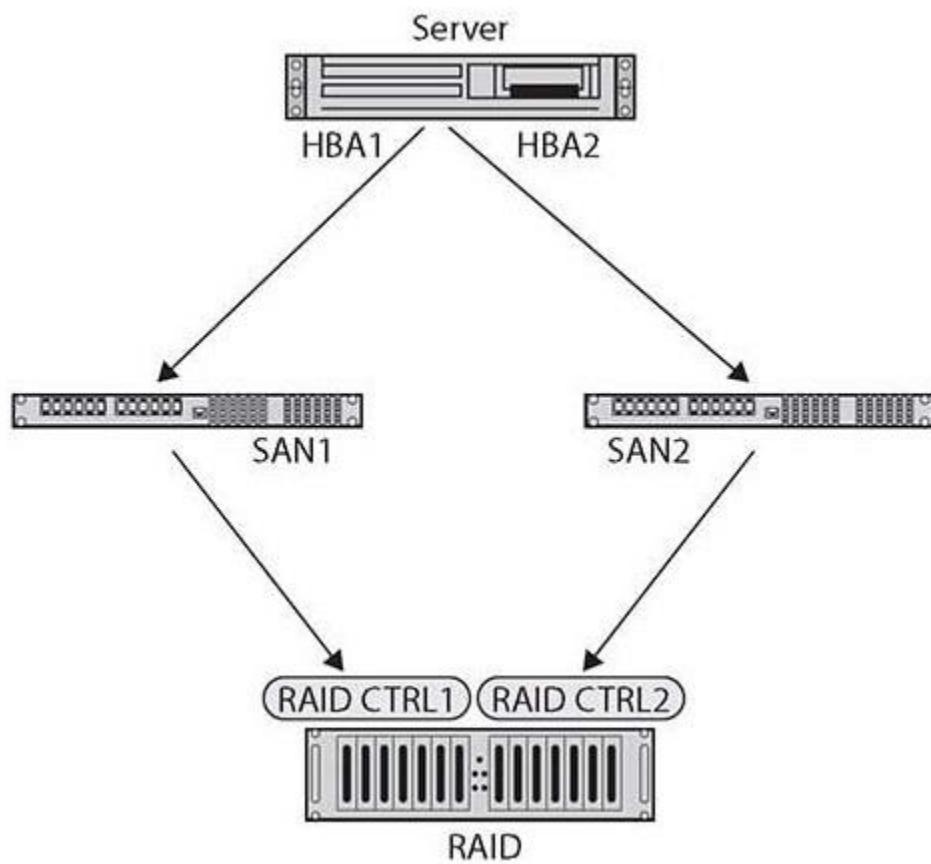
## MÁCH NƯỚC CHO KỲ THI

Kiến thức về các cấu trúc RAID cơ bản theo ký hiệu số là một yếu tố có thể kiểm tra được và nên được ghi nhớ cho kỳ thi. Cả RAID 0 và RAID 1 đều yêu cầu tối thiểu hai ổ đĩa. Cả RAID 3 và RAID 5 đều có tối thiểu ba ổ đĩa. RAID 10 (còn gọi là 1 + 0) yêu cầu tối thiểu bốn ổ đĩa.

## Đa đường

Giữa các hệ thống lưu trữ và máy tính/máy chủ là một giao diện Nhập/Xuất (I/O interface). Giao diện Nhập/Xuất này chuyển đổi thông tin từ máy tính thành một dạng hoạt động được với hệ thống lưu trữ cụ thể. Có một số giao diện khác nhau cho các kiểu hệ thống lưu trữ khác nhau (ví dụ, RAID, SCSI, Fiber Channel, và SATA), mỗi giao diện được thiết kế để xử lý những quá trình truyền dữ liệu cần thiết. Khi một thành phần

lưu trữ được kết nối bằng nhiều bộ điều hợp (adapter), việc này sẽ mang lại sự dự phòng trong trường hợp một vấn đề xảy ra với một bộ điều hợp. Đây được gọi là kết nối *đa đường* và thường được sử dụng trong các máy chủ có độ-tin-cậy-cao và các hệ thống tối quan trọng. Hình 13-1 cho thấy một máy chủ có hai bộ điều hợp bus chủ (HBA), cùng với hai bộ chuyển mạch mạng vùng lưu trữ (SAN) và hai bộ điều khiển RAID. Điều này cung cấp hai đường dẫn độc lập từ máy chủ đến dữ liệu.



**Hình 13-1** Cấu hình đa đường của một thiết bị RAID đối với một máy chủ

### Mạng

Mạng là yếu tố cơ sở hạ tầng để kết nối tất cả các thành phần CNTT trong doanh nghiệp. Một mạng có thể coi như một điểm lỗi hoặc nó có thể là

một hệ thống các kết nối dự phòng có thể được khôi phục theo các tǎi lưu lượng và các điều kiện kết nối khác nhau. Việc có được một mạng được kiến trúc phù hợp có nhiều đường dẫn độc lập và các phần tử cơ sở hạ tầng được thiết kế để gia tăng khả năng dự phòng là điều quan trọng. Hai phần tử chính cần phải xem xét là bộ cân bằng tải và thẻ giao diện mạng (network interface card - NIC) gội để loại bỏ một số chẽ độ phổ biến của lỗi lưu lượng liên-quan-đến-mạng.

## Bộ Cân bằng tải

Một số hệ thống nhất định, chẳng hạn như các máy chủ, sẽ có tầm quan trọng cao hơn đối với hoạt động kinh doanh và do đó phải là đối tượng của các biện pháp chịu-lỗi. Một kỹ thuật phổ biến được sử dụng trong khả năng chịu lỗi là việc cân bằng tải thông qua việc sử dụng *bộ cân bằng tải*, công cụ này di chuyển tải trên một tập hợp các nguồn tài nguyên với nỗ lực không làm quá tải từng máy chủ riêng lẻ. Kỹ thuật này được thiết kế để phân phối tải xử lý trên hai hoặc nhiều hệ thống. Nó được sử dụng để giúp cải thiện việc sử dụng tài nguyên và thông lượng nhưng cũng có thêm lợi thế là gia tăng khả năng chịu lỗi của hệ thống tổng thể vì một tiến trình quan trọng có thể được chia ra chạy trên nhiều hệ thống. Nếu bất kỳ một hệ thống nào bị lỗi, các hệ thống khác có thể tiếp nhận tiến trình mà hệ thống đã bị lỗi đang xử lý. Mặc dù có thể có tác động đến thông lượng tổng thể, nhưng hoạt động không bị sụt giảm hoàn toàn. Cân bằng tải thường được sử dụng cho các hệ thống xử lý trang web, truyền tải tập tin băng-thông-cao và mạng Internet Relay Chat (IRC) lớn. Cân bằng tải hoạt động bằng một loạt các kiểm tra sức khỏe để cho bộ cân bằng tải biết rằng máy nào đang hoạt động và bằng cơ chế lập lịch trình giúp phân tán công việc một cách đồng đều. Cân bằng tải là tốt nhất cho các hệ thống không có trạng thái, vì các yêu cầu tiếp theo có

thể được xử lý bởi bất kỳ máy chủ nào, không chỉ máy chủ đã từng xử lý yêu cầu trước đó.

### **Gộp Card Giao diện Mạng (NIC)**

Nếu một máy chủ có nhiều card giao diện mạng (NIC) kết nối nó với một bộ chuyển mạch hoặc bộ định tuyến, nó sẽ có rất nhiều địa chỉ, một địa chỉ cho mỗi NIC. *Gộp NIC (NIC teaming)* là một phương tiện kết nối thay thế được sử dụng bởi các máy chủ có nhiều card giao diện mạng và muốn tận hưởng các lợi ích của cân bằng tải, khả năng chịu lỗi và chuyển đổi dự phòng mà không đòi hỏi thêm cơ sở hạ tầng để thực hiện điều đó. Khi gộp NIC được sử dụng, hệ điều hành kết hợp các NIC thành một NIC ảo theo quan điểm của hệ điều hành. Nếu một hoặc nhiều kết nối có vấn đề về lưu lượng hoặc sự cố kết nối, các NIC khác có thể chịu tải của một hoặc nhiều kết nối đang gặp phải vấn đề đó. Sử dụng gộp NIC cho phép máy chủ của bạn có khả năng dự phòng và tăng băng thông, thậm chí ngay cả trong trường hợp bất kỳ bộ điều hợp vật lý hoặc hệ thống cáp nào của bạn bị lỗi.



### **MÁCH NƯỚC CHO KỲ THI**

Gộp NIC nhóm nhiều NIC lại với nhau để hình thành nên một thiết bị mạng luận lý được gọi là một sự liên kết (bond). Điều này sẽ mang lại cả khả năng cân bằng tải lẫn khả năng chịu lỗi.

### **Nguồn điện**

Nguồn điện là điều bắt buộc để tất cả các máy móc hoạt động, và việc có được một nguồn điện đáng tin cậy và có khả năng phục hồi là điều tối quan trọng đối với các hoạt động liên tục của máy tính của doanh nghiệp. Máy chủ và thiết bị mạng luôn ở trạng thái bật, và thậm chí thỉnh thoảng bị mất điện do lỗi thiết bị cần phải được lập kế hoạch và quản lý để cung

cấp một mức dịch vụ thích hợp. Trong một doanh nghiệp hiện đại, các thiết bị như nguồn cấp điện liên tục, máy phát điện, nguồn cung cấp kép và phân phối điện được quản lý đều hỗ trợ việc luôn có được mức sẵn sàng điện năng thích hợp cho thiết bị mạng tại mọi thời điểm.

### **Nguồn Cấp điện Liên tục (Uninterruptible Power Supply – UPS)**

*Nguồn cấp điện liên tục (UPS)* là hệ thống cung cấp điện có thể hoạt động bằng cách sử dụng một [hệ thống] pin dự phòng tạm thời trong trường hợp bị mất điện [từ nguồn cấp điện chính]. Các UPS thường không có đủ khả năng dự phòng của ắc quy để tồn tại trong thời gian dài, nhưng chúng được thiết kế để giữ cho thiết bị hoạt động trong khi nguồn điện dự phòng, chẳng hạn như từ máy phát điện, được kết nối trở lại. Trong một hệ thống doanh nghiệp, hầu hết các UPS được thiết kế và đánh giá cho thời gian hoạt động thường là trong 20 phút. Đây là khoảng thời gian đủ để các máy phát điện dự phòng khởi động hoặc trong trường hợp không thể khôi phục lại nguồn điện, để các máy chủ chuyển đến địa điểm thứ cấp như một phần của kế hoạch hoạt động liên tục và sau đó được tắt một cách duyên dáng.

### **Máy phát điện**

*Máy phát điện* dự phòng được sử dụng để cung cấp điện khi nguồn điện bình thường bị mất. Nguồn năng lượng cho các thiết bị này là khí đốt tự nhiên hoặc dầu diesel và chúng tạo ra năng lượng điện đủ để đáp ứng các dịch vụ mong muốn trong thời gian bị mất điện. Máy phát điện đi kèm với một loạt các yêu cầu, bao gồm cả bảo trì và kiểm nghiệm, và chúng đòi hỏi hoạt động kiến trúc điện đáng kể để cài đặt các mạch mong muốn. Mục tiêu thường không phải là cung cấp năng lượng cho mọi thứ mà nguồn điện thông thường cung cấp, vì quy mô cung cấp điện có thể sẽ tốn kém trong một số trường hợp. Các mạch được cấp điện bởi máy phát điện dự phòng là các mạch riêng biệt cung cấp điện cho các thành phần

mong muốn. Việc định cỡ (sizing) của máy phát điện dự phòng được thực hiện liên quan đến tải và do cơ sở hạ tầng vật lý, không hề là dễ dàng hoặc tiết kiệm chi phí để liên tục thay đổi kích thước nguồn dự phòng. Một vấn đề khác là khi sử dụng lâu dài trong trường hợp máy phát điện chạy dầu diesel, nguồn cung cấp nhiên liệu cần phải được quản lý. Vì các hệ thống này thường được sử dụng trong các thảm họa thiên nhiên, nên việc có được các hợp đồng để hoạt động trong thời gian xảy ra thảm họa là điều quan trọng đối với các hoạt động tiếp tế nhiên liệu và bảo trì.

### **Nguồn điện Kép (Dual Supply)**

Các bộ phận riêng lẻ của thiết bị có nguồn cấp điện trong đó để chuyển đổi công suất đường dây trong thiết bị thành điện áp và dòng điện được sử dụng bởi các thiết bị. Các nguồn cung cấp điện riêng lẻ là một trong những liên kết yếu nhất trong một thiết bị, vì chúng có xu hướng bị hỏng hóc ở tốc độ cao hơn nhiều so với thiết bị điện-áp-thấp-hơn mà chúng cung cấp điện, do đó, cần phải có một kế hoạch cho những nguồn cấp điện riêng lẻ này khi chúng bị lỗi. Trong những trường hợp mất điện nhẹ sẽ không sao, việc có nguồn cấp điện dự phòng có thể thay thế được sẽ hoạt động ngoại tuyến.

Tuy nhiên, đối với máy chủ và các phần khác của cơ sở hạ tầng tối quan trọng, việc được có một hệ thống nguồn kép và dự phòng là điều cần thiết. Một *nguồn kép* là hệ thống sử dụng hai bộ cấp nguồn điện độc lập đều có khả năng xử lý tải. Trong trường hợp một trong hai nguồn bị mất, nguồn còn lại tiếp tục chịu tải. Thông thường, các thiết bị này cũng được chế tạo để có thể thay thế nóng [thay thế trong khi vẫn đang hoạt động], vì vậy trong trường hợp hỏng hóc, nguồn cung cấp kém có thể được thay thế mà không cần phải tắt nguồn thiết bị.

### **Các Đơn vị Phân phối Điện Được quản lý (Managed Power Distribution Units – PDUs)**

Một đơn vị phân phối điện được quản lý (PDU) là một thiết bị được thiết kế để xử lý nguồn điện cho các tủ máy chủ. Một tủ máy chủ đồng dân cư có thể sử dụng lượng điện năng lên đến 30kVA, hoặc gấp 10 lần lượng điện năng cho một ngôi nhà thông thường. Đây là lý do tại sao các phòng máy chủ cần có hệ thống HVAC đặc biệt để xử lý việc phân phối nhiệt và chúng sử dụng các đơn vị phân phối điện được quản lý để xử lý hiệu quả về mặt điện. Một PDU có thể sử dụng nguồn điện ba-pha 440/240VAC và chuyển đổi nó thành nguồn 110VAC hoặc 48VDC một-pha. Mục tiêu của PDU là chuyển đổi năng lượng một cách hiệu quả và quản lý lượng nhiệt tỏa ra từ quá trình chuyển đổi, đồng thời tạo ra dòng điện được điều chỉnh từ các mức tăng đột biến và các điều kiện điện áp quá mức/quá thấp. Hầu hết các PDU đều cung cấp khả năng giám sát mở rộng, vì vậy toàn bộ tủ máy chủ có thể có nguồn điện của chúng được giám sát từ xa để tìm ra các điều kiện có thể gây ra sự cố.



**MÁCH NƯỚC CHO KỲ THI** Đối với một tình huống, bạn nên hiểu được cách mà mỗi thiết bị được sử dụng để quản lý nguồn điện và cung cấp khả năng phục hồi an ninh mạng.

### Nhân bản

*Nhân bản* là một dạng dự phòng đơn giản - nghĩa là, có được một bản sao khác của một thứ gì đó nếu điều gì đó sẽ xảy ra với bản gốc. Bộ nguồn kép nhân bản nguồn điện. Có được một mảng đĩa dự phòng để lưu trữ dữ liệu là một hình thức nhân bản khác, cũng như các bản sao lưu và có các hoạt động thay thế ở các địa điểm ngoại biên cho các mục đích liên tục kinh doanh. Trong những tình huống mà việc có một thứ gì đó cụ thể là điều thiết yếu thì việc nghe ai đó nói "hai là một, và một là không" là một điều rất phổ biến. Những cách thức phổ biến để nhận thấy sự nhân

bản trong các hoạt động hàng ngày của doanh nghiệp bao gồm việc sử dụng mạng khu vực lưu trữ và công nghệ máy ảo.

### **Mạng Khu vực Lưu trữ (SAN)**

*Mạng khu vực lưu trữ (SAN)* là một mạng chuyên dụng kết nối các phần tử tính toán với các phần tử lưu trữ. Mạng này có thể được tối ưu hóa đối với các loại lưu trữ dữ liệu cần thiết, xét về mặt kích thước và tốc độ dữ liệu, về định dạng và về tiêu chí truy cập. Việc có được mô hình cũ của dữ liệu được lưu trữ trên các đĩa được gắn trực tiếp vào máy đại diện cho một chế độ lỗi khi máy bị lỗi. Nó cũng sẽ có vấn đề khi mở rộng quy mô với số lượng lớn, chẳng hạn như cơ sở dữ liệu doanh nghiệp với rất nhiều người dùng. SAN giải quyết điểm lỗi này bằng cách làm cho việc lưu trữ dữ liệu trở nên độc lập với bất kỳ máy tính cá nhân nào và thậm chí có thể giao tiếp với nhiều hệ thống lưu trữ dự phòng để cho phép tính dự phòng cả về phía lưu trữ dữ liệu.

### **Máy ảo**

Những công nghệ *máy ảo (VM)* có thể cho phép nhân bản các đơn vị xử lý có thể được thao tác giữa các máy tính khác nhau. Việc có một đại điểm với nhiều máy chủ giống hệt nhau để xử lý tài sản có các vấn đề liên quan đến lỗi của các máy chủ riêng lẻ và việc xây dựng lại các thành phần máy chủ đó về phía phần mềm. Công nghệ VM giải quyết vấn đề đó bằng cách cho phép nhiều bản sao của một phiên bản cụ thể được sử dụng trên các phần cứng khác nhau và với sự giám sát và quản lý tập trung. Cần thêm một máy chủ web do vẫn đề với tải hệ thống hiện tại? Chỉ cần khởi động một máy ảo khác. Chỉ mất vài giây so với việc cung cấp và xây dựng một máy chủ - một quá trình được tính bằng giờ hoặc bằng ngày. Máy ảo đã cách mạng hóa hoạt động máy tính của công ty vì chúng cho phép quản trị viên quản lý máy tính dễ dàng bằng cách trỏ và nhấp để bổ sung thêm hoặc loại bỏ dung lượng và năng lực xử lý

bằng cách sử dụng hình ảnh tốt đã được biết. Nếu một trường hợp cụ thể được sửa đổi bởi một tác nhân trái phép, một hình ảnh thay thế tốt đã được biết có thể được thiết lập một cách nhanh chóng, trả lại năng lực cho doanh nghiệp. Ngoài ra, việc triển khai phù hợp các máy ảo và các công nghệ máy chủ có thể mang lại sự độc lập về phần cứng cho các hình ảnh hệ điều hành cụ thể, cho phép sử dụng tài nguyên máy chủ một cách hiệu quả.

### Tại chỗ so với Đám mây

Khi bạn đang kiểm tra sự dự phòng, một yếu tố cần xem xét là vị trí. Công việc sẽ diễn ra tại chỗ hay đang được thực hiện trên đám mây? Bản thân điều này không mang lại tính dự phòng, nhưng một khi đã xác định được vị trí thì các yếu tố có thể được sử dụng để đảm bảo các mức độ dự phòng phù hợp dựa trên rủi ro.

### Các kiểu Sao lưu

Một yếu tố then chốt trong các kế hoạch liên tục kinh doanh/khôi phục sau thảm họa (BC/DR) là tính sẵn sàng của các *bản sao lưu*. Điều này không chỉ đúng vì khả năng xảy ra của một thảm họa mà còn vì phần cứng và phương tiện lưu trữ sẽ bị lỗi theo định kỳ, dẫn đến việc mất hoặc hư hỏng dữ liệu quan trọng. Một tổ chức cũng có thể nhận thấy rằng các bản sao lưu là rất quan trọng khi các biện pháp bảo mật thất bại và một cá nhân có quyền truy cập vào thông tin quan trọng có thể đã bị hỏng hoặc ít nhất là không thể tin cậy được. Do đó, sao lưu dữ liệu là một yếu tố tối quan trọng trong các kế hoạch này cũng như trong các hoạt động bình thường. Có một số yếu tố cần được xem xét trong chiến lược sao lưu dữ liệu của tổ chức, bao gồm:

- Việc sao lưu nên được tiến hành với tần suất như thế nào?
- Các bản sao lưu cần mở rộng đến mức nào?
- Quy trình tiến hành sao lưu là gì?

- Ai chịu trách nhiệm đảm bảo các bản sao lưu được tạo ra?
- Các bản sao lưu sẽ được lưu trữ ở đâu?
- Các bản sao lưu sẽ được lưu giữ trong bao lâu?
- Có bao nhiêu bản sao sẽ được duy trì?

Hãy lưu ý rằng mục đích của bản sao lưu là cung cấp dữ liệu hợp lệ và không bị gián đoạn trong trường hợp tập tin gốc hoặc phương tiện lưu trữ dữ liệu bị hư hỏng hoặc bị mất. Tùy thuộc vào loại hình tổ chức, các yêu cầu pháp lý đối với việc duy trì các bản sao lưu cũng có thể ảnh hưởng đến cách nó được hoàn thành.

Có bốn hình thức sao lưu chính: toàn bộ, tăng dần, khác biệt và ảnh chụp nhanh. Mỗi hình thức đều có ưu và nhược điểm về thời gian sao lưu và khôi phục cũng như độ phức tạp. Các kiểu sao lưu này được mô tả trong các phần sắp tới.

Việc hiểu được mục đích của bit lưu trữ là điều quan trọng khi bạn đọc về các kiểu sao lưu. Bit lưu trữ được sử dụng để cho biết tập tin đã (1) hay không (0) được thay đổi kể từ lần sao lưu cuối cùng. Bit được đặt (thay đổi thành 1) nếu tập tin đã được sửa đổi hoặc trong một số trường hợp, nếu tập tin được sao chép, bản sao mới của tập tin sẽ có bộ bit lưu trữ của nó. Bit được đặt lại (thay đổi thành 0) khi tập tin được sao lưu. Bit lưu trữ cũng có thể được sử dụng để xác định tập tin nào cần được sao lưu khi sử dụng các phương pháp như phương pháp sao lưu khác biệt.



## MÁCH NƯỚC CHO KỲ THI

Khi tìm hiểu về các kiểu sao lưu dưới đây, hãy nhớ lưu ý đến các chi tiết liên quan đến số lượng bản sao lưu cần thiết để khôi phục. Đây là một câu hỏi điển hình trong đề thi: "Với kiểu sao lưu này (khác biệt hoặc tăng dần) và sơ đồ sao lưu bảy ngày, cần

bao nhiêu băng đĩa phòng để khôi phục?". Hãy lưu ý rằng đây không phải là trường hợp ghi nhớ đơn giản vì bạn cần các chi tiết từ kịch bản để trả lời câu hỏi. Ngoài ra, bạn cần biết được "thứ tự khôi phục" của các bản sao lưu.

### **Đầy đủ (Full)**

Kiểu sao lưu dễ hiểu nhất là *sao lưu đầy đủ*. Trong một bản sao lưu đầy đủ, tất cả các tập tin và phần mềm được sao chép vào phương tiện lưu trữ. Việc khôi phục từ bản sao lưu đầy đủ cũng đơn giản tương tự - bạn phải sao chép tất cả các tập tin trở lại hệ thống. Quá trình này có thể mất một lượng thời gian đáng kể. Hãy xem xét kích thước của ngay cả một máy tính cá nhân của gia đình trung bình ngày nay, dung lượng lưu trữ được tính bằng hàng chục và hàng trăm gigabyte (GB). Việc sao chép lượng dữ liệu này sẽ cần nhiều thời gian. Trong một bản sao lưu đầy đủ, bit lưu trữ sẽ bị xóa.



### **MÁCH NƯỚC CHO KỲ THI**

Một bản sao lưu đầy đủ sao chép toàn bộ dữ liệu và xóa/khôi phục bit lưu trữ. Quá trình này sẽ tiêu tốn thời gian đáng kể để hoàn tất nhưng cho phép khôi phục toàn bộ với chỉ một băng từ.

### **Gia tăng (Incremental)**

*Sao lưu gia tăng* là một biến thể của bản sao lưu khác biệt, với điểm khác biệt là thay vì sao chép tất cả các tập tin đã thay đổi kể từ lần sao lưu đầy đủ gần đây nhất, sao lưu gia tăng chỉ sao lưu các tập tin đã thay đổi kể từ lần sao lưu đầy đủ hoặc gia tăng gần đây nhất xảy ra, do đó đòi hỏi ít tập tin được sao lưu hơn. Với các bản sao lưu gia tăng, thậm chí ít thông tin hơn sẽ được lưu trữ trong mỗi bản sao lưu. Cũng giống như trong trường hợp sao lưu khác biệt, sao lưu gia tăng phụ thuộc vào việc

thực hiện sao lưu đầy đủ không thường xuyên. Sau đó, bạn chỉ cần sao lưu các tập tin đã thay đổi kể từ lần sao lưu cuối cùng của bất kỳ loại nào được tiến hành. Để khôi phục hệ thống bằng cách sử dụng phương pháp sao lưu này đòi hỏi nhiều công việc hơn. Trước tiên, bạn cần quay lại bản sao lưu đầy đủ cuối cùng và tải lại hệ thống với dữ liệu này. Sau đó, bạn phải cập nhật hệ thống với mọi bản sao lưu gia tăng đã xảy ra kể từ bản sao lưu đầy đủ sau cùng. Ưu điểm của kiểu sao lưu này là nó đòi hỏi ít dung lượng và thời gian để hoàn thành hơn. Điểm bất lợi là quá trình khôi phục có nhiều thứ liên quan hơn. Tuy nhiên, giả sử rằng bạn không thường xuyên phải tiến hành khôi phục hoàn toàn hệ thống của mình thì sao lưu gia tăng là một kỹ thuật hợp lý. Một bản sao lưu gia tăng sẽ xóa bit lưu trữ.



### **MÁCH NƯỚC CHO KỲ THI**

Để tiến hành khôi phục từ bản sao lưu gia tăng, bạn cần bản sao lưu đầy đủ sau cùng và mọi băng từ sao lưu gia tăng kể từ bản sao lưu đầy đủ sau cùng đó.

### **Ảnh chụp nhanh (Snapshot)**

*Ảnh chụp nhanh* là một bản sao của một máy ảo tại một thời điểm cụ thể. *Ảnh chụp nhanh* được tạo ra bằng cách sao chép các tập tin lưu trữ máy ảo. Một trong những ưu điểm của máy ảo so với máy vật lý là máy ảo dễ dàng có thể được sao lưu và khôi phục - khả năng hoàn nguyên về ảnh chụp nhanh trước đó dễ dàng như nhấp vào một nút và đợi máy được khôi phục thông qua một sự thay đổi của các tập tin.

### **Khác biệt (Differential)**

Trong một bản *sao lưu khác biệt*, chỉ những tập tin đã thay đổi kể từ lần sao lưu đầy đủ cuối cùng được hoàn tất mới được sao lưu. Điều này cũng ngụ ý rằng một bản sao lưu đầy đủ theo định kỳ cần phải được hoàn

thành. Tần suất của bản sao lưu đầy đủ so với các bản sao lưu khác biệt tạm thời tùy thuộc vào tổ chức của bạn và cần phải nằm trong chiến lược đã xác định của bạn. Sự khôi phục từ bản sao lưu khác biệt đòi hỏi hai bước: bản sao lưu đầy đủ cuối cùng trước tiên cần được tải lên và sau đó bản sao lưu khác biệt sau cùng đã được thực hiện có thể được áp dụng để cập nhật các tập tin đã bị thay đổi kể từ khi tiến hành sao lưu đầy đủ. Một lần nữa, đây không phải là một quá trình khó khăn, nhưng nó sẽ khá tốn thời gian. Tuy nhiên, lượng thời gian để thực hiện sao lưu khác biệt định kỳ ít hơn nhiều so với sao lưu đầy đủ và đây là một trong những ưu điểm của phương pháp này. Rõ ràng, nếu một lượng thời gian đáng kể đã trôi qua giữa các bản sao lưu khác biệt hoặc nếu hầu hết các tập tin trong môi trường của bạn thay đổi một cách thường xuyên thì bản sao lưu khác biệt không khác nhiều so với bản sao lưu đầy đủ. Cũng cần phải hiểu rõ rằng để thực hiện sao lưu khác biệt, hệ thống phải có một phương pháp để xác định tập tin nào đã được thay đổi kể từ một số thời điểm nhất định. Bit lưu trữ không bị xóa trong một bản sao lưu khác biệt vì chìa khóa cho một sự khác biệt là sao lưu tất cả các tập tin đã thay đổi kể từ lần sao lưu đầy đủ cuối cùng.



**MÁCH NƯỚC CHO KỲ THI** Để thực hiện khôi phục từ bản sao lưu khác biệt, bạn cần bản sao lưu đầy đủ sau cùng và băng từ sao lưu khác biệt gần đây nhất.

Lượng dữ liệu sẽ được sao lưu và thời gian cần tiêu tốn để hoàn thành việc này có ảnh hưởng trực tiếp đến kiểu sao lưu nên được thực hiện. Bảng dưới đây phác thảo ba kiểu sao lưu cơ bản có thể được tiến hành, tổng không gian cần thiết cho từng kiểu, và mức độ dễ dàng để khôi phục bằng cách sử dụng từng chiến lược.

	<b>Đầy đủ</b>	<b>Khác biệt</b>	<b>Gia tăng</b>
Tổng không gian	Lớn	Trung bình	Trung bình
Khôi phục	Đơn giản	Đơn giản	Có liên quan

Có những thời điểm mà từng phương pháp này đều có ý nghĩa. Nếu bạn có một lượng lớn dữ liệu, nhưng phần lớn chúng là tĩnh (thay đổi chậm, nếu có) thì những thay đổi nhỏ nhất nên được ghi nhận lại bằng [sao lưu] khác biệt. Nếu toàn bộ cấu trúc dữ liệu đang thay đổi thì các bản sao lưu đầy đủ sẽ có ý nghĩa hơn. Việc hiểu được dữ liệu là một phần của chìa khóa để hiểu đúng cơ chế để sao lưu và khôi phục.

### **Băng từ**

Các băng từ là một hình thức cũ hơn của cơ chế lưu trữ dữ liệu, và chúng được đặc trưng bởi việc truy cập đọc/ghi tuần tự. Một đĩa cho phép bạn truy cập trực tiếp vào các phần tử cụ thể một cách ngẫu nhiên, trong khi một hệ thống băng từ lưu trữ mọi thứ trong một cấu trúc dài, yêu cầu bạn phải di chuyển băng về mặt vật lý nếu bạn muốn truy cập vào một phần tử nằm ở giữa chừng trong quá trình lưu trữ. Đối với mục đích lưu trữ chung, cơ chế truy cập tuần tự này có xu hướng tạo ra những vấn đề về hiệu suất đáng kể. Nhưng đối với sao lưu và khôi phục, các hoạt động này có tính chất tuần tự, và do đó băng từ vẫn rất thích hợp cho loại hoạt động này. Để lưu trữ số lượng lớn các bản sao lưu, băng từ vẫn là một giải pháp thay thế khả thi về chi phí và hiệu suất.

### **Ổ đĩa**

Thuật ngữ *đĩa* dùng để chỉ ổ cứng vật lý có các đĩa quay hoặc thiết bị bộ nhớ ở trạng thái thể-rắn. Việc sao lưu một đĩa là một hoạt động phổ biến đối với một máy tính vì hầu hết các máy tính đều có rất ít đĩa và đây là một cấu trúc hợp lý để duy trì và khôi phục. Đối với các máy tính cá nhân dựa trên máy khách, một quá trình sao lưu đĩa có thể có ý nghĩa và nhiều

hệ thống có thể thực hiện quá trình sao lưu đầy đủ, gia tăng, ảnh chụp nhanh hoặc khác biệt của một đĩa.

### **Sao chép**

Sao chép là hình thức sao lưu đơn giản nhất đối với một tập tin hoặc một tập hợp các tập tin. Người dùng có thể sử dụng tùy chọn này một cách dễ dàng, vì phạm vi của yêu cầu sao lưu dữ liệu của họ thường là khá nhỏ (ví dụ, việc lưu một bản sao của các tài liệu tối quan trọng hoặc một hình ảnh quan trọng nào đó). Tuy nhiên, phương pháp này vô hiệu khi phạm vi mở rộng thành các tập hợp dữ liệu lớn hơn và lớn hơn, và đối với các sao lưu phạm-vi-lớn, một trong số các phương pháp đã được đề cập trước đó sẽ có hiệu quả hơn đối với cả việc sao lưu lẩn khôi phục. Một trong những ưu điểm của việc người dùng tạo ra bản sao của các tài liệu quan trọng là khả năng khôi phục nhanh chóng khi sự kiện lỗi ghi đè xảy ra.

### **Lưu trữ được Gắn vào Mạng (NAS)**

*Lưu trữ được gắn vào mạng (NAS)* là việc sử dụng một kết nối mạng tới một thiết bị lưu trữ gắn ngoài đối với máy tính. Đây là phương pháp đơn giản để mở rộng khả năng lưu trữ, và kết nối có thể được quản lý qua một kết nối USB hoặc kết nối mạng Ethernet. Trong cả hai trường hợp, NAS là một phần mở rộng đơn giản của việc lưu trữ dữ liệu trên một hệ thống bên ngoài, và thông thường thì những thiết bị này không truyền tải dữ liệu đủ nhanh cho các hoạt động thường xuyên. Tuy nhiên, chúng hoạt động đủ tốt như một địa điểm bên ngoài cho các giải pháp sao-lưu-và-khôi-phục-dữ-liệu trên một phạm vi máy-đơn nhỏ hơn.

### **Mạng Khu vực Lưu trữ (SAN)**

Như đã được đề cập trước đây, mạng khu vực lưu trữ (SAN) là một mạng chuyên dụng kết nối các phần tử tính toán với các phần tử lưu trữ. Mạng này có thể được tối ưu hóa cho những kiểu lưu trữ dữ liệu cần thiết, v

kích thước và tốc độ dữ liệu, về định dạng và về tiêu chí truy cập. Việc sử dụng SAN như một phần của giải pháp sao lưu là một ví dụ điển hình về việc sử dụng công nghệ để giải quyết các vấn đề phức tạp. Nhiều máy chủ khác nhau trong toàn bộ doanh nghiệp có đều thể kết nối qua SAN tới một mảng sao lưu, cho phép sao lưu hiệu quả và hiệu quả theo cách thức linh hoạt và có thể quản lý được.



**MÁCH NƯỚC CHO KỲ THI** NAS là một thiết bị lưu trữ đơn lẻ phục vụ các tập tin qua mạng cho một máy. Đây là một hình thức lưu trữ bên ngoài đơn giản. Một SAN, nói cách khác, là một mạng bao gồm nhiều thiết bị được thiết kế để quản lý các tập hợp dữ liệu lớn và phức tạp theo thời gian thực ở tốc độ xử lý.

### Đám mây

Khi NAS và SAN có thể được sử dụng làm vị trí để lưu trữ các bản sao lưu dữ liệu thì đám mây cũng vậy. Rất nhiều nhà cung cấp và sản phẩm bảo mật sao lưu dựa-trên-đám-mây đặt bộ lưu trữ dữ liệu của một bản sao lưu trên đám mây. Ưu điểm bao gồm tất cả các ưu điểm của đám mây: ngoại biên, có thể có nhiều bản sao dự phòng và có sẵn qua Web để khôi phục. Các nhược điểm đều giống nhau: bản sao lưu nằm trên một hộp khác và nó chỉ được bảo vệ bởi thỏa thuận pháp lý giữa người dùng và nhà cung cấp sao lưu. Ngoài ra, các hợp đồng này có xu hướng ưu tiên nhà cung cấp sao lưu chứ không phải khách hàng. Vì vậy, mặc dù đám mây có thể dẫn đến việc ít phải quản trị dữ liệu tại-chỗ hơn, nhưng nó có thể làm gia tăng mối lo ngại về bảo mật vì một người khác đang bảo vệ dữ liệu, theo hướng dẫn của một tài liệu hợp đồng có thể phản ánh hoặc cũng có thể sẽ không phản ánh các tình huống rủi ro hiện tại.

Điều quan trọng là phải nhận ra rằng lưu trữ đám mây đã xâm chiếm máy tính để bàn của rất nhiều người dùng. Một loạt các nhà cung cấp đồng bộ hóa đám mây cơ bản bao gồm Dropbox, Box, Microsoft OneDrive, Google Drive và iCloud, cũng như nhiều thực thể ít được biết đến hơn. Việc hiểu được rủi ro liên quan đến dữ liệu trong những tình huống này là vấn đề quan trọng trong môi trường doanh nghiệp vì những gì có thể thuận tiện hoặc trông có vẻ như là một ý tưởng tốt từ quan điểm của người dùng có thể khiến cho dữ liệu có nguy cơ bị tiết lộ.

## Hình ảnh

Một bản sao lưu dựa-trên-hình-ảnh là một cấu trúc cụ thể của tập tin sao lưu để khớp với cấu trúc của hệ thống đang được sao lưu. Điều này có thể làm tiêu tốn nhiều thời gian và không gian [lưu tr] hơn, nhưng nó cũng đảm bảo không bỏ sót bất kỳ thứ gì vì nó sao lưu mọi thứ, bao gồm cả dữ liệu đã xóa và dung lượng trống. Đối với các hệ thống tối quan trọng, việc này cung cấp khả năng ghi nhận lại toàn bộ hệ thống như tại thời điểm sao lưu, bao gồm tất cả dữ liệu không nhất quán được liên kết với Hệ điều hành. Các sao lưu bằng hình ảnh có thể cung cấp thêm mức độ đảm bảo khi một số loại lỗi nhất định (ví dụ, do bị tấn công bởi phần mềm độc hại) khiến hệ thống không thể sử dụng được.

## Trực tuyến so với Ngoại tuyến

Các bản sao lưu trực tuyến là những bản sao lưu được lưu trữ trên một vị trí có thể truy cập được qua Internet. Điều này đem lại tính linh hoạt cho việc khôi phục bằng cách khiến cho dữ liệu sao lưu sẵn sàng ở bất kỳ nơi nào có kết nối mạng. Các bản sao lưu ngoại tuyến là những bản sao lưu được lưu trữ trên một hệ thống ngoại tuyến không thể truy cập được qua Internet. Sao lưu trực tuyến có lợi thế là mang lại sự tách biệt về địa lý của các bản sao lưu khỏi hệ thống gốc.

## Lưu trữ Ngoại biên

Các *bản sao lưu ngoại biên* là những bản sao lưu được lưu trữ trong một địa điểm tách biệt với hệ thống đang được sao lưu. Điều này có thể rất quan trọng đối với các vấn đề ảnh hưởng đến một khu vực có diện tích lớn hơn một phòng đơn. Hòa hoạn trong tòa nhà, một cơn bão, lốc xoáy - tất cả đều là những thảm họa xảy ra thường xuyên và thường ảnh hưởng đến nhiều hơn chỉ một căn phòng hoặc một tòa nhà. Việc có được các bản sao lưu ngoại biên làm giảm thiểu nguy cơ bị mất các bản sao lưu bởi cùng một vấn đề [*hàm ý chỉ việc bị mất toàn bộ các bản sao lưu đang được lưu trữ tại cùng một địa điểm với thiết bị và dữ liệu đang được sao lưu vì những nguyên nhân như thảm họa thiên nhiên, cháy nổ, v.v... - người dịch*]. Trong thế giới mạng tốc-độ-cao với các dịch vụ đám mây ngày nay, việc lưu trữ các bản sao lưu trên đám mây là một tùy chọn có thể giải quyết nhiều rủi ro và vấn đề liên quan đến tính sẵn sàng của bản sao lưu.

## Cân nhắc về Khoảng cách

*Khoảng cách* liên quan đến một bản sao lưu ngoại biên là một vấn đề về hậu cần. Nếu bạn cần phải khôi phục một hệ thống và bản sao lưu đang được lưu trữ cách đó vài giờ di chuyển bằng ô tô, điều đó sẽ làm tăng thời gian khôi phục. Sự chậm trễ do vận chuyển vật lý của các băng từ sao lưu đã được giảm bớt trong nhiều hệ thống thông qua các mạng truyền tải dữ liệu tại tốc độ của mạng. Khoảng cách cũng rất quan trọng khi kiểm tra tầm với [*phạm vi ảnh hưởng*] của một thảm họa. Điều quan trọng là vị trí ngoại biên phải đủ xa để không bị ảnh hưởng bởi sự cố tương tự. Điều này bao gồm vị trí thực tế của các máy chủ của nhà cung cấp dịch vụ lưu trữ đám mây. Ví dụ: nếu doanh nghiệp của bạn ở Puerto Rico và các máy chủ của nhà cung cấp dịch vụ đám mây của bạn cũng vậy thì cơn bão Maria có thể đã khiến dữ liệu của bạn trở nên không khả dụng trong một thời gian dài.

## **Không bền**

*Không bền* đề cập đến các mục hệ thống không cố định và có thể thay đổi. Ví dụ về một điều gì đó không bền là registry trong Microsoft Windows, là một danh sách động bao gồm các tiêu chí cấu hình. Tính không bền bỉ cần được quản lý một cách thích hợp và các hệ thống có đặc điểm này thường có các cơ chế được tích hợp để quản lý sự đa dạng này. Đối với các máy ảo, nơi trạng thái hiện tại của hệ thống liên tục thay đổi và do đó hình ảnh [của máy ảo] cũng thay đổi, chúng ta có các ảnh chụp nhanh (snapshot). Ảnh chụp nhanh cung cấp một bản sao của hệ thống tại một thời điểm mà sau đó bạn có thể tiếp tục sử dụng như là điểm khôi phục hoặc bản sao lưu.



## **MÁCH NƯỚC CHO KỲ THI**

Khi một hệ thống không bền bị lỗi, mọi dữ liệu sẽ bị mất. Khả năng phục hồi và khôi phục các điều kiện đó phải xảy ra từ các nguồn bên ngoài. Hãy nghĩ đến bộ nhớ khi bạn tắt máy tính, nó phải được tải lại khi bạn khởi động lại.

## **Hoàn nguyên về Trạng thái Đã biết**

Mọi thứ cuối cùng vẫn sẽ gặp sự cố, và khi có sự cố xảy ra, bạn sẽ muốn khôi phục lại về một điểm đã được biết. Việc có khả năng khôi phục về trạng thái đã biết được gọi là *hoàn nguyên về một trạng thái đã biết*. Hệ điều hành hiện đại là một ví dụ điển hình về tính không bền, chúng thường xuyên thay đổi với dữ liệu mới, phần mềm mới, cấu hình mới, trình điều khiển mới, v.v... Trong khi sao lưu dữ liệu có thể khôi phục lại các phần tử dữ liệu của hệ thống thì việc khôi phục cấu hình của hệ thống, bao gồm các tập tin của trình điều khiển và các bản vá lỗi phức tạp hơn nhiều. Làm thế nào để bạn khôi phục hệ thống sau khi bản vá lỗi gặp phải sự cố hoặc trình điều khiển mới gây ra một mức độ không ổn định? Rất nhiều hệ điều hành có khả năng quay trở lại một cấu hình đã

biết trước đó: cả máy chủ và máy tính để bàn đều có thể được quay ngược, khôi phục hệ thống về thời điểm trước đó trong khi vẫn giữ nguyên các tập tin - trở lại tình trạng mà trước đó hệ điều hành đã đang hoạt động bình thường.

### **Cấu hình Tốt-Đã-biết Gần nhất (Last Known-Good Configuration)**

Khi bạn có một hệ thống không hoạt động ổn định, bạn cần một phương tiện để khôi phục về một trạng-thái-tốt đã được biết. Khi khởi động không thành công, Microsoft Windows có thể cung cấp cho bạn một tùy chọn để hoàn nguyên về *cấu hình tốt-đã-biết gần nhất*, đây là một phương tiện hoàn nguyên về trạng thái đã được biết. Trong Windows 7, đây là một tùy chọn menu trực tiếp. Trong Windows 10, tùy chọn này được giấu trong hệ thống Khôi phục Windows. Các phương pháp truy cập vào nó sẽ khác nhau tùy thuộc vào loại vấn đề và vào việc liệu bạn có thể truy cập vào chính Windows hay không. Nếu Windows không thành công trong ba lần khởi động tiếp theo theo trình tự, nó sẽ cung cấp cho bạn các tùy chọn khôi phục thay vì cố gắng khởi động lại.

### **Phương tiện Khởi động Trực tiếp (Live Boot Media)**

Một phương tiện bắt đầu với một cấu hình đã biết và một trạng thái đã biết là khởi động từ một *phương tiện khởi động trực tiếp*, vốn là một đĩa flash hoặc nguồn DVD có thể khởi động được có chứa một hình ảnh có thể khởi động hoàn chỉnh của Hệ điều hành. Việc sử dụng điều này như một phương tiện để bắt đầu ở một trạng thái đã biết là điều phổ biến trong điều tra pháp y kỹ thuật số.

### **Tính Sẵn sàng Cao**

Một trong những mục tiêu của bảo mật là tính sẵn sàng của dữ liệu và năng lực xử lý khi người dùng được ủy quyền mong muốn. *Tính sẵn sàng cao* đề cập đến khả năng duy trì tính sẵn sàng của dữ liệu và hoạt động xử lý (các dịch vụ) bất chấp một sự kiện gây gián đoạn. Nói chung, điều

này đòi hỏi các hệ thống dự phòng, cả về mặt năng lực và xử lý, để từ đó, nếu một hệ thống bị lỗi, hệ thống kia có thể tiếp quản các hoạt động mà không có bất kỳ sự cố nào trong quá trình sử dụng. Tính sẵn sàng cao không chỉ là dự phòng dữ liệu, nó đòi hỏi cả dữ liệu và dịch vụ đều phải sẵn sàng.

---



**MÁCH NƯỚC CHO KỲ THI** Khả năng chịu lỗi và tính sẵn sàng cao là tương tự nhau trong các mục tiêu của chúng, nhưng chúng lại khác biệt trong cách ứng dụng. *Tính sẵn sàng cao* đề cập đến việc duy trì cả dữ liệu và dịch vụ ở trạng thái hoạt động, ngay cả khi xảy ra sự kiện gây ra gián đoạn. Khả năng chịu lỗi là một mục tiêu thiết kế để đạt được tính sẵn sàng cao nếu xảy ra lỗi.

### **Khả năng mở rộng**

*Khả năng mở rộng* là một thành phần thiết kế cho phép một hệ thống đáp ứng được khối lượng công việc lớn hơn bằng cách bổ sung thêm tài nguyên hoặc khiến cho phần cứng trở nên mạnh mẽ hơn (scaling up) hoặc thêm các nút bổ sung (scaling out). Thuật ngữ này thường được sử dụng trong các cụm máy chủ và cụm cơ sở dữ liệu, vì cả hai đều đều có thể có vấn đề về quy mô liên quan đến khối lượng công việc. Cả tính đàm hồi lẫn khả năng mở rộng đều có ảnh hưởng đến tính sẵn sàng và thông lượng của hệ thống, đây có thể là những vấn đề quan trọng liên-quan-đến-bảo-mật và rủi ro.

---



**MÁCH NƯỚC CHO KỲ THI** Tính đàm hồi và khả năng mở rộng trông có vẻ giống nhau nhưng thực ra, chúng khác nhau. *Tính đàm hồi* liên quan đến việc mở rộng quy mô động một hệ thống với khối lượng công việc

(scaling out) trong khi *khả năng mở rộng* là một thành phần thiết kế cho phép một hệ thống mở rộng quy mô đến phần cứng có năng lực hơn và mở rộng ra cho nhiều trường hợp hơn.

### **Thứ tự Khôi phục**

Các hoạt động khôi phục dữ liệu được thiết kế để lấy ra một bản sao thay thế của dữ liệu và đưa nó trở lại một hệ thống đang hoạt động. Nếu bạn sao lưu một cơ sở dữ liệu và sau đó cần sử dụng bản sao lưu để khôi phục cơ sở dữ liệu thì đây là khôi phục dữ liệu. Tuy nhiên, thứ tự khôi phục có thể sẽ tạo ra sự khác biệt. Nếu bạn có một cơ sở dữ liệu lớn cần nhiều ngày để sao lưu và khôi phục, thì việc có một giải pháp sao lưu cho phép bạn khôi phục các phần đã chọn cần thiết nhanh hơn có thể là một cứu cánh. Đây không chỉ là vấn đề về công nghệ, nó đòi hỏi việc lập kế hoạch và sự phối hợp vì dữ liệu quan trọng nhất cần phải được xác định và sau đó được sao lưu theo một cách thức để tạo điều kiện cho việc khôi phục nhanh chóng. Việc phát triển một kế hoạch khôi phục, cùng với thứ tự của những gì cần được khôi phục đầu tiên, thứ hai, v.v... là điều quan trọng vì việc này sẽ thúc đẩy một số hoạt động nhất định khi sao lưu dữ liệu ngay từ đầu.

### **Tính đa dạng**

Hầu hết các lỗi đều xuất phát từ một loạt các nguyên nhân phổ biến, có thể là do môi trường hoặc do thiết bị. Nếu bạn có một loạt các thiết bị giống nhau, ưu điểm là bạn có thể có phụ tùng thay thế cho các vấn đề thường được biết đến. Khuyết điểm là những vấn đề thường được biết đến này có xu hướng ảnh hưởng đến mọi hệ thống. Việc có một nền tảng độc canh bao gồm tất cả các hệ điều hành giống hệt nhau sẽ tăng thêm hiệu quả đối với việc vá lỗi, nhưng đồng thời nó cũng làm gia tăng thêm rủi ro trong các chế độ lỗi phổ biến trong toàn bộ doanh nghiệp. Sự đa dạng về công nghệ, nhà cung cấp, quy trình và biện pháp kiểm soát có

thể hỗ trợ khả năng phục hồi thông qua sự khác biệt trong các chế độ lỗi. Vi-rút gây hại cho một hệ điều hành thường không ảnh hưởng đến hệ điều hành khác. Việc xây dựng tính đa dạng trong các hệ thống để cho phép các hoạt động song song bằng cách sử dụng các công nghệ, nhà cung cấp, quy trình và các biện pháp kiểm soát khác nhau có thể mang lại một phương tiện để tiếp tục hoạt động ngay cả trong thời gian hệ thống gặp sự cố.

### Công nghệ

Ngành công nghiệp bảo mật có rất nhiều công nghệ có thể được sử dụng trong toàn bộ doanh nghiệp trong một nỗ lực giảm thiểu những rủi ro về mặt bảo mật. Qua việc sử dụng khái niệm phòng thủ theo chiều sâu, cách tốt nhất là không sử dụng một công nghệ duy nhất mà sử dụng nhiều công nghệ khác nhau theo kiểu chồng chéo, buộc kẻ tấn công phải vượt qua tất cả để đạt được mục tiêu của chúng. Việc có được tường lửa, các ACL, máy chủ pháo đài nằm trong mạng con được sàng lọc (DMZ) và giám sát mạng là một ví dụ về nhiều công nghệ được thiết kế để phát hiện các hoạt động mạng trái phép. Có được một tập hợp đa dạng bao gồm các yếu tố này cải thiện cơ hội bắt được kẻ tấn công, ngay cả khi chúng có thể đánh bại một hoặc hai yếu tố kiểm soát.

### Nhà cung cấp

Các nhà cung cấp khác nhau tiếp cận các vấn đề bảo mật bằng các phương pháp khác nhau, các bộ công cụ khác nhau, các chính sách và quy trình khác nhau cũng như các công nghệ khác nhau. Kẻ thù đã phát triển những phương pháp để đánh bại các nhà cung cấp khác nhau, nhưng nếu có nhiều nhà cung cấp cùng tham gia thì điều này khiến kẻ thù gặp phải những khó khăn hơn nhiều khi phải vượt qua tất cả các lựa chọn đã được sử dụng. Có được sự đa dạng trong các nhà cung cấp được sử dụng để

bảo mật ngăn chặn các hình thức điểm đơn lõi của nhà-cung-cấp-cụ-thể và tạo ra một tập hợp những năng lực phòng thủ mạnh mẽ hơn.

## Mã hóa

Để các giải pháp mã hóa hoạt động, cả hai bên phải đồng ý về thuật toán, khóa và các tham số khác, tuy nhiên, sự đa dạng vẫn có thể tồn tại trong môi trường này. Một ví dụ điển hình là trong bộ mật mã TLS, một tập hợp các giao thức mã hóa khác nhau, đã được chỉ định trước để tạo điều kiện cho tính linh hoạt trong việc thiết lập một kết nối. Khi bạn thiết lập kết nối được-TLS-hỗ-trợ, cả máy chủ và máy khách đều thương lượng về sự lựa chọn các tham số giao thức từ danh sách đã được chỉ định trước, cho phép một kết nối an toàn được thiết lập. Cùng một máy chủ với một máy chủ khác, thực hiện cùng một bài tập, có thể dẫn đến các lựa chọn mã hóa khác nhau, nhưng cuối cùng thì đó vẫn là một kết nối an toàn. Việc có được nhiều tùy chọn được định cấu hình và sẵn có cho phép loại bỏ một tùy chọn nếu có điều gì đó ảnh hưởng đến nó, trong khi vẫn cung cấp một phương tiện kết nối thông qua các tùy chọn thay thế.

## Các Biện pháp kiểm soát

Phòng thủ theo chiều sâu là một nguyên tắc bảo mật trong đó nhiều lớp cơ chế bảo mật khác nhau được sử dụng để đảm bảo việc ngăn chặn rủi ro. Đây là việc sử dụng tính đa dạng trong các biện pháp kiểm soát. Các mạng hiện đại không chỉ sử dụng tường lửa mà còn sử dụng mạng con được sàng lọc (DMZ), máy chủ pháo đài và ACL, tất cả đều hoạt động cùng nhau theo cách được phối hợp để khiến việc vượt qua toàn bộ các biện pháp kiểm soát là điều gần như không thể.



## MÁCH NƯỚC CHO KỲ THI

Đa dạng là việc có nhiều tập hợp các biện pháp kiểm soát khác nhau để cung cấp cho việc giảm thiểu rủi ro. Sự đa

dạng cần được thực hành ở mọi khía cạnh và được sử dụng để tăng cường yếu tố bảo mật. Một câu hỏi dựa-trên-hiệu-suất xem xét tính đa dạng nên được kiểm tra dựa trên yếu tố nào là hiệu quả nhất để xử lý - công nghệ, nhà cung cấp, mã hóa hoặc biện pháp kiểm soát - và câu trả lời sẽ được tìm thấy trong các chi tiết cụ thể của câu hỏi.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các khía cạnh của khả năng phục hồi an ninh mạng. Chương mở đầu bằng việc kiểm tra các yếu tố dẫn đến sự dự phòng, chẳng hạn như sự phân tán về địa lý; đĩa, bao gồm các giải pháp RAID và đa đường; dự phòng mạng từ các bộ cân bằng tải và gộp NIC; và các mối quan tâm về nguồn điện, bao gồm UPS, máy phát điện, nguồn cung cấp kép và PDU. Các vấn đề xung quanh việc nhân bản sử dụng cả SAN lẫn VM đã được đề cập, cũng như một so sánh về tại-chỗ và đám mây.

Chủ đề sao lưu cũng đã được đề cập, bao gồm các phương pháp sao lưu đầy đủ, gia tăng, ảnh chụp nhanh và khác biệt. Công nghệ sao lưu bao gồm, đĩa, sao chép, NAS, SAN, đám mây và hình ảnh cũng được trình bày. Một bài kiểm tra các vị trí sao lưu trực tuyến và ngoại tuyến đã được cung cấp, bao gồm cả việc lưu trữ ngoại biên và xem xét về khoảng cách.

Các vấn đề liên quan đến tính không bền, bao gồm hoàn nguyên về một trạng thái đã biết, cấu hình tốt đã biết gần nhất và phương tiện khởi động trực tiếp đã được đề cập. Tiếp theo là kiểm tra tính sẵn sàng cao và khả năng mở rộng cũng như trình tự khôi phục. Chương này đã kết thúc với việc xem xét về sự đa dạng và cách sử dụng sự đa dạng trong công nghệ, nhà cung cấp, mã hóa và các biện pháp kiểm soát để giảm thiểu rủi ro.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Chiến lược sao lưu nào chỉ bao gồm các tập tin và phần mềm đã được thay đổi kể từ lần sao lưu đầy đủ gần nhất?

  - A. Gia tăng
  - B. Đầy đủ
  - C. Ảnh chụp nhanh
  - D. Khác biệt.
2. Chiến lược sao lưu nào tập trung vào các bản sao của các máy ảo?

  - A. Gia tăng
  - B. Đầy đủ
  - C. Ảnh chụp nhanh
  - D. Khác biệt.
3. Khi thảo luận về vị trí lưu trữ các bản sao lưu, tuyên bố nào dưới đây là đúng (Chọn tất cả những đáp án đúng)?.

  - A. Bản sao gần đây nhất nên được lưu trữ ngoại biên, vì nó là bản mới nhất và do đó có giá trị nhất.
  - B. Lưu trữ ngoại biên nói chung là không cần thiết, ngoại trừ trường hợp khả năng xảy ra đột nhập tại cơ sở chính là rất cao.
  - C. Lưu trữ ngoại biên là một ý tưởng hay để bạn không bị mất bản sao lưu trong cùng một trường hợp đã khiến bạn mất dữ liệu hoạt động và do đó cần đến bản sao lưu.

- D.** Bản sao gần đây nhất có thể được lưu trữ cục bộ, vì nó có nhiều khả năng được cần đến nhất, trong khi các bản sao khác có thể được lưu giữ ở các địa điểm khác.
- 4.** Để đối phó với sự không bền trong một hệ thống, mục nào sau đây giúp giảm thiểu rủi ro? (Chọn tất cả các đáp án đúng).
- A.** Các bản sao lưu hình ảnh
  - B.** Đám mây
  - C.** Cấu hình tốt được biết đến gần nhất
  - D.** Hoàn nguyên về một trạng thái đã biết.
- 5.** Để sao lưu nhanh các tài liệu quan trọng của người dùng một cách dễ dàng, cách nào sau đây được khuyến nghị để sao lưu các mục này?
- A.** Khác biệt
  - B.** Ảnh chụp nhanh
  - C.** Sao chép
  - D.** NAS.
- 6.** Bạn có văn phòng tại sáu địa điểm trên toàn thị trấn và muốn sử dụng một phương pháp sao lưu và khôi phục phổ biến. Giải pháp nào hiệu quả nhất cho văn phòng nhỏ của bạn?
- A.** SAN
  - B.** NAS
  - C.** Đám mây
  - D.** Ngoại tuyến.
- 7.** Phát biểu nào sau đây là đúng về dự phòng?
- A.** Nó ngăn chặn các lỗi.
  - B.** Nó quá phức tạp và tốn kém để thực hiện.
  - C.** Nó chỉ áp dụng được cho phần cứng.
  - D.** Nó có thể được thực hiện trên nhiều hệ thống.
- 8.** Điều gì phân biệt các hệ thống có tính sẵn sàng cao?

- A.** Khả năng thay đổi theo điều kiện sử dụng
  - B.** Khả năng xử lý, ngay cả khi bị gián đoạn
  - C.** Các chức năng sao lưu và phục hồi được tự động hóa
  - D.** Sử dụng sự đa dạng để giảm thiểu các mối đe dọa đơn lẻ.
- 9.** Sự thay đổi liên tục của thông tin trong một hệ thống được gọi là gì?
- A.** Không bền
  - B.** Ảnh chụp nhanh
  - C.** Sự khác biệt
  - D.** Hình ảnh.
- 10.** Một PDU cung cấp quản lý những gì trong một doanh nghiệp?
- A.** Xử lý sao lưu dự phòng
  - B.** Phân phối điện cho các máy chủ
  - C.** Kết nối mạng được cải thiện để lưu trữ dữ liệu
  - D.** Cân bằng tải.

## Đáp án

1. **D.** Trong một bản sao lưu khác biệt, chỉ những tập tin và phần mềm đã thay đổi kể từ lần sao lưu đầy đủ cuối cùng đã được hoàn tất mới được sao lưu. Sao lưu gia tăng là một biến thể của bản sao lưu khác biệt, với điểm khác biệt là thay vì sao chép tất cả các tập tin đã thay đổi kể từ lần sao lưu đầy đủ cuối cùng, sao lưu gia tăng chỉ sao lưu các tập tin đã thay đổi kể từ lần sao lưu đầy đủ *hoặc* gia tăng lần dần gần đây nhất, vì vậy, đòi hỏi ít tập tin được sao lưu hơn. Trong một bản sao lưu đầy đủ, tất cả các tập tin và phần mềm được sao chép vào phương tiện lưu trữ. Ảnh chụp nhanh để cập đến các bản sao của máy ảo.
2. **C.** Ảnh chụp nhanh để cập đến các bản sao của máy ảo. Sao lưu gia tăng là một biến thể của bản sao lưu khác biệt, với sự khác biệt là thay vì sao chép tất cả các tập tin đã thay đổi kể từ lần sao lưu đầy đủ cuối cùng, sao lưu gia tăng chỉ sao lưu các tập tin đã thay đổi kể từ lần sao lưu đầy đủ *hoặc* gia tăng dần gần đây nhất, vì vậy đòi hỏi ít tập tin được sao lưu hơn. Trong một bản sao lưu đầy đủ, tất cả các tập tin và phần mềm được sao chép vào phương tiện lưu trữ. Trong một bản sao lưu khác biệt, chỉ các tập tin và phần mềm đã thay đổi kể từ lần sao lưu đầy đủ cuối cùng đã được hoàn tất mới được sao lưu.
3. **C và D.** Lưu trữ ngoại tuyến là một ý tưởng hay để bạn không bị mất bản sao lưu trong cùng một trường hợp khiến bạn mất dữ liệu hoạt động và do đó cần đến bản sao lưu. Ngoài ra, bản sao gần đây nhất có thể được lưu trữ cục bộ, vì nó có nhiều khả năng được cần đến nhất, trong khi các bản sao khác có thể được lưu giữ ở các địa điểm khác.
4. **A, C và D.** Các bản sao lưu hình ảnh ghi lại tính không bền (ổn định) của Hệ điều hành. Ngoài ra, việc hoàn nguyên về trạng thái

đã biết và sử dụng cấu hình tốt đã biết gần nhất đều có thể giải quyết các vấn đề về tính không bền. Đám mây (đáp án B) không phải là một câu trả lời trực tiếp, vì bản thân đám mây không mang lại tính bền bỉ cho một hệ thống không nhất quán. Một bản sao lưu hình ảnh có tất cả mọi thứ, vì vậy việc khôi phục từ nó có thể giải quyết sự cố về tính ổn định. Đối với đám mây có liên quan, nó sẽ là một mục thứ cấp (nghĩa là một nơi để lưu trữ một bản sao lưu hình ảnh), nhưng sau đó nó không thực sự tham gia trực tiếp.

5. **C.** Các bản sao do người-dùng-quản-lý trên phương tiện bên ngoài của các tài liệu quan trọng có thể giúp người dùng đầu cuối dễ dàng quản lý việc khôi phục một cách nhanh chóng.
6. **C.** Các giải pháp sao lưu đám mây có thể lý tưởng cho các văn phòng nhỏ và với các văn phòng khác nhau, có thể bổ sung thêm quản trị tập trung.
7. **D.** Một loạt các tùy chọn có liên quan đến việc tạo ra các hệ thống dự phòng - một số đơn giản như các phần tử cấu hình và các lựa chọn hệ thống.
8. **B.** Hệ thống có tính sẵn sàng cao tiếp tục xử lý dữ liệu ngay cả khi xảy ra các sự kiện gây ra gián đoạn.
9. **A.** Tính không bền (ổn định) đề cập đến các hạng mục hệ thống như bộ nhớ và các registry không ổn định và có thể thay đổi theo thời gian, ngay cả khi đang hoạt động.
10. **B.** Đơn vị phân phối điện cung cấp một phương tiện tập trung để quản lý và giám sát điện năng được phân phối đến các máy chủ trong tủ rack.

## Chương 14 Các Hệ thống Nhúng và Hệ thống Chuyên biệt

### Các Hệ thống Nhúng và Hệ thống Chuyên biệt

Trong chương này bạn sẽ

- Khám phá những tác động bảo mật của các hệ thống nhúng,
- Khám phá những tác động bảo mật của các thiết bị thông minh/IoT,
- Khám phá những tác động bảo mật của các hệ thống SCADA.

An ninh mạng không chỉ giới hạn trong các hệ thống CNTT trong doanh nghiệp. Một lượng đáng kể các hệ thống nhúng và hệ thống chuyên biệt tạo ra và sử dụng dữ liệu để có khả năng hoạt động. Những hệ thống này cũng đòi hỏi an ninh mạng nếu chức năng của chúng cần được bảo vệ khỏi rủi ro gây bất lợi. Chương này đề cập đến bản chất độc đáo của các hệ thống này và cách thức liên quan đến việc cung cấp sự bảo vệ cho chúng.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 2.6 của kỳ thi CompTIA Security+: Giải thích tác động bảo mật của các hệ thống nhúng và hệ thống chuyên biệt.

## Các Hệ thống Nhúng

Các *hệ thống nhúng* là tên gọi của các máy tính được đưa vào như một phần không thể thiếu của một hệ thống lớn hơn, thông thường được kết nối cứng. Từ các thiết bị ngoại vi như các máy in, đến các thiết bị gia dụng như TV thông minh và máy điều nhiệt, các hệ thống nhúng có mặt ở khắp mọi nơi. Hệ thống nhúng có thể đơn giản như một bộ vi điều khiển với các giao diện được tích hợp đầy đủ (một hệ thống trên một con chip) hoặc phức tạp như hàng chục hệ thống nhúng được kết nối với nhau trong một chiếc ô tô hiện đại. Hệ thống nhúng được thiết kế với một mục đích kiểm soát duy nhất và hầu như không có chức năng bổ sung, nhưng điều này không có nghĩa là chúng không có rủi ro hoặc những mối lo ngại về bảo mật. Phần lớn các hành vi khai thác bảo mật liên quan đến việc yêu cầu một thiết bị hoặc hệ thống làm điều gì đó mà nó có khả năng thực hiện và được thiết kế về mặt kỹ thuật để thực hiện, ngay cả khi chức năng kết quả không bao giờ là mục đích sử dụng của thiết bị hoặc hệ thống.

Các nhà thiết kế hệ thống nhúng thường tập trung vào việc tối thiểu hóa chi phí, với việc bảo mật hiếm khi được coi trọng như một phần của thiết kế hoặc triển khai. Bởi vì hầu hết các hệ thống nhúng hoạt động như một hệ thống bị cô lập nên rủi ro là không đáng kể. Tuy nhiên, khi năng lực [của các hệ thống nhúng] gia tăng và các thiết bị này được nối mạng với nhau, rủi ro đã tăng lên đáng kể. Ví dụ, các máy in thông minh đã bị tấn công như một cách xâm nhập vào doanh nghiệp và như một cách để ẩn nấp khỏi những người bảo vệ. Ngoài ra, khi những chiếc ô tô thế-hệ-tiếp-theo bắt đầu nói chuyện với nhau, việc chuyển lưu lượng và thông tin khác giữa chúng và bắt đầu có điều hướng và các đầu vào khác được đưa vào hệ thống, rủi ro sẽ tăng lên và an ninh sẽ trở thành một vấn đề. Điều này đã được chứng kiến trong ngành hàng không, nơi mà việc tách biệt

mạng Wi-Fi trên-máy-bay, giải trí trên-máy-bay và mạng kiểm soát chuyến bay kỹ thuật số trong buồng lái đã trở thành một vấn đề về an ninh.

### **Raspberry Pi**

*Raspberry Pi* là một máy tính có bo-mạch-đơn, chi-phí-thấp, rất thành công. Hàng triệu thiết bị này đã được đưa vào một loạt các ứng dụng - từ việc sử dụng bởi những người có sở thích đến các kỹ sư nguyên mẫu và thậm chí là các thành phần sản xuất trong một số trường hợp. Thiết bị tính toán có năng lực cao giá rẻ (dưới 50 đô-la Mỹ) này cung cấp rất nhiều tính năng và khả năng kết nối. Bộ vi xử lý ARM quadcore, RAM 8 GB, kết nối qua Ethernet, Bluetooth, USB, Wi-Fi 2,4 GHz và 5 GHz, cùng một loạt các tùy chọn kết nối cho màn hình, I/O và lưu trữ, tất cả khiến cho nền tảng này trở thành một nền tảng linh hoạt. Bảo mật *Raspberry Pi* cũng tương tự như bảo mật bất kỳ hệ thống nào khác. Người ta phải xem xét môi trường mà nó sẽ được triển khai, cách thức nó sẽ được kết nối với những người dùng khác, và những dữ liệu và thông tin nhạy cảm nào có liên quan. Ngoài ra, hãy nhớ rằng trong hầu hết các trường hợp, đây là một môi trường Linux đầy đủ đòi hỏi các quyền và các yếu tố bảo mật cơ bản khác.

Một máy *Raspberry Pi* đang chạy một dự án hội chợ khoa học không có kết nối với Web có phạm vi hoàn toàn khác với một máy *Raspberry Pi* được kết nối với Internet và được sử dụng để ghi dữ liệu nhạy cảm cần thiết cho quá trình sản xuất trong môi trường doanh nghiệp. Việc xác định các hồ sơ rủi ro và giải quyết chúng khi thích hợp vẫn là một nhiệm vụ cần thiết và quan trọng.

### **Field Programmable Gate Arrays (FPGAs)**

*Field Programmable Gate Arrays (FPGAs)* là các mạch điện tử được lập trình để thực hiện một chức năng cụ thể. Các thiết bị bán dẫn này dựa trên một ma trận các khối logic có thể thiết lập cấu hình (configurable).

logic blocks - CLB) được kết nối thông qua các kết nối qua lại có thể lập trình được và về bản chất, logic là được lập trình trước khi sử dụng. FPGA được thiết kế để được lập trình lại theo các yêu cầu chức năng mong muốn sau khi sản xuất và chúng thường có thể được lập trình lại khi các thiết kế của chức năng tiến triển. Mặc dù không nhanh bằng các mạch tích hợp dành-riêng-cho-ứng-dụng (application-specific integrated circuits - ASIC), được sản xuất tùy chỉnh cho các nhiệm vụ thiết kế cụ thể, khả năng lập trình và khả năng tái lập trình của FPGA mang lại sự linh hoạt đáng kể cho thiết kế. FPGA và ASIC được tìm thấy trong rất nhiều thiết bị tùy chỉnh, nơi không cần một máy tính hoàn chỉnh với hệ điều hành (OS) và tất cả những gì nó đòi hỏi là không cần thiết.

## **Andruino**

Arduino là một bộ vi điều khiển một bo-mạch-đơn, không phải là một máy tính chính thức như Raspberry Pi. Arduino đơn giản hơn, được thiết kế để cung cấp khả năng điều khiển máy tính cho các dự án phần cứng mà không cần phải tốn chi phí cho đầy đủ máy tính, hệ điều hành, v.v... Trong khi Raspberry Pi được thiết kế như một máy tính, Arduino được thiết kế như một bộ điều khiển, đặc biệt để giao tiếp với các cảm biến và thiết bị. Arduino có thể ứng phó ở các mức cảm biến và khởi động thiết bị dựa trên lập trình đã được tải vào thiết bị. Mã này hoạt động khi có nguồn điện, nếu bị mất nguồn, và sau khi được khôi phục, thiết bị có thể bắt đầu hoạt động trở lại - không giống như máy tính, thiết bị sẽ phải khởi động lại và bắt đầu lại. Việc mở rộng nền tảng Arduino được thực hiện thông qua một loạt bảng được gọi là lá chắn có thể bổ sung thêm chức năng cụ thể trong mạng, hiển thị, thu thập dữ liệu, v.v...



**MÁCH NƯỚC CHO KỲ THI** Hãy tìm hiểu môi trường tĩnh - các hệ thống mà trong đó phần cứng, hệ điều hành, ứng dụng và mạng được thiết lập cấu hình cho một chức năng hoặc mục đích cụ thể. Các hệ thống này được thiết kế để không thay đổi trong suốt vòng đời của chúng, hiếm khi đòi hỏi phải cập nhật.

### **Giám sát Kiểm soát và Thu thập Dữ liệu (SCADA)/Hệ thống Kiểm soát Công nghiệp (ICS)**

SCADA là từ viết tắt của *giám sát kiểm soát và thu thập dữ liệu*, một hệ thống được thiết kế để kiểm soát các hệ thống tự động trong môi trường mạng-vật-lý. Hệ thống SCADA có các thành phần thông minh của riêng chúng, mỗi thành phần là một ví dụ về một hệ thống nhúng. Cùng nhau, chúng tạo thành một hệ thống SCADA, có thể kiểm soát và điều khiển các nhà máy sản xuất, đèn giao thông, nhà máy lọc dầu, mạng lưới năng lượng, nhà máy nước, tự động hóa tòa nhà và kiểm soát môi trường, và một loạt các hệ thống khác. Một hệ thống SCADA còn được gọi là hệ thống kiểm soát phân tán (distributed control system - DCS) hoặc hệ thống kiểm soát công nghiệp (industrial control system - ICS), tùy thuộc vào ngành và cấu hình. Khi máy tính kiểm soát trực tiếp quy trình vật lý, một hệ thống SCADA có nhiều khả năng sẽ tham gia.

Hầu hết các hệ thống SCADA đều liên quan đến nhiều thành phần được nối mạng với nhau để đạt được một tập hợp các mục tiêu chức năng. Các hệ thống này thường bao gồm giao diện người - máy (human-machine interface - HMI), nơi nhân viên vận hành có thể thực hiện một hình thức kiểm soát mang tính chỉ thị đối với hoạt động của hệ thống đang được kiểm soát. Các hệ thống SCADA trong lịch sử đã bị cô lập với các hệ thống khác, nhưng sự cô lập đang giảm dần vì các hệ thống này đang được kết nối qua các mạng truyền thống để cải thiện các chức năng nghiệp vụ. Rất

nhiều hệ thống SCADA cũ đã bị cô lập khỏi hệ thống mạng công ty, nghĩa là chúng không chia sẻ kết nối mạng trực tiếp. Điều này có nghĩa là các luồng dữ liệu vào và ra được xử lý theo cách thủ công và cần nhiều thời gian để hoàn thành. Các hệ thống hiện đại đã loại bỏ ràng buộc này và bổ sung các kết nối mạng trực tiếp giữa mạng SCADA và mạng CNTT của doanh nghiệp. Những kết nối này làm gia tăng bề mặt tấn công và rủi ro cho hệ thống, chúng càng giống một hệ thống được nối mạng CNTT thì nhu cầu đối với các chức năng bảo mật càng lớn.

Các hệ thống SCADA đã được chú ý về mặt bảo mật với cuộc tấn công Stuxnet vào các cơ sở hạt nhân của Iran, được báo cáo ban đầu vào năm 2010. Stuxnet là phần mềm độc hại được thiết kế để tấn công một hệ thống SCADA cụ thể và gây ra lỗi, dẫn đến hư hỏng thiết bị của nhà máy. Cuộc tấn công này rất phức tạp và được thiết kế tốt, làm tê liệt quá trình xử lý nhiên liệu hạt nhân ở Iran trong một khoảng thời gian đáng kể. Cuộc tấn công này đã nâng cao nhận thức về những rủi ro liên quan đến hệ thống SCADA, cho dù có được kết nối với Internet hay không (Stuxnet đã vượt qua một lỗ hổng trên không để tấn công mục tiêu của nó).

### **Cơ sở vật chất**

Hệ thống SCADA được sử dụng rất nhiều trong các *cơ sở vật chất*, từ hệ thống tự động hóa hệ thống HVAC của tòa nhà, đến máy bơm áp lực nước, thang cuốn và thang máy, và hệ thống báo cháy - danh sách vẫn còn rất dài. Rất nhiều trong số các hệ thống này là những hệ thống độc lập, nơi dữ liệu được thu thập từ các cảm biến và được sử dụng cho một mục đích cụ thể (ví dụ, lập lịch trình thang máy căn cứ các nút trên các tầng). Những thứ khác, chẳng hạn như hệ thống kiểm soát ra vào tòa nhà, hệ thống cửa khóa/an toàn và hệ thống báo cháy, có thể được kết nối với nhau để đảm bảo an toàn trong các điều kiện cụ thể và an ninh trong các điều kiện khác. Một vài trong số các hệ thống này được kết nối qua

Internet để được giám sát hoặc điều khiển từ xa. Đối với tất cả các hệ thống, việc hiểu được cách truy cập vào hệ thống và bảo vệ các điểm truy cập chính là chìa khóa để đảm bảo kiểu triển khai SCADA này.

### Công nghiệp

Các cơ sở *công nghiệp* có một số nhu cầu tương tự như các cơ sở vật chất khác - máy tính kiểm soát các quy trình khác nhau, chẳng hạn như an ninh, giám sát môi trường, báo động cháy và hơn thế nữa. Yếu tố then chốt là phải hiểu được rằng hầu như bất kỳ cơ sở vật chất nào đều có hệ thống thu thập - phản hồi dữ liệu, cho dù đó là hệ thống HVAC đơn giản hoặc hệ thống điều nhiệt hay hệ thống phức tạp hơn như hệ thống giám sát hoặc báo cháy. Mỗi hệ thống này có thể hoạt động độc lập, được tích hợp một phần, tích hợp hoàn toàn với các hệ thống khác hoặc được kết nối với Internet, sự kết hợp gần như vô tận và được điều chỉnh để đáp ứng các yêu cầu của cơ sở.

### Sản xuất

Các hệ thống *sản xuất* bổ sung thêm một lớp quy trình do-máy-tính-kiểm-soát vào hỗn hợp công nghiệp/cơ sở vật chất - những quy trình của chính bản thân quy trình sản xuất thực tế. Các thiết bị sản xuất thường được điều khiển bằng máy tính, sử dụng các thiết bị như bộ điều khiển logic có thể lập trình (programmable logic controller - PLC), để thực hiện một bộ hướng dẫn dành riêng cho quy trình dựa trên các kết quả đọc của cảm biến và các thiết lập cơ cấu khởi động. Các hệ thống này có thể được phân biệt bằng một loạt các thuộc tính cụ thể, nhưng thuật ngữ SCADA cũng thường được sử dụng để bao hàm chúng.

Các hệ thống này có thể được kết nối với Internet hoặc có quyền truy cập từ bên ngoài đối với các nhà cung cấp bên thứ ba. Vì các hệ thống SCADA đang vận hành sản xuất của bạn thường rất quan trọng đối với doanh nghiệp của bạn, các hệ thống này cũng cần được bảo vệ khỏi những

kẻ tấn công. Thực tiễn tiêu chuẩn cho điều này là một trong những sự phân đoạn mạng nghiêm ngặt.

### Năng lượng

Các hệ thống *năng lượng* bao gồm từ điện đến hóa chất, dầu khí, đường ống, hạt nhân, năng lượng mặt trời, thủy nhiệt, và hơn thế nữa. Mỗi hệ thống này có nhiều hệ thống chịu sự kiểm soát của máy tính, thường sử dụng các loại thành phần SCADA giống như những loại khác đã được thảo luận. Trong trường hợp phân phối năng lượng, chẳng hạn như đường ống và điện, một vấn đề phức tạp nữa là bản chất phân tán của các yếu tố này, nơi chúng được trải rộng về mặt địa lý (rất nhiều trường hợp trong các cộng đồng của chúng ta). Sự phân bố các thành phần "nằm bên ngoài các bức tường của công ty" bổ sung một khía cạnh bảo mật vật lý độc nhất cho các hệ thống này.

### Hậu cần

Các hệ thống *hậu cần* là những hệ thống vận chuyển nguyên vật liệu từ điểm A đến điểm B. Những hệ thống này có thể liên quan đến vận tải biển, đường bộ (chẳng hạn đường giao thông và đường sắt), và đường hàng không. Có hai yếu tố cơ bản sẽ phải chịu sự kiểm soát: bản thân các hệ thống vận tải và nguyên vật liệu đang được vận chuyển.



**MÁCH NƯỚC CHO KỲ THI** Khi kiểm tra các hệ thống SCADA, bạn có ba điều cần phải quan tâm: giá trị của thông tin đang được bảo vệ, quyền truy cập vật lý vào hệ thống, và quyền truy cập luận lý (thường là mạng) vào dữ liệu. Khi kiểm tra các câu hỏi, hãy phân tích cú pháp của câu hỏi để biết chi tiết cụ thể về các vấn đề.

## Internet Vạn vật

*Internet vạn vật (IoT)* là một thuật ngữ được sử dụng để mô tả một loạt các thiết bị kết nối trực tiếp qua Internet để tạo ra một bộ cảm biến và hệ thống xử lý phân tán để thực hiện một chức năng cụ thể. Trái ngược với các thiết bị có mục đích chung, như máy tính và thiết bị mạng, các thiết bị IoT được xây dựng có mục đích, chúng được thiết kế để thực hiện một nhiệm vụ cụ thể. Tất cả các thiết bị này có một vài điểm tương đồng. Tất cả đều có giao diện mạng vì mục đích của chúng là kết nối với tư cách là thiết bị thông minh hoặc thành viên của câu lạc bộ Internet of Things. Trên giao diện mạng đó là một số hình thức nền tảng điện toán. Với chức năng máy tính hoàn chỉnh hiện đã được đưa vào hệ thống trên nền tảng một chip (sẽ được đề cập ở phần sau), những thiết bị nhỏ bé này có thể có một máy tính hoạt động hoàn chỉnh với chi phí chỉ vài đô la. Việc sử dụng nhân kiểng-Linux làm công cụ cốt lõi giúp cho việc lập trình trở nên dễ dàng hơn, vì cơ sở của các lập trình viên là rất lớn. Các thiết bị này cũng có thể được sản xuất hàng loạt với chi phí tương đối thấp. Việc mở rộng quy mô phát triển phần mềm trên hàng triệu đơn vị theo đúng nghĩa đen khiến cho chi phí có thể mở rộng quy mô. Chức năng là vua, có nghĩa là bảo mật hoặc bất kỳ thứ gì có thể ảnh hưởng đến chức năng mới được mở rộng phải nhường chỗ.

## Cảm biến

Các *cảm biến* là thiết bị đo lường một số thông số vật lý và trả về dữ liệu có thể được sử dụng bởi một hệ thống. Các cảm biến có vô số kích thước, hình dạng và các ràng buộc vật lý. Cảm biến có thể được sử dụng để đo nhiệt độ, áp suất, điện áp, vị trí, độ ẩm – và danh sách vẫn còn tiếp tục. Cảm biến có thể trả về dữ liệu dưới dạng tín hiệu số hoặc tín hiệu tương tự. Các cảm biến [tín hiệu] tương tự đòi hỏi sự chuyển đổi từ tín hiệu tương-tự-sang-kỹ-thuật-số trước khi dữ liệu có thể được sử dụng bởi một máy tính, mặc dù nhiều bảng giao diện thực hiện việc diễn dịch này một

cách tự động. Khi thiết kế một hệ thống, bạn cần xác định những gì cần phải được đo lường, trên phạm vi nào, và ở độ chính xác nào, cũng như môi trường và các điều kiện khác, tất cả những yếu tố này định hình nên đặc tả thông số kỹ thuật cho một cảm biến và xác định chi phí.

### **Thiết bị Thông minh**

Các *thiết bị thông minh* và thiết bị cấu thành nên IoT đã chiếm lĩnh thị trường của thế giới như một cơn bão. Từ những người bán hàng chịu trách nhiệm quan trọng có thể theo dõi vị trí của các mặt hàng qua GPS đến camera có thể cung cấp giám sát, đến các thiết bị gia dụng được kết nối, TV, máy rửa bát, tủ lạnh, chậu sành [vì từ này được viết thường nên không chắc chắn là nhãn hiệu của một loại nồi hầm thức ăn hay không – người dịch], máy giặt và máy sấy - bất kỳ thứ gì có bộ vi điều khiển giờ đây dường như đều được kết nối với Web để nó có thể được điều khiển từ xa. Trí tuệ nhân tạo (AI) cũng đã tham gia vào hỗn hợp, cho phép chức năng thậm chí còn lớn hơn, được thể hiện trong các sản phẩm như Amazon Echo, Google Home, Microsoft Cortana và Apple Siri. Công tắc đèn điều khiển bằng máy tính, bóng đèn LED, bộ điều nhiệt và màn hình giám sát em bé - ngôi nhà thông minh đã trở thành hiện thực, kết nối mọi thứ với Internet. Bạn có thể mang theo một chìa khóa mà cửa trước của bạn nhận ra, tự mở khóa trước khi bạn đi đến nó. Tất nhiên, camera an ninh nhìn thấy bạn đầu tiên và cảnh báo hệ thống rằng ai đó đang đến trên đường lái xe. Điều duy nhất có thể nói một cách tự tin về cuộc cách mạng này là ai đó sẽ tìm ra cách thức và lý do tại sao để kết nối hầu như mọi thứ với mạng.

### **(Các thiết bị) Có thể đeo trên người**

Các *thiết bị công nghệ có thể đeo được trên người* bao gồm mọi thứ, từ cảm biến sinh trắc học để đo nhịp tim, đến bộ đếm bước đo quãng đường đi bộ của một người, đến đồng hồ thông minh kết hợp tất cả các chức

năng này và hơn thế nữa. Bằng cách đo các tín hiệu sinh trắc học, chẳng hạn như nhịp tim và chuyển động của cơ thể, có thể đo được thể lực và thậm chí cả giấc ngủ. Các thiết bị đeo được này được chế tạo bằng các máy tính rất nhỏ chạy hệ điều hành theo thời gian thực, thường được xây dựng từ nhân Linux đã được rút gọn. Như với tất cả các thiết bị có chứa thông tin, làm cách nào để người ta bảo vệ được dữ liệu? Khi thiết bị đeo được ngày càng tìm hiểu nhiều dữ liệu cá nhân của bạn, chúng trở thành một nguồn quan tâm của tin tặc. Bảo vệ dữ liệu là mục tiêu bảo mật cho các thiết bị này.

Những việc bạn có thể làm để bắt đầu bảo vệ dữ liệu cá nhân của bạn bao gồm kiểm tra cài đặt mặc định, kiểm tra cài đặt quyền riêng tư, tắt theo dõi vị trí, đọc chính sách bảo mật và nếu có thể, sử dụng mật mã để bảo vệ thông tin cá nhân của bạn (PI).

### **Cơ sở vật chất Tự động hóa**

Các cảm biến chi-phí-thấp trong một gói IoT mang lại một số lợi thế, bao gồm nhưng không giới hạn, phân phối dữ liệu qua mạng, khả năng thu thập dữ liệu đáng kể và lợi thế về chi phí theo quy mô. Trong các cơ sở lớn, điều này có nghĩa là các hệ thống an ninh, HVAC, cảm biến cháy, v.v... có thể cung cấp phạm vi phủ sóng trên quy mô lớn, cho phép tự động hóa việc thu thập dữ liệu mà trước đây thường được thực hiện một cách thủ công thông qua một người đi bộ xung quanh. Tự động hóa không chỉ là hoạt động từ xa, các ứng dụng như hệ thống IFTTT (If This Then That) có thể ứng phó với các điều kiện thay đổi và sử dụng nhiều chỉ báo, bao gồm cả ngày và giờ. Tự động hóa có thể cải thiện rủi ro vì nó loại bỏ lỗi và cải thiện tốc độ phản ứng.

### **Điểm yếu Mặc định**

Bất cứ khi nào các mặt hàng được sản xuất hoặc sản xuất với số lượng lớn, các chuyên môn hóa cụ thể như thông tin xác thực mặc định là một

thách thức. Quy trình điển hình là có thông tin xác thực mặc định trên một thiết bị và sau đó mong đợi người dùng sẽ thay đổi chúng. Kỳ vọng này vào việc người dùng sẽ thay đổi thông tin đăng nhập thường dẫn đến bảo mật kém. Những *điểm yếu mặc định* là một điều kiện mà các điều kiện mặc định thường được biết đến, bao gồm tài khoản quản trị và mật khẩu, khiến cho hệ thống hoàn toàn dễ bị tấn công. Nhưng ngay cả khi mật khẩu đã được thay đổi, trong trường hợp số lượng lớn thiết bị được triển khai, có hợp lý không khi mong đợi tất cả chúng đều được thay đổi thông tin đăng nhập mặc định thành mật khẩu duy nhất? Một trong những thách thức của việc triển khai và bảo mật IoT là quản lý hàng nghìn hoặc hàng triệu thiết bị - và thông tin đăng nhập.



## MÁCH NƯỚC CHO KỲ THI

Internet vạn vật là tất cả về kết nối các mặt hàng chi phí thấp (tương đối) trên quy mô lớn. Việc triển khai hàng trăm, hàng nghìn và thậm chí hàng triệu thiết bị đã được thực hiện, và dữ liệu có thể cung cấp những thông tin chi tiết tuyệt vời mà chỉ có thể nhìn thấy với dữ liệu trên quy mô lớn. Tuy nhiên, quy mô đó đi kèm với sự thách thức trong việc quản lý và bảo mật số lượng rất lớn các thiết bị.

## Các Hệ thống Chuyên biệt

Như tên gọi chỉ ra, các *hệ thống chuyên biệt* là những hệ thống được thiết kế cho những mục đích đặc biệt. Có bốn kiểu hệ thống chuyên biệt được nhắm mục tiêu bởi CompTIA là các hệ thống trong thiết bị y tế, xe cộ, máy bay và đồng hồ đo thông minh. Mỗi một trong số các thể loại này đều có các hệ thống máy tính quan trọng cung cấp nhiều chức năng kiểm soát cho thiết bị, và mỗi hệ thống này đều có các vấn đề bảo mật của riêng mình.

## Các Hệ thống Y tế

Các *hệ thống y tế* là một nhóm rất đa dạng - từ các thiết bị cấy ghép nhỏ, chẳng hạn như máy điều hòa nhịp tim, đến các máy MRI nặng nhiều tấn. Nằm ở giữa là một loạt các thiết bị, từ những thiết bị đo những dấu hiệu quan trọng đến những thiết bị thực sự kiểm soát các chức năng quan trọng. Mỗi thiết bị trong số này có một số đặc điểm thú vị và tất cả chúng đều có một cảnh báo thú vị - chúng có thể ảnh hưởng trực tiếp đến cuộc sống của con người. Điều này khiến cho bảo mật của các thiết bị này cũng là một chức năng an toàn.

Các thiết bị y tế như thiết bị phòng thí nghiệm và máy bơm truyền dịch đã hoạt động theo các kiểm soát của máy tính trong nhiều năm. Tiêu chuẩn được lựa chọn là một nhân Linux đã được nhúng đã được loại bỏ các chức năng thừa và được đưa vào dịch vụ trong thiết bị nhúng. Một trong những vấn đề với cách tiếp cận này là làm thế nào để vá nhân Linux này khi các lỗ hổng được phát hiện. Một vấn đề khác có liên quan là khi hệ thống cơ sở được cập nhật lên phiên bản mới hơn, hệ thống nhúng vẫn còn mắc kẹt trên phiên bản cũ. Điều này đòi hỏi sự kiểm tra hồi quy cho các vấn đề, và hầu hết các nhà sản xuất sẽ không thực hiện những công việc đòi hỏi nhiều nhân công như vậy.

Các thiết bị y tế được sản xuất theo các hướng dẫn quy định nghiêm ngặt được thiết kế dành cho các hệ thống tĩnh không cần vá lỗi, cập nhật hoặc thay đổi. Bất kỳ thay đổi nào cũng sẽ buộc phải tái thẩm định - một quá trình kéo dài, tiêu tốn thời gian và tốn kém. Do đó, các thiết bị này có xu hướng không bao giờ được vá lỗi. Với sự xuất hiện của một số lỗ hổng nổi tiếng, bao gồm cả các cuộc tấn công Heartbleed và Bash shell, hầu hết các nhà sản xuất chỉ đơn giản khuyến cáo rằng các thiết bị này phải được cách ly và không bao giờ được kết nối với mạng bên ngoài. Về mặt khái niệm thì điều này là tốt, nhưng trên thực tế, điều này không bao giờ

có thể xảy ra, vì tất cả các mạng trong bệnh viện hoặc trung tâm y tế đều được kết nối với nhau.

Một vụ thu hồi gần nửa triệu máy điều hòa nhịp tim gần đây vào năm 2017 vì một lỗ hổng phần mềm có thể cho phép tin tặc truy cập và thay đổi các đặc tính hoạt động của thiết bị là bằng chứng của vấn đề. Tin tốt là các thiết bị có thể được cập nhật mà không cần gỡ bỏ chúng, nhưng nó sẽ cần một chuyến viếng thăm của bác sĩ để cài đặt firmware mới.

### Các Hệ thống Vận tải

Một *phương tiện xe* hiện đại không phải chỉ có một máy tính trong đó, mà thực sự là hàng trăm chiếc, tất cả đều được kết nối với nhau trên một bus. Bus mạng khu vực điều khiển (controller area network - CAN) được thiết kế để cho phép nhiều bộ vi điều khiển giao tiếp với nhau mà không cần một máy chủ trung tâm. Trước khi bus CAN được phát minh, các bộ vi điều khiển riêng lẻ được sử dụng để điều khiển động cơ, khí thải, truyền động, phanh, hệ thống sưởi, hệ thống điện và các hệ thống khác, và các bộ dây được sử dụng để kết nối mọi thứ trở nên cồng kềnh, khó sử dụng. Robert Bosch đã phát triển bus CAN dành cho xe ô tô, đặc biệt để giải quyết vấn đề về hệ thống dây điện, và khi được triển khai lần đầu tiên vào năm 1986 tại BMW, trọng lượng đã giảm được hơn 100 pound.

Kể từ năm 2008, tất cả các xe ô tô mới của Hoa Kỳ và Châu Âu đều phải sử dụng bus CAN, theo quy định của SAE – một sự bắt buộc kỹ thuật đã sẵn lòng được chấp nhận khi họ tiếp tục bổ sung ngày càng nhiều hệ thống phụ. Bus CAN có một đặc tả thông số kỹ thuật giao thức tham chiếu, nhưng những khám phá về tấn công tự động gần đây đã cho thấy một số điều thú vị. Đầu tiên, để bảo vệ những cáo buộc rằng một số phương tiện của mình có thể tăng tốc đột ngột mà không cần sự tác động của người lái, Toyota tuyên bố rằng cách duy nhất để khiến xe tăng tốc nhanh là đạp vào bàn đạp ga - chỉ phần mềm đó sẽ không làm được điều

đó. Tuy nhiên, điều này đã được chứng minh là sai. Tin tức đã chứng minh quyền kiểm soát gần như hoàn toàn đối với tất cả các chức năng của Toyota Prius bằng cách sử dụng các máy tính và các lệnh bus CAN. Thứ hai, mọi nhà sản xuất ô tô đã diễn giải/bỏ qua đặc tả thông số kỹ thuật của giao thức tham chiếu ở các mức độ khác nhau. Cuối cùng, như được chứng minh bởi tin tức tại DEF CON, có thể vô hiệu hóa một chiếc ô tô đang chuyển động, qua Internet, cũng như đánh lừa nó bằng cài đặt bảng điều khiển giải trí và các hệ thống khác.

Điểm mấu chốt là, để hoạt động một cách đúng đắn, các phương tiện mới hơn phải dựa vào nhiều hệ thống máy tính, tất cả đều hoạt động một-cách-bán-tự-động và bảo mật rất ít. Bộ Giao thông Vận tải Hoa Kỳ đang thúc đẩy công nghệ giao tiếp giữa-các-phương-tiện để các phương tiện có thể thông báo cho nhau khi giao thông đang thay đổi ngay trước mắt. Kết hợp điều đó với những tiến bộ trong công nghệ tự-lái và tầm quan trọng của bảo mật mạnh mẽ hơn trong ngành là rõ ràng. Có những bằng chứng cho thấy điều này đang bắt đầu, rằng vẫn đề bảo mật đang được cải thiện, nhưng tốc độ cải thiện còn chậm khi so sánh với tốc độ đổi mới máy tính điển hình.

### Các Hệ thống Máy bay

Máy bay cũng có một dấu vết máy tính đáng kể ở bên trong vì hầu hết các máy bay phản lực hiện đại đều có cái gọi là "buồng lái hoàn toàn bằng kính", nghĩa là các đồng hồ đo và công tắc riêng lẻ cũ kỹ đã được thay thế bằng một màn hình máy tính bao gồm cả một màn hình cảm ứng. Điều này cho phép chức năng nhiều hơn và đáng tin cậy hơn so với các hệ thống cũ. Nhưng giống như với các phương tiện giao thông, việc kết nối tất cả các thiết bị này với các bus sau đó cuối cùng được kết nối với các mạng bên ngoài đã dẫn đến rất nhiều nghi vấn về an ninh cho ngành hàng không. Và, cũng đúng như với các thiết bị y tế, việc vá lỗi hệ điều

hành cho hệ thống máy bay là một quá trình khó khăn vì ngành này được quy định rất nhiều, với những yêu cầu kiểm tra nghiêm ngặt. Điều này khiến cho các hệ thống, theo thời gian, sẽ trở nên dễ bị tấn công vì Hệ điều hành cơ sở đã được khám phá kỹ lưỡng và mọi lỗ hổng đã được lập bản đồ và khai thác trong các hệ thống phi-hàng-không, và các trường hợp sử dụng này có thể chuyển sang máy bay một cách dễ dàng.

Những tiết lộ gần đây đã chỉ ra rằng các hệ thống giải trí trên-chuyến-bay, trên các bản phân phối Linux tiêu chuẩn, được tách biệt khỏi hệ thống kiểm soát chuyến bay không phải bởi các mạng riêng biệt mà bởi một tường lửa. Điều này đã khiến tin tặc gióng lên hồi chuông cảnh báo về sự an toàn của vấn đề điện toán trong lĩnh vực hàng không.

### **Đồng hồ đo Thông minh**

*Đồng hồ đo thông minh* là tên gọi chung của cơ sở hạ tầng đo lường tiên tiến, một chương trình được khởi xướng bởi Bộ Năng lượng [Hoa Kỳ] nhằm cung cấp chức năng tự động hóa từ xa cho đồng hồ đo trong các tiện ích. Truyền thông hai-chiều theo thời-gian-thực, cơ sở hạ tầng máy tính để phân tích dữ liệu và một loạt các chính sách và thủ tục mới để tận dụng lợi thế của tự động hóa đã tạo ra một cuộc cách mạng trong hoạt động tiện ích. Đối với lĩnh vực điện năng, điều này có nghĩa là dữ liệu sử dụng theo thời-gian-thực (với độ chi tiết được đo bằng phút, không phải tháng như các lần đọc thủ công trước đây) cho phép khớp cung và cầu với hiệu quả cao hơn. Đối với tất cả các tiện ích, khả năng đọc đồng hồ đo, thay đổi dịch vụ, ngắt kết nối, kết nối lại và phát hiện và quản lý tình trạng mất điện giúp tiết kiệm chi phí và mức độ dịch vụ không bao giờ có với các đồng hồ đo được quản lý thủ công theo cách cũ. Việc quản lý việc triển khai trên quy mô lớn cơ sở hạ tầng theo cách thức an toàn đòi hỏi một thiết lập mã hóa mở rộng, với một số đồng hồ có nhiều mật khẩu cho các cấp độ vận hành khác nhau. Hãy nhân số này với hàng triệu đồng hồ

đo, và đây không phải là một nhiệm vụ tầm thường để quản lý. Tuy nhiên, có những gói phần mềm được thiết kế để tự động hóa các yếu tố này.



**MÁCH NƯỚC CHO KỲ THI** Các hệ thống chuyên biệt được xây dựng tùy biến để phục vụ cho một mục đích và mức độ bảo mật cần thiết đi cùng với mục đích đó. Nếu dữ liệu cần được bảo vệ, thì các vấn đề và giải pháp tương tự được sử dụng để khắc phục chúng sẽ được áp dụng. Trong hầu hết các hệ thống chuyên biệt, rủi ro là rất lớn và các giải pháp mã hóa được thiết kế vào hệ thống để hạn chế quyền truy cập cho người dùng được cấp phép.

### **Âm thanh thoại qua nền IP (VoIP)**

*Âm thanh thoại qua IP* - truyền tải thông tin liên lạc âm thanh thoại qua mạng IP - hiện là một phương thức cung cấp dịch vụ điện thoại phổ biến. VoIP khiến cho việc quản lý điện thoại trở nên dễ dàng như một ứng dụng trong doanh nghiệp, nhưng nó cũng mang đến những rủi ro và lỗ hổng bảo mật. Hệ thống VoIP đòi hỏi sự bảo vệ khỏi các cuộc tấn công dựa-trên-lưu-lượng tiêu chuẩn như từ chối dịch vụ, nhưng cũng cần được bảo vệ khỏi sự giả mạo. Giả sử bạn nhận được một cuộc điện thoại nội bộ từ bà Jones, giám đốc tài chính của công ty và màn hình của bạn cho biết "Ms. Jones,", nhưng làm thế nào để bạn biết được ai đang ở trên đường dây? Nếu bạn chưa từng nghe cô Jones nói trước đây bao giờ, liệu bạn có tin vào giọng nói, màn hình hay điều gì không? Xác thực và bảo vệ các kênh liên lạc đã là địa phận của công ty điện thoại, nhưng trong VoIP không có công ty điện thoại tổng thể để quản lý những rủi ro này.

Những rủi ro khác bao gồm những người bên ngoài sử dụng VoIP của bạn để kết nối để nhận các dịch vụ điện thoại quốc tế và cung cấp các cuộc gọi điện thoại miễn phí hoặc sử dụng dịch vụ điện thoại của bạn để thực hiện

cuộc gọi người máy cho mọi người. Cũng giống như chúng ta cần phải bảo mật các hệ thống như email từ bên ngoài, người dùng trái phép, chúng ta cũng cần làm như vậy với các dịch vụ VoIP.

### **Hệ thống Sưởi, Thông gió, Điều hòa Không khí (HVAC)**

Các hệ thống tự-động-hóa-tòa-nhà, hệ thống kiểm-soát-khí-hậu và hệ thống *HVAC* (*sưởi ấm, thông gió và điều hòa không khí*) đều là những ví dụ về hệ thống được quản lý bằng hệ thống nhúng. Mặc dù những hệ thống này từng là những hệ thống độc lập và không-phụ-thuộc nhưng sự gia tăng của siêu-kết-nối đã cho thấy giá trị trong việc tích hợp chúng. Việc có một “tòa nhà thông minh” giúp giảm thiểu việc sử dụng các nguồn lực của tòa nhà phù hợp với số lượng và sự phân bố của những người bên trong sẽ làm tăng hiệu quả và giảm chi phí. Việc kết nối các hệ thống này với nhau và bổ sung thêm các cơ chế kiểm soát trung tâm dựa-trên-Internet sẽ làm tăng hồ sơ rủi ro từ các cuộc tấn công từ bên ngoài. Những cuộc tấn công từ bên ngoài này có thể dẫn đến sự cố hoặc hỏng hóc của hệ thống HVAC, khiến cho một tòa nhà văn phòng lớn không thể ở được do nhiệt độ và sự an toàn.

Mặc dù không được dành riêng cho hệ thống HVAC theo một nghĩa nào đó, nhưng vụ tấn công năm 2014 của Target Corporation đã bắt đầu khi một nhà cung cấp HVAC bị xâm nhập, dẫn đến việc xâm nhập vào mạng của Target và quyền truy cập vào mạng các điểm-bán-hàng của nó. Câu chuyện về vụ tấn công đã gây ra ồn ào và tiêu tốn của Target hàng trăm triệu đô la và dẫn đến một số thay đổi ở cấp quản lý điều hành đáng kể. Nhà cung cấp dịch vụ bảo mật đám mây Qualys cho biết, các nhà nghiên cứu của họ đã phát hiện ra rằng hầu hết trong số khoảng 55.000 hệ thống HVAC được kết nối với Internet trong hai năm qua đều có những lỗ hổng có thể dễ dàng bị khai thác bởi các tin tặc.

## Drones

Máy bay không người lái (drone), hoặc thiết bị bay không người lái (unmanned aerial vehicles - UAV), đại diện cho lĩnh vực tiếp theo của chuyến bay. Những chiếc máy này có nhiều loại từ máy bay không người lái nhỏ mà những người có sở thích có thể chơi với giá dưới 300 đô la đến máy bay kích thước với đầy đủ có thể bay qua những đại dương. Điều khiển cho các hệ thống này trở nên khác biệt so với máy bay thông thường là phi công đang ở trên mặt đất, điều khiển thiết bị bay thông qua bộ điều khiển từ xa. UAV có các camera, cảm biến và bộ xử lý để quản lý thông tin, và ngay cả những phiên bản đơn giản dành cho người yêu thích cũng có chức năng lái tự động tinh vi. Do kết nối từ xa, các UAV được kết nối mạng và vận hành dưới sự điều khiển trực tiếp bằng sóng vô tuyến (hiếm gặp) hoặc thông qua hệ thống nối mạng (phổ biến hơn nhiều).

## Máy in Đa chức năng (MFPs)

Các máy in đa chức năng (MFP), sự kết hợp máy in, máy quét và máy fax, có năng lực tính toán được nhúng để hoạt động như một máy chủ in ấn, quản lý quá trình in hoặc quét thực tế và cho phép kết nối mạng hoàn chỉnh. Những thiết bị này giao tiếp theo kiểu hai chiều, chấp nhận lệnh in và gửi lại trạng thái lệnh, trạng thái máy in và các thông tin khác đến máy tính. Điều này đã tách chức năng in ra khỏi máy tính, khiến máy in trở thành một thực thể độc lập. Hệ thống chạy tất cả các chức năng này đã được thiết kế để cung cấp chức năng tối đa cho thiết bị và bảo mật là yếu tố được nghĩ đến sau các yếu tố thiết kế. Do đó, các thiết bị này đã được chứng minh là có thể tấn công và có khả năng lan truyền phần mềm độc hại từ máy in sang máy tính. Những cuộc tấn công này vẫn tồn tại chủ yếu như một bằng chứng về khái niệm trái ngược với một mối đe dọa trong thế giới thực, điều này thật may mắn [hàm ý rằng việc biết được sự tồn tại của các cuộc tấn công vào máy in là điều may mắn], vì thế hệ

phần mềm bảo mật hiện tại đã không giám sát hoạt động in ấn đến và đi từ máy tính.

### **Hệ điều hành Thời gian Thực (RTOSs)**

*Hệ điều hành thời-gian-thực (RTOS)* được thiết kế cho các thiết bị khi mà quá trình xử lý phải diễn ra theo thời gian thực và dữ liệu không thể được xếp vào hàng đợi hoặc lưu vào bộ đệm trong bất kỳ khoảng thời gian đáng kể nào. RTOS không phải là máy có mục đích chung chung mà được lập trình cho một mục đích cụ thể. Chúng vẫn phải đối phó với sự tranh chấp và chúng có các thuật toán lập lịch trình để ứng phó với các xung đột về thời gian, nhưng nói chung một RTOS xử lý từng đầu vào khi nó được nhận hoặc trong một lát cắt thời gian cụ thể được xác định là thời gian phản hồi. Các ví dụ về RTOS bao gồm từ những thứ phổ biến như hệ thống máy tính chống bó cứng phanh trên ô tô đến những thứ phức tạp như hệ thống robot được sử dụng trên dây chuyền lắp ráp.

Hầu hết các hệ điều hành máy tính có mục-đích-chung đều có khả năng đa nhiệm theo thiết kế. Điều này bao gồm cả Windows và Linux. Các hệ thống đa nhiệm khiến cho bộ xử lý thời-gian-thực trở nên kém cỏi, chủ yếu là do chi phí liên quan đến việc tách các tác vụ và tiến trình. Windows và Linux có thể có các ngắt, nhưng đây là ngoại lệ chứ không phải là quy luật đối với bộ xử lý. Phần mềm dựa-trên-RTOS được viết theo một kiểu hoàn toàn khác, được thiết kế để nhấn mạnh vào luồng đang xử lý thay vì xử lý đa luồng.

Tác động bảo mật xoay quanh các hệ điều hành thời-gian-thực nằm ở chỗ thời gian của chúng. Nếu một sự kiện thực hiện điều gì đó gây cản trở khả năng phản hồi của hệ thống trong khoảng thời gian được phân bổ thì bản thân hệ thống có thể không thực hiện được nhiệm vụ của mình. Hệ điều hành thời-gian-thực cũng có xu hướng cụ thể ở mức độ mà các bản cập nhật và bản vá có xu hướng không được phổ biến, vì nhà sản xuất hệ

thống không cung cấp mức hỗ trợ đó. Khi các mặt hàng như ô tô được kết nối mạng nhiều hơn, những điểm yếu này đang trở nên rõ ràng và người ta có thể kỳ vọng tình trạng này sẽ thay đổi theo thời gian.



**MÁCH NƯỚC CHO KỲ THI** Các hệ thống VoIP, HVAC, máy bay không người lái/UAV, và các hệ thống giám sát đều có một điểm yếu chung: truy cập được qua Internet. Véc-tơ tương tự có thể được sử dụng để chống lại bất kỳ hệ thống được kết nối nào, và nếu không có biện pháp bảo vệ, chúng thường sẽ là các hệ thống không được bảo mật. Chúng phải được kết nối để hoạt động, và do đó, chúng cần được bảo vệ ở mức cơ bản như mật khẩu.

### **Hệ thống trên một con chip (SoC)**

*Hệ thống trên một con chip (SoC)* đề cập đến một hệ thống máy tính hoàn chỉnh được thu nhỏ trên một mạch tích hợp duy nhất, được thiết kế để cung cấp đầy đủ chức năng của một nền tảng máy tính chỉ trên một con chip duy nhất. Điều này bao gồm cả việc kết nối mạng và hiển thị đồ họa. Một số giải pháp SoC đi kèm với bộ nhớ, trong khi những giải pháp khác có bộ nhớ riêng biệt. Các SoC rất phổ biến trên thị trường máy tính di động (cả điện thoại và máy tính bảng) vì mức tiêu thụ điện năng thấp và thiết kế hiệu quả. Một số thương hiệu SoC đã trở thành cái tên quen thuộc bởi vì các công ty điện thoại di động đã quảng cáo sự bao gồm của chúng trong một hệ thống, chẳng hạn như bộ vi xử lý Snapdragon trong các thiết bị Android. Các hệ thống SoC lõi tứ và lõi tám đã sẵn sàng, và chúng thậm chí còn có các thiết kế tiên tiến như quad plus one, trong đó bộ xử lý thứ năm chậm hơn và được thiết kế cho các quy trình đơn giản và sử dụng lượng điện năng cực kỳ nhỏ. Vì vậy, khi các lõi tứ không cần thiết, sẽ không sử dụng năng lượng đáng kể.

Việc lập trình các hệ thống SoC có thể xảy ra ở một số cấp độ khác nhau. Các hệ điều hành và ứng dụng chuyên dụng có thể được viết cho chúng, chẳng hạn như Android fork của Linux, dành riêng cho thị trường thiết bị di động. Bởi vì những thiết bị này đại diện cho nền tảng máy tính với hàng tỷ thiết bị trên toàn thế giới, chúng đã trở thành một thế lực đáng kể trên thị trường. Các tác động bảo mật của các hệ thống dựa-trên-SoC không liên quan đến các chi tiết cụ thể của SoC, mà trên thực tế là chúng có mặt khắp nơi trong cuộc sống do-công-nghệ-điều-khiển của chúng ta. Các vấn đề bảo mật được xử lý bởi thiết bị, không phải bởi bản thân khía cạnh SoC cụ thể.

### **Những cân nhắc về Giao tiếp**

Các hệ thống nhúng và hệ thống chuyên biệt hữu ích cho một mục đích, và nhiều khi những mục đích đó yêu cầu thông tin liên lạc qua mạng cho những tài nguyên khác. Các *cân nhắc về giao tiếp* đối với các hệ thống nhúng và hệ thống chuyên biệt phụ thuộc vào dịch vụ, nhiệm vụ mà nó đang thực hiện và các tài nguyên cần thiết. Các phương pháp giao tiếp rất rộng và đa dạng, và sự lựa chọn thường phụ thuộc vào phạm vi cần thiết và đối tượng cần giao tiếp. Đối với liên lạc nội hạt, cự-ly-ngắn, một số công nghệ nhất định có thể vượt trội. Đối với thông tin liên lạc trên toàn thế giới, những công nghệ khác sẽ hoạt động tốt hơn. Việc áp dụng công nghệ đã được sử dụng bởi người dùng cũng có những lợi thế, chẳng hạn, tại sao lại sử dụng mạch vô tuyến đặc biệt trong môi trường đã có Wi-Fi?

### **5G**

5G là mạng di động dựa-trên-vô-tuyến thế hệ mới nhất. Nó được thiết kế để kết nối hầu như tất cả mọi người và mọi thứ với nhau, bao gồm máy móc, đồ vật và thiết bị, tập trung vào tốc độ dữ liệu và băng thông cao hơn. Các mạng 5G không chỉ là những đường ống lớn hơn, tiêu chuẩn có

nhiều yếu tố chức năng để cải thiện cả hiệu suất lẫn hiệu quả. 5G đang trong quá trình triển khai trên toàn thế giới và kết nối thông qua một mạch di động - điện thoại, modem hoặc chipset được thiết kế trong một sản phẩm.

Giống như việc có một máy chủ toàn diện là điều quá mức cần thiết đối với một cảm biến đơn giản, 5G có thể quá mức cần thiết cho nhiều nhu cầu giao tiếp. Nếu phạm vi toàn cầu, băng thông lớn và độ trễ thấp là quan trọng, thì 5G có thể được bảo đảm, nhưng nếu không, vẫn có những lựa chọn thay thế có chi phí thấp hơn.

### **Vô tuyến Băng tần-Hẹp**

Giao tiếp *vô tuyến băng-tần-hẹp* sử dụng các dải tần số hẹp cho truyền thông tốc-độ-dữ-liệu-thấp. Mặc dù tốc độ dữ liệu thấp trông có vẻ như là một vấn đề lớn, nhưng không phải tất cả các hệ thống đều có nhu cầu về tốc độ dữ liệu cao và vô tuyến băng tần hẹp mang lại lợi thế về phạm vi và mức sử dụng điện năng. Máy phát tín hiệu công-suất-thấp-hơn là bình thường, và cũng có phạm vi dài hơn đáng kể. Vì vậy, nếu một công ty có nhiều giàn khoan trên một khu vực địa lý rộng lớn và cần di chuyển lượng dữ liệu tương đối nhỏ giữa chúng, thì radio băng-tần-hẹp có thể là giải pháp lý tưởng.

### **Vô tuyến Băng tần cơ sở**

*Băng tần cơ sở* đề cập đến băng thông ban đầu được tạo ra bởi một tín hiệu. Đối với tín hiệu âm thanh điển hình, nó là 20 - 20.000 Hz. Đối với một tín hiệu được truyền qua mạch vô tuyến, nó thường được mã hóa hoặc điều chỉnh theo cách mà sau đó có thể được hòa trộn với sóng vô tuyến, mang thông tin về những thay đổi trên sóng vô tuyến. *Vô tuyến băng tần cơ sở* đề cập đến tín hiệu đang được truyền đi và đại diện cho một kênh liên lạc duy nhất. Vô tuyến băng thông rộng là khi nhiều tín hiệu được đóng gói lại với nhau để truyền tải và thiết bị thường là càn

thiết để tách các giao tiếp riêng lẻ. Theo thiết kế, vô tuyến băng tần cơ sở rất đơn giản, vì nó chỉ mang một kênh duy nhất để quản lý thông tin liên lạc.

### **Thẻ Mô-đun Nhận dạng Người thuê bao (SIM)**

Một *thẻ mô-đun nhận dạng thuê bao (SIM)* là một thiết bị được sử dụng để chứa thông tin quan trọng cần thiết để thực hiện truyền thông giao tiếp qua các mạng viễn thông. Thẻ SIM cung cấp một phương tiện nhận dạng người dùng và các mục thông tin quan trọng khác khi sử dụng mạng viễn thông. Khi truy cập vào một mạng viễn thông, một người phải xác định chính bản thân họ cho các mục đích thanh toán. Thẻ SIM cung cấp thông tin mà mạng cần để phân bổ cuộc gọi. Các phần tử như nhà cung cấp, số sê-ri và khóa được lưu trữ trên một thẻ mạch tích hợp đa năng hoạt động như một tiêu chuẩn để lưu trữ và quản lý thông tin này trên các thiết bị. Thẻ SIM rất quan trọng vì chúng có thể chứa dữ liệu người dùng và thông tin xác thực cũng như cung cấp các dịch vụ nhận dạng. Khi người ta di chuyển thẻ SIM từ điện thoại này sang điện thoại khác, phần cứng mới sẽ hoạt động giống như phần cứng cũ về khả năng kết nối và ở một mức độ nào đó, là dữ liệu đã được lưu trữ.

### **Zigbee**

*Zigbee* là dịch vụ vô tuyến lưới công-suất-thấp được sử dụng để kết nối các cảm biến và các thiết bị cơ bản.



**MÁCH NƯỚC CHO KỲ THI** Nhu cầu giao tiếp là điều phổ biến giữa rất nhiều thiết bị, nhưng các phương pháp sẽ khác nhau. Việc hiểu được những hạn chế của các phương pháp khác nhau và các tùy chọn bảo mật là điều rất quan trọng.

## Các Ràng buộc

Các hệ thống nhúng và hệ thống chuyên biệt có tập hợp những yếu tố ràng buộc khác nhau mà chúng đã được thiết kế để hoạt động trong phạm vi những ràng buộc đó. Những ràng buộc điển hình đối với các thiết bị này bao gồm các hạn chế về nguồn điện, năng lực tính toán, thông lượng và băng thông mạng, mã hóa và chi phí. Những vấn đề bổ sung trong các hạng mục như xác thực và tin cậy cũng có thể là các yếu tố thúc đẩy. Khi những thiết bị này được chế tạo vì một mục đích cụ thể, các ràng buộc này là các yếu tố thiết kế thực tế và là một phần của khả năng của hệ thống để thực hiện nhiệm vụ của nó trong môi trường mong đợi.

## Năng lượng

Các mạch điện tử lấy *năng lượng* (*nguồn điện*) để hoạt động và năng lượng này đến từ một trong số các nguồn sau: một nguồn điện được kết nối với lưới điện, pin, năng lượng mặt trời hoặc một loại thiết bị khác. Năng lượng là một yếu tố thúc đẩy then chốt trong nhiều hệ thống nhúng và hệ thống chuyên biệt bởi vì nó là một giới hạn thực sự. Khi nguồn điện bị ngắt và không có nguồn điện dự phòng, thiết bị sẽ ngừng hoạt động. Pin lithium-ion có thể nạp lại đã được một chặng đường dài trong vài năm qua và đối với các thiết bị di động, chúng chính là nguồn cung cấp [năng lượng] chính. Năng lượng thúc đẩy rất nhiều yếu tố thiết kế bởi vì các chức năng bổ sung không cần thiết, bao gồm cả tốc độ, chỉ tiêu tốn năng lượng và không bổ sung thêm chức năng của thiết bị.

## Điện toán

Năng lực *tính toán* của các hệ thống nhúng và hệ thống chuyên biệt là một thành phần quan trọng khác phù hợp với nhiệm vụ mà thiết bị được thiết kế để thực hiện. Hiệu suất tính toán là một trong những yếu tố chính trong phương trình công suất và dung lượng tính toán vượt mức dẫn đến việc tiêu hao nhiều năng lượng hơn và thời gian sử dụng pin kém hơn. Các bộ vi điều khiển, mảng cổng có thể lập trình trường (FPGA) và

mạch tích hợp dành riêng cho ứng dụng (ASIC), tất cả đều đã được thảo luận trước đó trong chương, là những tùy chọn hợp lý cho phân đoạn tính toán của thiết kế và mỗi loại này đều có một loạt năng lực. Từ các bộ vi điều khiển nhỏ bé có kích thước bằng hạt gạo với khả năng rất hạn chế đến các ASIC được thiết kế để xử lý hình ảnh/lidar [*một loại ra-đa phát sáng từ tia laser*] trong ô tô tự-lái hiện đại, phạm vi của năng lực là rất rộng. Điểm mấu chốt cần ghi nhớ là năng lực tính toán, công suất nguồn và tuổi thọ hữu ích mà nếu không có nguồn năng lượng từ bên ngoài đều bị khóa trong một trận chiến, mỗi bên sẽ lấy từ hai bên còn lại [*hàm ý nếu không có nguồn năng lượng từ bên ngoài, để tăng một trong ba yếu tố sẽ bắt buộc giảm hai yếu tố còn lại*].

## Mạng

Các hạn chế về *mạng* là do hạn chế từ nguồn điện và từ kết nối. Nếu không có kết nối trực tiếp, hệ thống mạng yêu cầu phải có bộ thu phát sóng vô tuyến và điều này làm gia tăng nhu cầu về điện năng. Do đó, nơi nào cần kết nối mạng, nó sẽ phải gánh chịu chi phí. Có một loạt các phương pháp khác nhau được sử dụng để kết nối mạng, và phương pháp được chọn sẽ là giải pháp rẻ nhất và tốt nhất đối với nhu cầu mạng đang hiện diện tại thời điểm thiết kế hệ thống.

Bỏ lại các cân nhắc về đơn-vị-riêng-lẻ sang một bên, mạng là thành phần giá trị then chốt đứng đằng sau cuộc cách mạng Internet of Things. Tiện ích của năng lực mạng liên quan đến một hàm số mũ liên quan đến số lượng các nút mạng. Do đó, nếu số lượng nút càng lớn, tiện ích càng lớn và sự tăng trưởng này có tính chất cấp số nhân. Các triển khai lớn hơn (hãy nghĩ về đồng hồ đo thông minh trong một khu vực đô thị lớn) cung cấp một lượng lớn dữ liệu thông qua mạng đến trung tâm dữ liệu một cách thường xuyên và kịp thời. Việc quản lý các luồng dữ liệu lớn đặt ra một gánh nặng cho địa điểm trung tâm, nếu địa điểm này không được lập

kế hoạch và vận hành một cách đúng đắn sẽ trở thành một hạn chế đối với hoạt động tổng thể của toàn hệ thống.

### Các chức năng Mã hóa

Các *chức năng mã hóa* có thể rất cần thiết để bảo mật dữ liệu trong quá trình truyền tải, nhưng đi cùng với chức năng này là chi phí. Mức độ tài nguyên tính toán cho các chức năng mã hóa có thể là rất đáng kể, do đó, trở thành một hạn chế đối với hệ thống tổng thể. Các thuật toán mã hóa hạng nhẹ đang được phát triển để giải quyết một cách cụ thể những thách thức này và chúng được đề cập trong Chương 16, "Các khái niệm Mã hóa".

### Không có khả năng Vá lõi

Việc *không có khả năng vá lõi* một thành phần đại diện cho một rủi ro bảo mật và một hạn chế. Điều này thường có nguyên nhân xuất phát từ một loạt các quyết định thiết kế dựa trên việc sản xuất các mặt hàng không phải là máy tính mà thay vào đó là các thiết bị phục vụ mục-dích-đuy-nhất. Mặc dù các Raspberry Pi và Arduino có thể nhận được các bản vá lõi từ các nhà phát triển của chúng, nhưng bộ điều khiển được nhúng trong camera giám sát hoàn toàn lại là một câu chuyện khác. Nói một cách đơn giản, hệ sinh thái cho hầu hết các thiết bị nhúng đang thiếu phương tiện, văn hóa và trong nhiều trường hợp là khả năng tuyệt đối để quản lý quá trình vá lõi.

### Xác thực

*Xác thực* là một vị ngữ quan trọng đối với chức năng bảo mật. Các định nghĩa về tính bảo mật, tính toàn vẹn và nhiều thuộc tính bảo mật khác đều có thuật ngữ *người dùng đã được xác thực* trong đó. Điều này khiến cho xác thực trở thành một thuộc tính quan trọng, tuy nhiên, với hệ sinh thái phi-máy-tính, nơi mà trong đó hầu hết các thiết bị nhúng và chuyên dụng hoạt động, có một vấn đề với việc áp dụng trực tiếp khái niệm xác thực. Tuy nhiên, đây không phải là một hạn chế đáng kể vì không giống

như máy tính, vốn thực hiện vô số chức năng khác nhau cho những người dùng khác nhau, các hệ thống nhúng và hệ thống chuyên biệt có xu hướng chỉ thực hiện một chức năng đơn lẻ với một người dùng không xác định theo thiết kế. Có thể cần một giao diện quản trị cho một số chức năng, nhưng việc kích hoạt điều này với một mã PIN đơn giản sẽ không có vấn đề gì, đặc biệt nếu các giá trị mặc định đã được tính đến trong quá trình thiết kế và triển khai. Để biết thêm thông tin về chủ đề này, hãy xem lại “Điểm yếu Mặc định” ở phần trước của chương.

### **Phạm vi**

Trong hầu hết các trường hợp, *phạm vi* là một chức năng của năng lực - một trong những hạn chế thực sự của rất nhiều hệ thống nhúng và hệ thống chuyên biệt. Một trong những thách thức của việc triển khai IoT là đưa chúng vào Internet, vì ở đó [trên Internet] phạm vi là không bị giới hạn. Tuy nhiên, điều này phải trả giá bằng bảo mật/rủi ro.

### **Chi phí**

Toàn bộ mục đích đằng sau việc phát triển các hệ thống nhúng/hệ thống chuyên biệt là giá trị ở đó. Chức năng hoàn trả *chi phí* của thiết bị biện minh cho việc thiết kế và triển khai, vì vậy, ở một mức độ nào đó biện minh cho chi phí. Tuy nhiên, chi phí cũng là một vấn đề kinh tế vì chức năng bổ sung dẫn đến chi phí bổ sung và nếu chức năng này không còn cần thiết trong giải pháp cuối cùng, tiền bạc sẽ bị lãng phí.

### **Niêm tin Ngụ ý**

*Niêm tin ngụ ý*, theo định nghĩa, là niềm tin chưa được xác lập một cách cụ thể nhưng vẫn tồn tại. Điều này hầu như được đưa ra trong rất nhiều hệ thống chuyên biệt vì chúng không được dự định hoặc thiết kế để trở thành các thiết bị máy tính có mục-đích-chung, do đó, các quá trình suy nghĩ liên quan đến sự tin cậy thường xuyên đối với máy tính và Internet

không tồn tại. Điều này giúp kết nối dễ dàng hơn, nhưng cũng mở ra cánh cửa cho kẻ tấn công.

---



**MÁCH NƯỚC CHO KỲ THI** Khi được hỏi về những ràng buộc và các hệ thống chuyên biệt (không phải máy tính có mục-đích-chung), hãy nhớ về hệ sinh thái mà thiết bị dự định hoạt động và cân nhắc điều đó khi hình thành đáp án. Nhiều khi nó sẽ khác với các hệ thống chuyên dụng/hệ thống nhúng hơn là đối với một máy tính có mục-đích-chung.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các tác động bảo mật của các hệ thống nhúng, vốn đã trở nên phổ biến trong cuộc sống hàng ngày của chúng ta. Chương mở đầu bằng một cuộc thảo luận về các hệ thống nhúng dưới dạng Raspberry Pi, mảng cổng lập trình trường (FPGA) và nền tảng vi điều khiển Arduino. Sau đó, chương trình bày về không gian SCADA/ICS và cách thức hoạt động của công nghệ trong thế giới riêng của nó và là một trong những quy mô đáng kể. Việc kiểm tra các hệ thống này trong các cơ sở vật chất cũng như trong ngành công nghiệp, sản xuất, năng lượng và hậu cần đã được đề cập. Sau đó, chương chuyển sang thế giới của các thiết bị thông minh và Internet of Things, bao gồm các cảm biến, thiết bị thông minh, thiết bị công nghệ đeo được trên người, tự động hóa cơ sở vật chất và các điểm yếu mặc định.

Sau đó, chương này đề cập đến các hệ thống chuyên biệt, bao gồm hệ thống y tế, xe cộ, máy bay và đồng hồ đo thông minh. Tiếp theo là cuộc thảo luận về Âm thanh thoại qua IP, hệ thống HVAC, máy bay không người lái và máy in đa chức năng. Tiếp theo, chúng tôi xem xét hệ điều hành theo thời-gian-thực, các hệ thống giám sát và hệ thống trên một con chip, tiếp theo là cân nhắc giao tiếp cho các hệ thống nhúng và hệ thống đặc biệt như 5G, băng tần hẹp, băng tần cơ sở, thẻ SIM và Zigbee. Chương này kết thúc với việc kiểm tra những ràng buộc của hệ thống trong các hệ thống này, bao gồm năng lượng, hiệu suất tính toán, chức năng mạng, chức năng mã hóa, khả năng vá lỗi, xác thực, phạm vi, chi phí và niềm tin ngụ ý.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

- 1.** Tuyên bố nào dưới đây *không* đúng?
  - A.** Các hệ thống nhúng được thiết kế với một mục đích kiểm soát duy nhất và thường không có chức năng bổ sung.
  - B.** Hệ thống nhúng không có rủi ro và lo ngại về bảo mật.
  - C.** *Nhúng* là tên gọi được đặt cho một máy tính được bao gồm như một phần không thể thiếu của một hệ thống lớn hơn.
  - D.** Hệ thống nhúng có thể phức tạp như hàng chục hệ thống nhúng được kết nối với nhau trong một chiếc ô tô hiện đại.
- 2.** Phát biểu nào sau đây là đúng về rủi ro của các phương tiện xe cộ thế hệ kế tiếp?
  - A.** Có rất ít rủi ro khi ô tô thế hệ tiếp theo chia sẻ thông tin.
  - B.** Việc chuyển lưu lượng giao thông và các thông tin khác giữa các phương tiện không làm gia tăng rủi ro về bảo mật.
  - C.** Việc chia sẻ điều hướng và các đầu vào khác giữa các phương tiện có thể gây ra một vấn đề về bảo mật.
  - D.** Thời gian tiếp cận thị trường và giảm thiểu chi phí có tác động tối thiểu đến các rủi ro tiềm ẩn được khai thác.
- 3.** Điều nào sau đây là định nghĩa đúng về kiểm soát giám sát và thu thập dữ liệu (SCADA)?
  - A.** Một phiên bản thu nhỏ của Linux được thiết kế để sử dụng trong hệ thống nhúng
  - B.** Tiêu chuẩn được sử dụng để giao tiếp giữa các hệ thống xe hơi thông minh

- C. Tạo ra rủi ro do kết nối các hệ thống điều khiển trong các tòa nhà
- D. Một hệ thống được thiết kế để điều khiển các hệ thống tự động trong môi trường vật lý mạng.
4. Phát biểu nào sau đây là đúng về thiết bị thông minh và Internet of Things (IoT)?
- A. Việc sử dụng nhân kiểu-Linux làm động cơ cốt lõi khiến cho việc lập trình trở nên phức tạp hơn.
- B. Sản xuất hàng loạt dẫn đến những rủi ro an ninh đáng kể.
- C. Việc mở rộng quy mô phát triển phần mềm trên một số lượng lớn các đơn vị làm cho chi phí có thể gia tăng và chức năng là điều tối quan trọng.
- D. Bảo mật hoặc bất kỳ điều gì có thể ảnh hưởng đến chức năng mở rộng mới được xem xét sớm và nhận được sự tập trung và nguồn lực cần thiết.
5. Phát biểu nào sau đây là đúng về HVAC và hệ thống tự động hóa tòa nhà?
- A. Chúng vẫn chưa được khai thác ở bất kỳ mức độ nào.
- B. Việc kết nối các hệ thống này với nhau và sử dụng các cơ chế kiểm soát trung tâm dựa trên Internet làm gia tăng nguy cơ bị tấn công từ bên ngoài.
- C. Việc có một "tòa nhà thông minh" làm giảm việc sử dụng các nguồn lực của tòa nhà phù hợp với số lượng và sự phân bố của những người bên trong đã không làm tăng hiệu quả hoặc giảm chi phí.
- D. Sự gia tăng của siêu kết nối đã không làm tăng thêm mối lo ngại về bảo mật.
6. Phát biểu nào sau đây *không* đúng về hệ thống trên một con chip?

- A.** Nó cung cấp đầy đủ chức năng của một nền tảng máy tính trên một con chip.
- B.** Nó thường có mức tiêu thụ điện năng thấp và thiết kế hiệu quả.
- C.** Việc lập trình các hệ thống SoC có thể xảy ra ở một số cấp độ khác nhau, và do đó các rủi ro tiềm ẩn dễ dàng được giảm thiểu.
- D.** Vì SoC đại diện cho nền tảng máy tính với hàng tỷ thiết bị trên toàn thế giới, nên nó đã trở thành một thế lực đáng kể trên thị trường.
- 7.** Điều gì phân biệt hệ điều hành theo thời gian thực (RTOS) với hệ điều hành có mục đích chung?
- A.** Không giống như RTOS, hầu hết các hệ điều hành có mục đích chung xử lý các ngắt trong phạm vi các ràng buộc thời gian đã được xác định.
- B.** Không giống như các hệ điều hành có mục đích chung, hầu hết các RTOS đều có khả năng đa nhiệm theo thiết kế.
- C.** Không giống như RTOS, hầu hết các hệ điều hành đa nhiệm theo thiết kế.
- D.** Không giống như các hệ điều hành có mục đích chung, RTOS được thiết kế để xử lý đa luồng.
- 8.** Phát biểu nào sau đây là đúng về máy in và các thiết bị đa chức năng?
- A.** Chúng dựa vào máy tính để quản lý quá trình in và quét.
- B.** Do có lịch sử lâu đời và được sử dụng rộng rãi, tính bảo mật đã được thiết kế cho các sản phẩm này.
- C.** Các thiết bị này giao tiếp theo kiểu hai chiều, chấp nhận lệnh in và gửi lại trạng thái lệnh, trạng thái máy in, v.v...
- D.** Cho đến nay, chúng vẫn chưa được chứng minh là có thể bị tấn công hoặc có khả năng truyền phần mềm độc hại vào máy tính.

- 9.** Điều nào sau đây là khía cạnh rất quan trọng cần luôn ghi nhớ khi xử lý vấn đề bảo mật các thiết bị y tế?
- A.** Chúng vẫn còn tương đối mới trong cách sử dụng của chúng.
  - B.** Chúng có thể ảnh hưởng trực tiếp đến tính mạng con người.
  - C.** Bảo mật không liên quan đến an toàn.
  - D.** Chúng hầu như chỉ là những thiết bị hoạt động độc lập, không có kết nối Internet.
- 10.** Điều nào dưới đây gây ra rủi ro tiềm tàng đáng kể cho các phương tiện bay không người lái?
- A.** Chúng có chức năng lái tự động tinh vi.
  - B.** Chúng có máy ảnh, cảm biến và trọng tải.
  - C.** Một số mô hình có một mức giá thấp.
  - D.** Vì chúng không có phi công, hệ thống điều khiển từ xa của chúng có thể được nối mạng và do đó dễ gặp rủi ro tiềm ẩn.

## Đáp án

1. **B.** Hệ thống nhúng *không* phải là không có rủi ro hoặc lo ngại về bảo mật, như tin tặc đã chứng minh.
2. **C.** Việc chia sẻ điều hướng và các yếu tố đầu vào khác có thể gây ra vấn đề về bảo mật cho các phương tiện thế hệ tiếp theo. Thông tin sai lệch, khi được chia sẻ, có thể gây ra vấn đề.
3. **D.** SCADA là một hệ thống được thiết kế để kiểm soát các hệ thống tự động trong môi trường vật lý mạng.
4. **C.** Việc mở rộng quy mô phát triển phần mềm trên một lượng lớn các đơn vị làm cho chi phí có thể gia tăng và chức năng là điều tối quan trọng trong các thiết bị thông minh và IoT.
5. **B.** Kết nối HVAC và hệ thống tự động hóa tòa nhà và sử dụng cơ chế điều khiển trung tâm dựa trên Internet để quản lý chúng làm gia tăng nguy cơ bị tấn công từ bên ngoài.
6. **C.** Việc lập trình các hệ thống SoC có thể xảy ra ở một số cấp độ khác nhau, và do đó rủi ro tiềm ẩn *rất khó* để giảm thiểu.
7. **C.** Một điểm phân biệt hệ điều hành thời-gian-thực (RTOS) với các hệ điều hành có mục-đích-chung là hầu hết các hệ điều hành có mục-đích-chung đều được thiết kế cho đa nhiệm.
8. **C.** Máy in và các thiết bị đa chức năng giao tiếp theo kiểu hai chiều, chấp nhận lệnh in và gửi lại trạng thái lệnh, trạng thái máy in, v.v...
9. **B.** Một khía cạnh rất quan trọng cần luôn nhớ khi xử lý vấn đề bảo mật của các thiết bị y tế là chúng có thể ảnh hưởng trực tiếp đến tính mạng con người.
10. **D.** Một rủi ro tiềm ẩn đáng kể đối với các phương tiện bay không người lái là do chúng không có người lái nên hệ thống điều khiển từ xa của chúng có thể bị nỗi mạng và do đó dễ bị rủi ro tiềm ẩn.

## Chương 15 Các Biện pháp kiểm soát Bảo mật Vật lý

### Các Biện pháp kiểm soát Bảo mật Vật lý

Trong chương này bạn sẽ

- Khám phá tầm quan trọng của các biện pháp kiểm soát vật lý,
- Tìm hiểu về các biện pháp kiểm soát môi trường quan trọng.

Bảo mật về mặt vật lý là một chủ đề quan trọng để doanh nghiệp xử lý vấn đề bảo mật của hệ thống mạng và hệ thống thông tin. Các doanh nghiệp chịu trách nhiệm cho việc quản lý khả năng tiếp xúc với rủi ro của họ, vốn yêu cầu sự bảo mật cho sự kết hợp của các tài sản bao gồm: nhân viên, kho thành phẩm, bí mật thương mại, và thông tin chiến lược. Những tài sản này và những tài sản quan trọng khác ảnh hưởng đến khả năng mang lại lợi nhuận của một công ty và sự sinh tồn của họ trong tương lai. Do đó, các công ty tiến hành rất nhiều hoạt động để cố gắng cung cấp các yếu tố bảo mật vật lý – khóa các cửa, thiết lập các hệ thống cảnh báo, sử dụng các két sắt, thuê nhân viên bảo vệ, thiết lập kiểm soát truy cập và hơn thế nữa.

Kiểm soát môi trường đóng một vai trò quan trọng trong việc bảo vệ các hệ thống được sử dụng để xử lý thông tin. Hầu hết các công ty ngày nay đã đầu tư rất nhiều thời gian, tiền bạc và công sức cho cả bảo mật hệ thống mạng và bảo mật hệ thống thông tin. Trong chương này, bạn sẽ tìm hiểu về cách mà các chiến lược bảo mật mạng và bảo mật hệ thống thông tin được liên kết như thế nào và bạn sẽ tìm hiểu một số phương pháp mà các công ty có thể giảm thiểu khả năng tiếp xúc với các sự kiện bảo mật vật lý có thể làm sụt giảm khả năng bảo mật mạng của họ.

## Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 2.7 của kỳ thi CompTIA Security+: Giải thích tầm quan trọng của các biện pháp kiểm soát bảo mật vật lý.

## Rào chắn/Chướng ngại vật

Biện pháp phòng thủ chủ yếu chống lại phần lớn các cuộc tấn công vật lý là các *chướng ngại* giữa tài sản và một kẻ tấn công tiềm năng – những bức tường, hàng rào, cổng và cửa ra vào. Các chướng ngại vật cung cấp nền tảng cho tất cả các sáng kiến bảo mật khác nhưng bảo mật phải được thiết kế một cách cẩn trọng, vì một kẻ tấn công chỉ phải tìm ra một kẽ hở để có được quyền truy cập. Các chướng ngại vật cũng có thể được sử dụng để kiểm soát phương tiện ra vào và gần một tòa nhà hoặc công trình kiến trúc. Rào chắn kiểu-đơn-giản ngăn phương tiện vượt qua nhưng cho phép người đi bộ qua được gọi là một *rào chắn*.



### MÁCH NƯỚC CHO KỲ THI

Các rào chắn là những trụ chắc chắn thường được làm bằng bê tông hoặc thép mạ kẽm hoặc thép không rỉ. Chúng được sử dụng để bảo vệ các lối ra vào và ngăn chặn các cuộc tấn công xâm nhập trái phép hoặc các vụ đâm xe.

Tường có thể là một trong những phát minh đầu tiên của con người. Một khi chúng ta đã học được cách sử dụng các chướng ngại vật tự nhiên như các ngọn núi để ngăn cách chúng ta với kẻ thù, tiếp theo chúng ta học cách xây dựng ngọn núi của riêng mình cho cùng một mục đích. Hadrian's Wall ở Anh, Vạn Lý Trường Thành ở Trung Quốc và Bức tường Berlin đều là những ví dụ nổi tiếng về khả năng phòng thủ vật lý cơ bản như vậy. Các bức tường của bất kỳ tòa nhà nào cũng phục vụ cho cùng một mục đích nhưng ở quy mô nhỏ hơn: chúng tạo ra các rào cản đối với việc tiếp cận về mặt vật lý với các tài sản của công ty. Trong trường hợp tài sản thông tin, theo nguyên tắc chung, tài sản có giá trị nhất được chứa trên máy chủ của công ty. Để bảo vệ các máy chủ vật lý, bạn phải nhìn theo mọi hướng. Cửa ra vào và cửa sổ phải được bảo đảm an toàn, và chỉ sử

dụng một lượng tối thiểu mỗi cửa sổ trong phòng máy chủ khi chúng là những thứ ngăn cách máy chủ với nhân viên được phép truy cập chúng. Điều rất quan trọng là bất kỳ cửa sổ hoặc cửa ra vào trong suốt nào đều không cho phép việc lướt qua vai từ bên ngoài phòng máy chủ. Thật tốt khi nhìn thấy mọi người trong phòng, không phải là những gì họ gõ trên màn hình của họ. Các điểm truy nhập ít rõ ràng hơn cũng cần được xem xét: Có sử dụng trần thả trong phòng máy chủ không? Các bức tường bên trong có kéo dài đến mái nhà, sàn nâng hoặc không gian trống trên trần không? Quyền truy cập vào phòng máy chủ chỉ nên được giới hạn cho những người cần phải truy cập, không phải cho tất cả nhân viên của tổ chức. Nếu bạn định sử dụng một bức tường để bảo vệ một tài sản, hãy đảm bảo rằng không có lỗ hổng rõ ràng nào xuất hiện trên bức tường đó.



### LƯU Ý

Có cửa sổ hay không có cửa sổ? Các cửa sổ mang lại sự rõ ràng, cho phép mọi người quan sát được các hoạt động trong phòng máy chủ. Điều này có thể cung cấp bảo mật nếu những người thực hiện việc quan sát có quyền xem xét hoạt động trong phòng máy chủ. Nếu những người bên ngoài không có quyền này, thì việc sử dụng cửa sổ nên được tránh.

Một phương pháp khác để ngăn chặn sự truy cập lén lút là sử dụng cửa sổ. Nhiều khu vực an ninh cao có số lượng cửa sổ đáng kể để không thể ẩn giấu các hoạt động của những người trong khu vực. Phòng máy chủ kín không có cửa sổ tạo nên một nơi yên tĩnh cho ai đó có thể truy cập thực tế vào thiết bị mà không lo việc bị nhìn thấy. Các cửa sổ loại bỏ yếu tố riêng tư này mà nhiều tội phạm phụ thuộc vào nó để đạt được mục đích và các hoạt động bất hợp pháp của chúng.



**MÁCH NƯỚC CHO KỲ THI** Tất cả các điểm truy nhập vào phòng máy chủ và các tủ cáp nên được kiểm soát một cách chặt chẽ, và, nếu có thể, việc truy cập nên được ghi nhật ký lại trong một hệ thống kiểm soát truy cập.

### **Hành lang Kiểm soát Truy cập**

Việc triển khai một hành lang kiểm soát ra vào, còn được gọi là bẫy người, là một cách để chống lại việc theo đuôi (tailgating). Hành lang kiểm soát ra vào bao gồm hai cửa đặt gần nhau đòi hỏi người dùng sử dụng phái thẻ để đi qua một cửa và sau đó tuần tự qua cửa khác. Bẫy người khiến cho gần như không thể đi qua một cửa mà không bị phát hiện - nếu kẻ xâm nhập tình cờ qua được cửa đầu tiên trước khi nó đóng lại, anh ta sẽ bị mắc kẹt bởi cánh cửa thứ hai, vì cánh cửa thứ hai vẫn bị khóa cho đến khi cánh cửa đầu tiên được đóng lại và khóa.



**MÁCH NƯỚC CHO KỲ THI** Việc bố trí một hành lang kiểm soát truy cập có thể ngăn chặn những người trái phép theo sau một người đã được cấp phép truy cập để đi qua một cửa được-kiểm-soát-truy-cập, vốn được gọi là *theo đuôi* (*tailgating*).

### **Huy hiệu**

Khi các tổ chức phát triển về mặt quy mô, không phải ai cũng có thể nhận biết được những người khác bằng mắt thường. Do đó, một số hình thức nhận dạng vật lý là điều cần thiết để nhận biết nhân viên. Một huy hiệu với hình ảnh trên đó có thể cho phép người khác nhanh chóng xác định xem bạn có phải là nhân viên hay không. Khách truy cập được cấp huy

hiệu riêng để xác định họ là khách. Nhận dạng tần số vô tuyến (RFID) sử dụng trường điện từ để tự động xác định và ghi lại thông tin. Thẻ RFID được sử dụng rộng rãi trong các huy hiệu nhận dạng, thay thế các thẻ có dải từ tính trước đó và làm cho chúng có thể sử dụng được chỉ bằng một cái vuốt gần đầu đọc.

## Báo động

*Báo động* dùng để cảnh báo cho người vận hành về các điều kiện bất thường. Bảo mật vật lý có thể bao gồm nhiều cảm biến, cảnh báo xâm nhập, thiết bị phát hiện chuyển động, công tắc cảnh báo cửa đang mở, giám sát video và âm thanh, v.v... Mỗi một trong số các hệ thống này đều có thể thu thập những thông tin hữu ích, tuy nhiên, nó chỉ thực sự hữu ích nếu nó được hành động theo. Khi một trong những hệ thống này có thông tin có thể được sử dụng cho nhân viên vận hành, báo động là phương pháp dễ dàng nhất để thông báo cho nhân viên về tình trạng này. Báo động không hề đơn giản, nếu một công ty có quá nhiều điều kiện báo động, đặc biệt là báo động giả, thì nhân viên vận hành sẽ không phản ứng với các điều kiện như được mong muốn. Việc điều chỉnh báo động để chúng cung cấp thông tin hữu ích, chính xác và có thể hành động là điều quan trọng nếu bạn muốn chúng hoạt động hiệu quả.



## MÁCH NƯỚC CHO KỲ THI

Hệ thống đèn chiếu sáng, biển báo, hàng rào và chuông báo động là tất cả các hạng mục có liên quan đến bảo mật vật lý. Câu trả lời thích hợp cho một câu hỏi trong đề thi sẽ dựa trên các chi tiết cụ thể của câu hỏi – hãy quan sát các manh mối và chọn đáp án tốt nhất dựa trên ngữ cảnh của câu hỏi.

## Biển báo chỉ dẫn

Các dấu hiệu hoạt động như một thiết bị thông tin và có thể được sử dụng theo nhiều cách khác nhau để hỗ trợ cho bảo mật vật lý. *Biển báo chỉ dẫn* có thể cung cấp thông tin về những khu vực bị hạn chế hoặc có thể chỉ ra nơi cần phải có các biện pháp phòng ngừa cụ thể, chẳng hạn như khóa cửa, nếu cần thiết. Một cách sử dụng các biển báo chỉ dẫn phổ biến trong các cơ sở đòi hỏi bảo mật cao là để phân định nơi cho phép du khách và khu vực an ninh cần có người đi cùng. Các manh mối bảo mật trực quan có thể hỗ trợ cho việc cảnh báo người dùng về sự cần thiết của các biện pháp phòng ngừa bảo mật cụ thể. Các manh mối trực quan về các kiểu bảo vệ cần thiết có thể ở dạng huy hiệu tên có màu-sắc-khác-nhau biểu thị cho các mức độ truy cập, dây buộc trực quan cho biết khách truy cập, các thư mục màu, v.v...

## Máy ghi hình

Máy ghi hình là một công cụ rất quan trọng đối với bảo mật. Câu ngạn ngữ cổ “một bức tranh đáng giá bằng một ngàn lời nói” luôn đúng và điều này đặc biệt đúng trong lĩnh vực bảo mật. Từ việc ghi lại những bằng chứng để sử dụng sau này, như chụp ảnh thiết bị, bảng số sê-ri, v.v..., cho đến thu thập bằng chứng tại hiện trường vụ án, *máy ghi hình* cho phép tái-tạo lại hiện trường vào một ngày nào đó sau này. Máy ảnh đã có tuổi đời hơn 100 năm, nhưng với sự phát minh ra nhiếp ảnh kỹ thuật số, sau đó là việc bổ sung máy ảnh vào điện thoại di động, ngày nay thực sự có hàng tỷ máy ảnh trên toàn thế giới chụp được hàng chục tỷ bức ảnh. Một trong những cách áp dụng thú vị của công nghệ này là khả năng chia sẻ hình ảnh với người khác một cách nhanh chóng, cho phép ai đó “nhìn thấy” vượt xa phạm vi thị lực bình thường. Vào năm 2020, khi bạo loạn nổ ra trên khắp nước Mỹ, rất nhiều người biểu tình đã ghi lại phản ứng của cảnh sát bằng camera của điện thoại di động. Trong khi họ đang sử dụng máy ảnh của mình để ghi hình lại những cảnh sát, họ cũng ghi

lại những hình ảnh mà cơ quan thực thi pháp luật sau này sẽ sử dụng để bắt những kẻ gây ra tội ác.

Các máy quay phim thậm chí còn mang lại nhiều năng lực giám sát hơn nữa, và các máy ghi hình TV mạch-kín sẽ được đề cập đến trong một phần sau đây.

### **Phát hiện Chuyển động**

*Phát hiện chuyển động* là một công nghệ rất quan trọng để giới hạn thời gian tìm kiếm và không gian ghi nhận liên quan đến các hình ảnh video. Bức xạ hồng ngoại (IR) không thể nhìn thấy được bằng mắt người, nhưng có thể được sử dụng giống như một nguồn sáng để phát hiện một loạt các sự vật. Chuyển động từ các sinh vật sống có thể được nhìn thấy do các ký hiệu nhiệt của cơ thể của chúng. Phát hiện bằng tia hồng ngoại là một phương tiện kỹ thuật để tìm kiếm những thứ mà nếu không có tia hồng ngoại thì rất có thể đã không được chú ý đến. Vào ban đêm, khi trời tối, ai đó có thể ẩn mình trong bóng tối, nhưng ánh sáng hồng ngoại có thể hướng họ đến các camera cảm biến hồng ngoại. Các máy dò tia hồng ngoại có thể cảm nhận sự khác biệt về nhiệt độ, có thể là từ một người bước vào phòng, ngay cả khi người đó không được nhìn thấy do bóng tối. Báo động hồng ngoại được sử dụng rộng rãi để theo dõi chuyển động của người xuất hiện ở những khu vực mà họ không nên có mặt.

### **Nhận diện Đối tượng**

Những hệ thống video giám sát hiện đại đi kèm với một số phần mềm rất ấn tượng. Ngay cả những chiếc máy ảnh được bán cho chủ nhà cũng có thể quét video để tìm chuyển động và phát hiện người, xe hơi và các đồ vật được chỉ định khác như gói hàng bị bỏ lại trên hiên nhà. Việc sử dụng phần mềm video để phát hiện đối tượng không thay thế cho mắt người, nhưng nó nâng cao đáng kể khả năng của người bảo vệ trong việc sử dụng hiệu quả các cảnh quan sát lớn của camera để bao quát một cơ sở.

Hệ thống video giám sát toàn thành phố ở London là nguồn bằng chứng chính đã xác định được những kẻ khủng bố đã thực hiện hàng loạt vụ đánh bom khắp thành phố vào năm 2005.

### **Truyền hình Mạch kín (CCTV)**

Giám sát video thường được thực hiện thông qua *truyền hình mạch kín* (*closed-circuit television - CCTV*). Việc sử dụng camera CCTV vào mục đích giám sát bắt đầu ít nhất là từ năm 1961, khi các camera được lắp đặt ở ga xe lửa Giao thông vận tải London. Sự phát triển của các thành phần camera nhỏ hơn và chi phí thấp hơn đã mang lại lợi ích cho ngành công nghiệp camera quan sát kể từ đó.

Camera quan sát được sử dụng để giám sát một khu vực làm việc vì các mục đích an ninh. Những hệ thống này phổ biến ở các ngân hàng và cửa hàng trang sức - những nơi có hàng hóa giá trị cao rất hấp dẫn những kẻ trộm. Khi chi phí của các hệ thống này giảm xuống, chúng đã trở nên thực tế đối với nhiều phân khúc ngành khác. Các máy ảnh truyền thống dựa trên tín hiệu tương tự (analog) và yêu cầu một bộ ghép kênh video để kết hợp tất cả các tín hiệu và làm cho nhiều khung cảnh xuất hiện trên một màn hình. Máy ảnh kỹ thuật số dựa trên IP đã thay đổi điều đó, vì hầu hết chúng là các đơn vị độc lập có thể xem được thông qua trình duyệt web, chẳng hạn như máy ảnh được hiển thị trong Hình 15-1.



**Hình 15-1** Các camera dựa-trên-IP tận dụng các mạng IP hiện tại thay vì cần đến một đường cáp CCTV độc quyền.

Những hệ thống dựa-trên-IP này bổ sung thêm các tính năng hữu ích, chẳng hạn như khả năng kiểm tra các tòa nhà từ Internet. Tính năng qua mạng này, tuy nhiên, khiến cho các camera trở thành đối tượng của các cuộc tấn công mạng dựa-trên-IP như bình thường. Một cuộc tấn công DoS được phát động vào hệ thống CCTV ngay khi một vụ đột nhập đang xảy ra là điều cuối cùng mà bất kỳ ai (ngoại trừ bọn tội phạm) muốn. Vì lý do này, các camera quan sát dựa-trên-IP nên được đặt trên mạng riêng của chúng mà chỉ có nhân viên an ninh mới có thể truy cập được. Sự phân tách vật lý tương tự áp dụng cho bất kỳ cơ sở hạ tầng camera dựa-trên-IP nào. Các máy ghi băng từ thời-gian-chậm (time-lapse) đang dần được thay thế bằng các máy quay video kỹ thuật số. Mặc dù tiến bộ về công nghệ là đáng kể, nhưng hãy cẩn trọng nếu và khi các thiết bị này được

kích-hoạt-IP, vì chúng sẽ trở thành một vấn đề về bảo mật, giống như mọi thứ khác kết nối vào mạng.

Nếu bạn phụ thuộc vào một hệ thống CCTV để bảo vệ những tài sản của tổ chức của bạn, hãy cân nhắc một cách cẩn trọng việc thay thế các camera và các kiểu camera được sử dụng. Các loại mắt ghi hình khác nhau, độ dài tiêu cự và màu sắc và khả năng hồng ngoại là tất cả những tùy chọn khiến cho một camera vượt trội hơn những camera khác ở một vị trí cụ thể.

### **Ngụy trang Công nghiệp**

*Ngụy trang* là hành động cụ thể để kết xuất một đề mục không dễ quan sát được. Được rất nhiều người coi là một công cụ quân sự, ngụy trang bắt đầu có trong tự nhiên, nơi côn trùng và động vật có các hoa văn khiến chúng dường như trông khác với thực tế của chúng. Nguyên tắc này luôn luôn được sử dụng để làm cho mọi thứ ẩn trong tầm nhìn rõ ràng của một ai đó. Tháp điện thoại di động được xây dựng để trông giống như cây cối khiến chúng khó thấy hơn - và nói chung là cải thiện hình ảnh xung quanh chúng. Để đối phó với các tác động vật lý đối với các trạm biến áp điện, nhiều công ty tiện ích đã đặt các bức tường xung quanh trạm biến áp, làm cho các thiết bị bên trong không còn được nhìn thấy và ít được nhắm mục tiêu hơn.



### **LƯU Ý**

Nếu bạn muốn nhìn thấy sự ngụy trang công nghiệp trong thực tế, hãy sử dụng Street View trong Google Maps và tìm kiếm tại những vị trí sau đây:

- 58 Joralemon Street, New York City, là một trực thông gió và lối vào khẩn cấp cho tàu điện ngầm New York.

- 640 Millwood Road, Toronto, Canada, là một trạm biến áp điện - một trong số 250 trạm biến áp trong thành phố.
- 51 W. Ontario Street, Chicago, Illinois, là một trạm biến áp khác - trạm này thuộc về Commonwealth Edison. Cửa ra vào là giả và không mở được, còn cửa sổ thực sự là lỗ thông hơi.

### **Con người**

Bảo mật vật lý nên là một phần của một chương trình bảo mật tổng thể của một công ty. Các biện pháp bảo mật vật lý là những biện pháp được thực hiện để đảm bảo sự phân tách của các mục sẽ được bảo vệ khỏi tất cả những rủi ro về mặt vật lý. Con người là một phần quan trọng của phương trình này – từ nhân viên bảo vệ đến nhân viên hành lang, người đóng vai trò như người gác cửa cho khách thăm viếng và hàng hóa, con người là một phần của hệ thống bảo mật vật lý.

### **Nhân viên bảo vệ**

*Nhân viên bảo vệ* cung cấp một biện pháp an ninh tuyệt vời, bởi vì nhân viên bảo vệ là sự hiện diện hữu hình với trách nhiệm trực tiếp về mặt an ninh. Những nhân viên khác mong đợi nhân viên bảo vệ sẽ cư xử theo một cách nhất định với sự quan tâm đến việc đảm bảo an ninh cho cơ sở. Nhân viên bảo vệ thường giám sát lối vào và lối ra và có thể duy trì nhật ký truy cập của những người đã đi vào và rời khỏi tòa nhà. Trong rất nhiều tổ chức, tất cả những ai đi qua khu vực an ninh với tư cách là khách truy cập đều phải ký vào nhật ký, điều này có thể sẽ hữu ích trong việc truy tìm ai đã ở vị trí nào và lý do tại sao [họ lại ở đó].

Nhân viên an ninh rất hữu ích trong việc bảo mật vật lý những máy móc, nơi tài sản thông tin cư trú, nhưng để có được lợi ích cao nhất từ sự hiện diện của họ, họ phải được đào tạo để thực hiện một phương pháp tiếp cận toàn diện đối với bảo mật. Giá trị của dữ liệu thường có thể gấp nhiều lần giá trị của các máy mà dữ liệu được lưu trữ trên đó. Nhân viên

bảo vệ thường không phải là chuyên gia bảo mật máy tính, vì vậy họ cần được đào tạo về giá trị của dữ liệu và được đào tạo về an ninh mạng cũng như bảo mật vật lý có liên quan đến người dùng. Họ là tai mắt của công ty đối với hoạt động đáng ngờ, vì vậy, bộ phận an ninh mạng cũng cần đào tạo họ để nhận thấy những hoạt động mạng đáng ngờ. Nhiều điện thoại nhánh đổ chuông liên tục trong đêm, các máy tính khởi động lại đồng thời và người lạ đậu trong bãi đậu xe với máy tính xách tay hoặc các thiết bị điện toán di động khác đều là dấu hiệu của một cuộc tấn công mạng có thể bị bỏ sót nếu không được đào tạo thích hợp.

### **Robot Canh gác**

Nhiệm vụ bảo vệ là công việc rất nhàn chán và mặc dù các vệ sĩ không được trả lương cao theo thời gian, nhưng việc có một số vệ sĩ có thể sẽ rất tốn kém. Công nghệ robot đã phát triển đến mức giờ đây robot có thể thực hiện nhiều nhiệm vụ đơn giản và nhiệm vụ canh gác có thể là một trong những nhiệm vụ này. Các lính canh robot có thể tuần tra các tòa nhà trống và sử dụng cảm biến để có thể phát hiện sự hiện diện của những cá nhân trái phép. Sau đó, các lính canh robot có thể báo cáo vấn đề với một trạm có người canh gác để từ đó có thể cảnh báo cho các cơ quan chức năng thích hợp để có phản ứng.

### **Lễ tân**

Các *khu vực lễ tân* được sử dụng làm vùng đệm giữa các khu vực khác nhau của cơ sở, phân chia tòa nhà thành những khu vực riêng biệt. Có một bàn làm để thủ tục cho khách cho phép kiểm soát khách viếng thăm cũng như cho phép các chức năng như ghi lại nhật ký khách, quản lý việc giao hàng và cung cấp người hộ tống cho khách. Trong môi trường an ninh thấp hơn, khu vực tiếp tân này có thể chỉ đơn giản là một người nào đó ngồi tại bàn làm việc và không có rào cản vật lý. Ở những cơ sở an ninh hơn, lễ tân không chỉ chịu trách nhiệm cho việc lưu giữ nhật ký, cấp

thẻ ra vào và thông báo cho những người hộ tống mà còn kiểm soát những cánh cửa mà mọi người phải đi qua. Trong môi trường được kiểm soát rất chặt chẽ, việc kiểm soát cửa thực tế được thực hiện từ xa từ phía bên kia của cánh cửa để mọi người không thể vượt qua khu vực lề tân.

### **Kiểm soát/Toàn vẹn Hai-Người**

Khi các nhiệm vụ là tối quan trọng hoặc các lỗi có thể dẫn đến những rủi ro đáng kể thì nên áp dụng nguyên tắc tổ chức về sự phân tách giữa các nhiệm vụ. Chủ đề này được đề cập đầy đủ trong Chương 33, "Các Chính sách tổ chức". Khi có các nhiệm vụ liên quan đến vật lý, chẳng hạn như việc mở cánh cửa được đề cập trong phần trước, sẽ cần có hai người để cùng thực hiện nhiệm vụ để cung cấp một phương tiện kiểm tra và cân bằng. *Sự toàn vẹn/kiểm soát của-hai-người* chính là nguyên tắc hành động này: đó là khi hai người khác nhau phải thực hiện các nhiệm vụ tương ứng và cả hai đều cần thiết để hành động xảy ra. Người thứ nhất có thể bắt đầu quy trình, kiểm tra ID, nhập dữ liệu vào nhật ký và cấp thẻ khách, trong khi người thứ hai có thể kiểm soát việc ra vào cửa. Bằng cách này, lỗi của một trong hai người sẽ không làm phát lộ quá trình [hàm ý rằng lỗi của một trong hai người sẽ không khiến cho quá trình gặp phải rủi ro].



**MÁCH NƯỚC CHO KỲ THI** Hãy đảm bảo bạn có khả năng để giải thích những biện pháp kiểm soát bảo mật vật lý quan trọng, bao gồm nhân viên bảo vệ, rô-bốt canh gác, lề tân, và kiểm soát/toàn vẹn hai-người.

### **Khóa**

Khóa là một biện pháp an ninh phổ biến được sử dụng với tần suất gần như phổ biến. Mọi người đều quen thuộc với việc sử dụng khóa để bảo

về một thứ gì đó. Rất nhiều *loại khóa* khác nhau được sử dụng trong và xung quanh lĩnh vực bảo mật máy tính. Có những loại dành cho máy tính xách tay và các thiết bị di động khác, dành cho máy tính để bàn và thậm chí cả máy chủ. Cũng giống như các ổ khóa có thể giữ cho ô tô hoặc xe đạp của bạn không bị đánh cắp, chúng cũng có thể bảo vệ máy tính. Máy tính xách tay là mục tiêu phổ biến của kẻ trộm và phải được khóa bên trong bàn làm việc khi không sử dụng hoặc được bảo vệ bằng cáp khóa máy tính đặc biệt. Các vụ trộm máy tính xách tay từ ô tô có thể xảy ra chỉ trong vài giây và những tên trộm đã bị bắt quả tang lấy trộm máy tính xách tay từ khu vực kiểm tra an ninh tại sân bay trong khi chủ sở hữu bị phân tâm với quá trình kiểm tra. Nếu tổ chức sử dụng máy tính để bàn dạng tháp, tổ chức đó nên sử dụng bàn máy tính cung cấp không gian để khóa máy tính lại. Trong một số trường hợp, phương tiện có giá trị được lưu trữ trong một két sắt được thiết kế cho mục đích đó. Tất cả các biện pháp này có thể cải thiện bảo mật vật lý của máy tính, nhưng hầu hết chúng có thể bị đánh bại bởi những kẻ tấn công nếu người dùng không hiểu biết về chương trình bảo mật và không tuân theo nó.

## Sinh trắc học

*Sinh trắc học* là phép đo các thuộc tính hoặc quá trình sinh học với mục tiêu nhận dạng một bên đang sở hữu các phép đo đó. Yếu tố sinh trắc học nổi tiếng nhất là dấu vân tay. Các đầu đọc dấu vân tay đã được sử dụng trong và năm qua trên các máy tính xách tay và các thiết bị di động khác, như được minh họa trong Hình 15-2, và như là một thiết bị USB đơn-lẻ.



**Hình 15-2** Những máy tính xách tay mới hơn thường có một đầu đọc dấu vân tay.

Các phép đo sinh trắc học khác có thể được sử dụng cho mục đích bảo mật vật lý bao gồm võng mạc hoặc mõm mắt của mắt, hình dạng của bàn tay và hình dạng của khuôn mặt. Khi bất kỳ thứ nào trong số này được sử dụng để xác thực, sẽ có một quy trình bao gồm hai phần: đăng ký và sau đó là xác thực. Trong quá trình đăng ký, một máy tính sẽ lấy hình ảnh của yếu tố sinh học và biến nó thành một giá trị số. Khi người dùng cố gắng xác thực, đặc trưng của họ sẽ được quét bởi đầu đọc và máy tính sẽ so sánh giá trị số đang được đọc với giá trị đã được lưu trữ trong cơ sở dữ liệu. Nếu chúng khớp, quyền truy cập sẽ được cho phép. Vì các yếu tố vật lý này là duy nhất nên về mặt lý thuyết, chỉ có người được ủy quyền thực sự mới được phép truy cập.

Sinh trắc học thường được sử dụng trong bảo mật vật lý và đang trở nên gần như phổ biến để kiểm soát quyền truy cập vào các thiết bị di động, chẳng hạn như điện thoại và máy tính bảng. Với rất nhiều tình huống bảo mật vật lý, câu hỏi thực sự đối với quyền truy cập là bạn có phải chính xác là người cần có quyền truy cập không? Việc sử dụng sinh trắc học để xác nhận danh tính của người được xuất trình để truy cập với cùng một người đã trải qua giai đoạn nhận dạng khi đăng ký là một cách hay để trả lời câu hỏi này. Bạn không thể cho mượn dấu vân tay, mõng mắt hoặc võng mạc của mình để quét hoặc bàn tay của bạn để tìm hình học. Sinh trắc học của một người liên kết mã thông báo nhận dạng (identification token) với người đó.

Sinh trắc học không phải là dễ dàng sử dụng mà không thể có sai sót. Một số biện pháp sinh trắc học có thể bị sao chép để đánh lừa cảm biến và trong nhiều trường hợp, sinh trắc học thực tế được chuyển đổi thành một số cũng có thể bị can thiệp và sử dụng trong một cuộc tấn công phần mềm. Các biện pháp bảo vệ tồn tại đối với hầu hết các cơ chế bỏ-quasinh-trắc-học, khiến cho chúng trở thành một công nghệ bảo mật có thể sử dụng được.

### **Điện tử**

Khóa điện tử là những thiết bị cản trở một chức năng cụ thể trừ khi một mã số được nhập vào. Mã này được so sánh với một mã bí mật đã được lưu trữ và nếu mã chính xác được nhập, khóa sẽ dừng về mặt cơ học và cho phép cơ chế mở khóa. Khóa điện tử có một lợi thế là chúng không dễ bị thao tác về mặt cơ học và bỏ qua, tuy nhiên chúng vẫn dễ bị tấn công trong nhiều trường hợp, thông qua cơ chế cập nhật "sự kết hợp" bí mật.

### **Vật lý**

Các ổ khóa vật lý đã được sử dụng trong hàng trăm năm qua, thiết kế của chúng không có nhiều thay đổi: một "mã thông báo" bằng kim loại

được sử dụng để căn chỉnh các chốt trong một thiết bị cơ khí. Khóa vật lý đã tồn tại trong nhiều năm bởi vì chúng có giá thành khá thấp. Do tất cả các thiết bị cơ khí đều có dung sai, nên có thể lách qua những dung sai này bằng cách “cạy” khóa. Hầu hết các ổ khóa có thể dễ dàng được cạy bằng các dụng cụ đơn giản, một số trong số đó được trình bày trong Hình 15-3.



**Hình 15-3** Các công cụ để cạy khóa

Con người luôn cố gắng tạo ra một cái bẫy chuột tốt hơn và điều đó cũng áp dụng cho các ổ khóa. Các khóa bảo-mật-cao, chẳng hạn như khóa trong Hình 15-4, đã được thiết kế để đánh bại các cuộc tấn công, những ổ khóa này phức tạp hơn một hệ thống chốt cửa tiêu chuẩn tại nhà. Thường được tìm thấy trong các ứng dụng thương mại yêu cầu bảo mật cao, những ổ khóa này được tạo ra để chống lại việc cạy và khoan, cũng như các cuộc tấn công thông thường khác như chỉ cần đập khóa qua cửa. Một đặc điểm chung khác của các loại khóa có độ bảo mật cao là kiểm soát chìa khóa, đề cập đến các hạn chế được đặt ra đối với việc sao chép chìa khóa. Đối với hầu hết các ổ khóa dân dụng, một chuyến đi đến cửa

hàng kim khí sẽ cho phép bạn tạo ra được một bản sao của chìa khóa. Các khóa kiểm soát chìa khóa sử dụng các chìa khóa đã được cấp bằng sáng chế mà chỉ thợ khóa mới có thể sao chép, người này sẽ lưu hồ sơ về những người dùng được cấp phép của một chìa khóa cụ thể.



**Hình 15-4** Một ổ khóa bảo-mật-cao và chìa khóa của nó

Giờ đây, bảo mật khóa cao-cấp quan trọng hơn khi các cuộc tấn công như “bật khóa” đã được nhiều người biết đến và được phổ biến một cách rộng rãi. Một chìa khóa bật là một vết cắt khóa có tất cả các rãnh ở độ sâu tối đa, còn được gọi là “tất cả các số 9”. Chìa khóa này sử dụng một kỹ thuật đã có từ lâu nhưng gần đây đã trở nên phổ biến. Chìa khóa được đưa vào ổ khóa và sau đó đập mạnh, làm bật chốt khóa lên trên đường cắt và cho phép khóa mở. Các khóa bảo mật cao-cấp cố gắng ngăn chặn kiểu tấn công này thông qua các phương tiện cơ học khác nhau như bố trí chốt phi truyền thống, các thanh bên và thậm chí cả chìa khóa từ.

Các khóa kết hợp, hoạt động thông qua một mặt số xoay, phổ biến trên các két sắt cao cấp và có thể nâng cao mức độ bảo mật về cơ bản. Trong rất nhiều trường hợp, cách duy nhất để vượt qua một trong những ổ khóa này là tự vượt qua ổ khóa một cách vật lý thông qua việc khoan hoặc các phương pháp khác. Các cấp độ bảo vệ bổ sung tồn tại, chẳng hạn như các chốt dễ vỡ vụn, khi các chốt gài bị gãy khiến cửa không thể mở được.

### **Khóa Cáp**

Các thiết bị có thể di động có một đặc trưng chính là có thể di chuyển được. Đây cũng có thể là một vấn đề, vì thiết bị di động - máy tính xách tay, máy chiếu và những thứ tương tự - có thể dễ dàng bị lấy đi hoặc bị đánh cắp. Các *khóa cáp* cung cấp một phương tiện đơn giản để cố định thiết bị di động vào đồ nội thất hoặc một vật cố định khác trong phòng nơi thiết bị đó đang cư trú. Khóa cáp có thể được sử dụng bởi những chiến binh trên đường để bảo vệ máy tính xách tay khỏi những hành vi trộm cắp thông thường. Chúng cũng có thể được sử dụng trong các khu vực mở như trung tâm hội nghị hoặc các phòng nơi thiết bị di động tiếp xúc với nhiều khách tham quan.

### **Khóa Dữ liệu USB**

Các đầu nối USB trên máy tính cung cấp một đường dẫn cho dữ liệu đi vào hệ thống. Bất kỳ ai có quyền truy cập vật lý vào máy đều có thể cắm thiết bị USB và thực thi mã phần mềm từ thiết bị. Có rất nhiều cách để chặn cổng USB hoặc khiến cho chúng trở nên không thể hoạt động được, nhưng trong một số trường hợp, cổng USB có một vai trò thứ yếu là nguồn cung cấp điện cho các thiết bị bên ngoài. Kết nối USB có bốn dây dẫn: hai dây dẫn điện và hai dây truyền dữ liệu. Nếu bạn chặn dây dẫn dữ liệu, bạn vẫn có thể sạc thiết bị của mình từ nguồn USB mà không cần cấp cho thiết bị đó bất kỳ quyền truy cập nào vào dữ liệu. Khi sạc điện thoại của bạn ở các địa điểm như sân bay hoặc các nguồn điện không xác

định khác, việc sử dụng một *bộ khóa dữ liệu USB* sẽ bảo vệ điện thoại nhưng vẫn cho phép sạc.



**MÁCH NƯỚC CHO KỲ THI** Một bộ khóa dữ liệu USB ngăn chặn những kẻ tấn công làm lây nhiễm thiết bị bằng phần mềm mã độc hoặc đánh cắp dữ liệu. Hãy nhớ rằng việc tắt thiết lập AutoPlay trong hệ điều hành cũng sẽ ngăn chặn phần mềm mã độc tự động chạy khi bạn cắm một USB hoặc thiết bị lưu trữ bên ngoài vào máy tính của bạn.

### Đèn chiếu sáng

*Chiếu sáng* thích hợp là điều thiết yếu đối với an ninh vật lý. Các khu vực không được chiếu sáng hoặc thiếu ánh sáng cho phép những kẻ xâm nhập ẩn nấp và thực hiện các hoạt động trái phép mà không có nguy cơ bị nhân viên bảo vệ hoặc nhân viên khác phát hiện rõ. Ánh sáng bên ngoài tòa nhà rất quan trọng để đảm bảo rằng các hoạt động trái phép không thể xảy ra mà không được quan sát và ứng phó. Ánh sáng bên trong cũng quan trọng không kém vì nó cho phép nhiều người quan sát các hoạt động và phát hiện thấy các điều kiện không chính xác. Như đã mô tả trước đó trong phần “Chướng ngại/rào cản”, cửa sổ có thể đóng một vai trò quan trọng trong việc hỗ trợ quan sát cơ sở. Việc bố trí các khu vực nhạy cảm đủ ánh sáng và có thể quan sát được qua cửa sổ sẽ ngăn cản các hoạt động diễn ra trong bí mật nếu không có đủ ánh sáng. Các bên trái phép trong phòng máy chủ có nhiều khả năng bị phát hiện hơn nếu máy chủ được đặt ở vị trí trung tâm, có cửa sổ bao quanh và được chiếu sáng đầy đủ.

### Hàng rào

*Hàng rào* đóng vai trò như một rào cản vật lý xung quanh tài sản. Nó có thể ngăn mọi người ra hoặc vào, ngăn cản việc di chuyển tự do qua các

khu vực trái phép. Hàng rào có thể là một phần quan trọng của kế hoạch bảo mật vật lý. Nếu được sử dụng một cách đúng đắn, nó có thể giúp bảo vệ các khu vực khỏi những người truy cập trái phép. Bên ngoài các bức tường của tòa nhà, rất nhiều tổ chức muốn có hàng rào chu vi như một lớp phòng thủ vật lý đầu tiên. Hàng rào kiểu-liên-kết-chuỗi được sử dụng phổ biến nhất và nó có thể được tăng cường bằng dây thép gai dọc phía trên. Hàng rào chống-mở-rộng-quy-mô, trông giống như các cột thằng đứng rất cao được đặt gần nhau để tạo thành hàng rào, được sử dụng cho các triển khai bảo mật cao yêu cầu chống lại việc mở rộng quy mô và giả mạo.

Bên trong một tòa nhà, hàng rào có thể được sử dụng để cung cấp một phương tiện hạn chế xâm nhập vào các khu vực nơi các chính sách an ninh vật lý riêng biệt đang được áp dụng. Bộ phận lưu trữ tài liệu, các máy chủ, thiết bị mạng và các hạng mục nhạy cảm khác có thể được ngăn cách khỏi truy cập trái phép bằng hàng rào liên kết chuỗi đơn giản. Những khu vực này thường được gọi là *buồng (cage)* và việc ra/vào các khu vực buồng là đi qua một *cổng (gate)*. Cổng cho phép truy cập có kiểm soát và giúp giám sát dễ dàng hơn ai và cái gì được ra vào khu vực được kiểm soát. Cổng cũng được sử dụng để làm hàng rào bên ngoài. Các cổng cung cấp một điểm giám sát sự ra vào từ một khu vực đã được kiểm soát.

## Chữa cháy

Theo Hiệp hội các Hệ thống Ngăn chặn Hỏa hoạn (Fire Suppression Systems Association - [www.fssa.net](http://www.fssa.net)), 43% doanh nghiệp đóng cửa do bị hỏa hoạn nghiêm trọng sẽ không bao giờ có thể mở cửa trở lại. Thêm 29% nữa thất bại trong vòng ba năm kể từ sau sự kiện này. Do đó, khả năng ứng phó với đám cháy một cách nhanh chóng và hiệu quả là điều tối quan trọng đối với sự thành công lâu dài của bất kỳ tổ chức nào. Việc giải quyết các nguy cơ hỏa hoạn và lỗ hổng bảo mật tiềm ẩn từ lâu đã là

một mối quan tâm của các tổ chức trong quá trình phân tích rủi ro của họ. Mục tiêu rõ ràng là không bao giờ để xảy ra hỏa hoạn, nhưng nếu có hỏa hoạn xảy ra, điều quan trọng là phải có các cơ chế để hạn chế thiệt hại mà hỏa hoạn có thể gây ra. Hệ thống ngăn chặn đám cháy được thiết kế để bảo vệ chống lại thiệt hại do đám cháy lan rộng trong một cơ sở. Bởi vì chúng là hệ thống đàn áp, chúng sẽ không ngăn chặn việc đám cháy xảy ra, nhưng chúng sẽ ngừng đám cháy nó khi nó bắt đầu.

### **Hệ thống Chữa cháy Băng-Nước**

Hệ thống ngăn chặn đám cháy băng nước từ lâu đã và vẫn đang là công cụ chính để giải quyết và kiểm soát các đám cháy một cách có kết cấu. Khi xem xét số lượng thiết bị điện được tìm thấy trong môi trường văn phòng ngày nay và thực tế là, vì những lý do rõ ràng, thiết bị này không phản ứng tốt với việc sử dụng nước trên phạm vi lớn, điều quan trọng là phải biết phải làm gì với thiết bị nếu nó trở thành đối tượng của một hệ thống đầu dò phun nước. NFPA 75 năm 2017: *Tiêu chuẩn về Bảo vệ Thiết bị Công nghệ Thông tin* đưa ra các biện pháp có thể được thực hiện để giảm thiểu thiệt hại cho thiết bị điện tử tiếp xúc với nước.

### **Hệ thống Ngăn chặn Cháy bằng Tác-nhân-Sạch**

Khí Carbon dioxide (CO<sub>2</sub>) đã được sử dụng như một chất chữa cháy trong một thời gian dài. Công ty Điện thoại Bell đã sử dụng các bình chữa cháy CO<sub>2</sub> di động vào đầu thế kỷ 20. Bình chữa cháy CO<sub>2</sub> tần công cả ba yếu tố cần thiết để đám cháy xảy ra. CO<sub>2</sub> chiếm chỗ của oxy nên lượng oxy còn lại không đủ để duy trì đám cháy. Nó cũng cung cấp một số yếu tố làm mát trong vùng cháy và làm giảm nồng độ của nhiên liệu “đã được khí hóa”.

Khí Argon dập lửa bằng cách giảm nồng độ oxy xuống dưới mức 15% cần thiết để các vật dụng dễ cháy bùng cháy. Hệ thống Argon được thiết kế để giảm hàm lượng oxy xuống khoảng 12,5%, thấp hơn mức 15% cần

thiết cho đám cháy nhưng vẫn cao hơn 10% theo yêu cầu của EPA đối với sự an toàn của con người.

Inergen, một sản phẩm của Ansul Corporation, được cấu thành từ ba loại khí: 52% nitơ, 40% argon và 8% carbon dioxide. Theo cách tương tự như hệ thống argon tinh khiết, hệ thống Inergen giảm mức oxy xuống khoảng 12,5%, đủ cho sự an toàn của con người nhưng không đủ để duy trì một đám cháy.

### Các Bình Chữa cháy Cầm tay

Mặc dù các chuyên gia bảo mật máy tính thường không có nhiều ảnh hưởng đến loại hệ thống dập lửa mà văn phòng của họ bao gồm nhưng họ cần phải biết loại nào đã được thiết lập, những gì họ nên làm trong trường hợp khẩn cấp và những gì họ cần làm gì để khôi phục sau khi hệ thống đi vào hoạt động. Tuy nhiên, một lĩnh vực mà họ có thể ảnh hưởng là loại bình chữa cháy cầm tay được đặt trong khu vực của họ (xem Bảng 15-1).

<b>Phân loại Đám cháy</b>	<b>Kiểu Đám cháy</b>	<b>Ví dụ về Chất dễ cháy</b>	<b>Vật liệu Mẫu của Phương pháp Nén</b>
A	Chất cháy thông thường	Gỗ, giấy, quần áo, nhựa	Nước hoặc hóa chất khô
B	Chất lỏng dễ cháy	Sản phẩm dầu mỏ, dung môi hữu cơ	CO2 hoặc hóa chất khô
C	Điện	Cáp và thiết bị điện, các công cụ năng lượng	CO2 hoặc hóa chất khô
D	Kim loại dễ cháy	Magnesium, titanium	Kim loại đồng hoặc Natri clorua

**Bảng 14-1** Các loại Hỏa hoạn và Phương pháp Chữa cháy

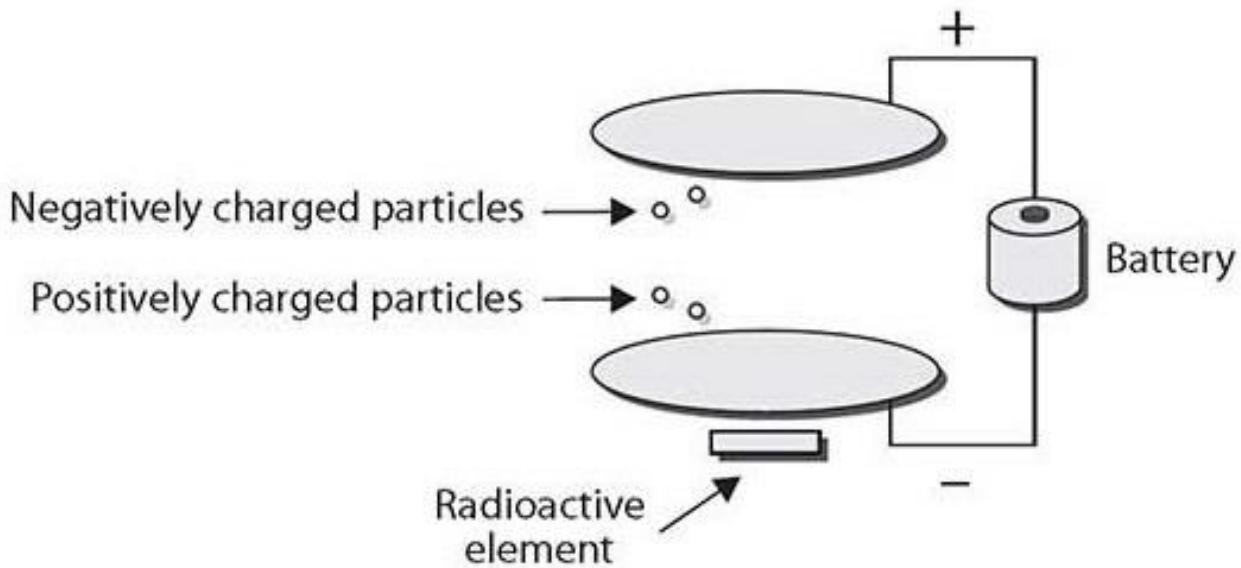
Hệ thống chữa cháy tự động được thiết kế để phỏng ra khi đám cháy được phát hiện không phải là hệ thống duy nhất bạn nhận thức được. Nếu đám cháy có thể được phát hiện và dập tắt trước khi hệ thống tự động hoạt động, điều đó có thể giúp tổ chức tiết kiệm đáng kể cả về thời gian và chi phí thiết bị (bao gồm cả việc nạp lại hệ thống tự động). Bình chữa cháy cầm tay rất thông dụng trong các văn phòng, nhưng cách sử dụng đúng đắn phải được hiểu rõ, nếu không, thảm họa có thể xảy ra.

### **Thiết bị Phát hiện Cháy**

Một thành phần bổ sung cần thiết cho các hệ thống và thiết bị dập lửa là các thiết bị phát hiện cháy (đầu dò báo cháy). Các thiết bị phát hiện có thể phát hiện đám cháy ngay trong giai đoạn ban đầu của nó, trước khi hệ thống chữa cháy được kích hoạt và phát ra âm thanh cảnh báo có khả năng cho phép nhân viên giải quyết đám cháy trước khi nó trở nên đủ nghiêm trọng để thiết bị chữa cháy hoạt động.

Có một số loại đầu dò báo cháy khác nhau. Một loại, trong đó có hai biến thể, được kích hoạt bằng khói. Hai loại máy dò khói là ion hóa và quang điện. Một đầu dò quang điện rất tốt để có khả năng đưa ra cảnh báo trước về một đám cháy đang âm ỉ. Loại thiết bị này giám sát chùm ánh sáng bên trong. Nếu có thứ gì đó làm suy giảm ánh sáng (ví dụ, băng cách cản trở nó), máy dò sẽ cho rằng đó là thứ giống như khói và âm thanh báo động sẽ phát ra. Một kiểu đầu dò ion hóa sử dụng một buồng ion hóa và một nguồn phóng xạ nhỏ để phát hiện những đám cháy đang cháy nhanh. Được thể hiện trên hình 15-5, buồng bao gồm hai đĩa: một đĩa mang điện tích dương và một đĩa mang điện tích âm. Các phân tử oxy và nitơ trong không khí trở nên "ion hóa" (một ion được giải phóng khỏi phân tử). Ion giải phóng mang điện tích âm bị hút về bản dương, phần còn lại của phân tử mang điện tích dương bị hút về bản âm. Sự chuyển động này của các hạt tạo ra một dòng điện rất nhỏ mà thiết bị đo được.

Khói [có khả năng phát ra từ đám cháy] làm cản trở quá trình này, và máy dò sẽ phát hiện sự sụt giảm của dòng điện và sẽ phát ra âm thanh báo động.



**Hình 15-5** Một buồng ion hóa dành cho một loại đầu dò báo khói ion hóa Cả hai thiết bị này thường được gọi chung là thiết bị phát hiện khói, và sự kết hợp cả hai loại là hoàn toàn khả thi. Để biết thêm thông tin về thiết bị phát hiện khói, hãy truy cập trang web tại địa chỉ <http://home.howstuffworks.com/homeimprovement/family-safe/fire/smoking2.htm>. Vì cả hai thiết bị này đều được kích hoạt bởi sự gián đoạn của tín hiệu mà không cần biết lý do tại sao nên chúng có thể đưa ra cảnh báo sai. Chúng không thể phân biệt được sự khác nhau giữa khói từ bếp lửa và bánh mì bị nướng cháy.

Một loại đầu báo cháy khác được kích hoạt bằng nhiệt. Các thiết bị này cũng có hai biến thể. Các thiết bị có nhiệt-độ-cố-định hoặc điểm-cố-định sẽ kích hoạt nếu nhiệt độ trong khu vực vượt quá một số đã được xác định trước. Các thiết bị đo tốc-độ-gia-tăng hoặc tốc-độ-gia-tăng-nhiệt-

độ kích hoạt khi có sự gia tăng đột ngột về nhiệt độ cục bộ có thể chỉ ra các giai đoạn ban đầu của đám cháy. Các cảm biến tốc độ gia tăng có thể cung cấp cảnh báo sớm hơn nhưng cũng chịu trách nhiệm cho nhiều cảnh báo sai hơn.

Loại máy dò thứ ba được kích hoạt bằng ngọn lửa. Loại thiết bị này dựa vào ngọn lửa từ đám cháy để cung cấp sự thay đổi năng lượng hồng ngoại có thể phát hiện được. Các thiết bị kích-hoạt-bởi-ngọn-lửa thường đắt hơn hai loại còn lại nhưng thường có thể phát hiện đám cháy sớm hơn.

### Các Cảm biến

Một trong những đề mục đầu tiên trong phương trình bảo mật là phát hiện. Việc phát hiện một tín hiệu cụ thể sau đó có thể được so sánh với một điều kiện tham chiếu xem nó có được chấp thuận hay không. Phần tử cảm biến cung cấp khía cạnh phát hiện cho hệ thống bảo mật, cho phép đưa ra các quyết định và quy trình kết quả. Ví dụ: một máy dò chuyển động được đào tạo để phát hiện lưu lượng đang tới có thể cảm nhận được ai đó đang đi sai đường trong đường hầm hoặc không gian lối ra đã được kiểm soát.

### Phát hiện Chuyển động

Khi giám sát một khu vực có hoạt động trái phép, một công cụ hữu ích tiềm năng là một *máy phát hiện chuyển động*. Ở những khu vực có ít hoặc không có lưu lượng như dự kiến, một máy phát hiện chuyển động có thể cảnh báo cho người kiểm soát về hoạt động trong khu vực. Máy dò chuyển động có nhiều loại, nhưng hầu hết đều dựa trên bức xạ hồng ngoại (nhiệt) và có thể phát hiện ra những thay đổi của thân nhiệt đang chuyển động. Chúng có thể được điều chỉnh kích thước, bỏ qua chuyển động nhỏ hơn chẳng hạn như động vật nhỏ trong môi trường ngoài trời. Mặc dù không hữu ích trong các tòa nhà văn phòng bận rộn trong quá trình sử dụng bình thường hàng ngày, nhưng thiết bị phát hiện chuyển động có thể hữu

ích trong những thời điểm ngoài-giờ-làm-việc, khi giao thông ở mức tối thiểu. Máy dò chuyển động có thể được sử dụng để kích hoạt hệ thống video, vì vậy chúng không ghi lại lượng lớn hoạt động “trống - empty”. Hệ thống video giám sát khu vực bến xếp hàng ở phía sau tòa nhà có thể được kích hoạt theo cách này, bằng cách sử dụng bộ máy phát hiện chuyển động để bật camera bất cứ khi nào có hoạt động.

### **Phát hiện Tiếng ồn**

*Phát hiện tiếng ồn* là một phương pháp cảm biến để lắng nghe những âm thanh cụ thể. Những thứ bình thường có thể tạo ra những âm thanh khác nhau và mỗi thứ này có thể có một dấu hiệu quang phổ cụ thể có thể được sử dụng để lắng nghe một số mục trong khi bỏ qua những mục khác. Kính vỡ có một âm thanh cụ thể và các cảm biến có thể được điều chỉnh để “nghe thấy” tiếng vỡ của kính và đưa ra cảnh báo khi việc này xảy ra. Việc sử dụng các cảm biến được nhắm mục tiêu đến các sự kiện như vậy và cung cấp thông tin cho bảng điều khiển báo động trung tâm có thể làm gia tăng đáng kể tính hiệu quả của nhân viên an ninh trong việc giám sát một cơ sở lớn hơn.

### **Đầu đọc Tiệm cận**

Đầu đọc tiệm cận là cảm biến cung cấp tín hiệu ở một khoảng cách được xác định. Ứng dụng phổ biến nhất trong số này là đầu đọc thẻ được kết nối với cửa ra vào: bạn “quẹt” thẻ của mình bằng cách đặt thẻ gần đầu đọc và nếu mã chính xác, bạn được cấp quyền truy cập. Tuy nhiên, những thiết bị này có tiện ích lớn hơn nhiều. Một loạt các đầu đọc tiệm cận nằm rải rác trong một cơ sở có thể hoạt động như một cảm biến báo cáo, giám sát các nhân viên bảo vệ khi họ đi qua các vòng được chỉ định của họ. Bảo vệ có thể kiểm tra từng điểm bằng cách tương tác với đầu đọc ở gần, thường bằng cách vuốt thẻ gần thiết bị và thiết bị ghi lại sự hiện diện của họ tại địa điểm đó vào thời điểm đó. Với giao tiếp trường gần (near

field communication - NFC) và Bluetooth tiên tiến qua điện thoại thông minh, việc sử dụng đầu đọc tiệm cận ngoài việc chỉ trả tiền cho mọi thứ đang tăng dần lên theo cấp số nhân. Ví dụ, các thiết bị ở gần các trạm dừng xe buýt có thể cho phép điện thoại thông minh của bạn cập nhật lịch trình xe buýt. Khả năng cảm nhận và giao tiếp trong khoảng cách ngắn gần như là vô tận.

### **Phát hiện Độ ẩm**

Độ ẩm, hoặc hơi nước, có thể có những tác động bất lợi đáng kể đối với một số vật dụng nhất định. Cảm biến phát hiện độ ẩm cung cấp một phương tiện từ xa để giám sát mọi thứ, từ rò rỉ nước đến các vấn đề về độ ẩm. Nước có thể gây ra hư hỏng cho các thiết bị điện tử, tác phẩm nghệ thuật và nhiều vật dụng khác. Khả năng giám sát độ ẩm cung cấp cho đội an ninh một phương tiện phát hiện hư hỏng tiềm ẩn từ các vật dụng như đầu voi phun bị rò rỉ hoặc rò rỉ nước. Như trong tất cả các cảm biến, mục tiêu là cung cấp “tai mắt” tốt hơn cho nhân viên an ninh, cho phép đưa tin 24/7 về các vấn đề, nhiều lần ở những khu vực hẻo lánh, đối với những điều kiện có thể cần đến sự chú ý.

### **Thẻ**

Việc kiểm soát quyền truy cập vật lý vào một cơ sở nhỏ có thể đạt được thông qua khóa cửa và chìa khóa vật lý, nhưng giải pháp đó khó sử dụng đối với các cơ sở lớn hơn với rất nhiều người ra vào. Nhiều tổ chức dựa vào hệ thống huy hiệu bằng cách sử dụng các *token* hoặc *thẻ* có thể được liên kết với việc kiểm tra ID tự động và ghi nhật ký vào/ra. Việc này có thể cung cấp chi tiết hơn nhiều trong việc theo dõi ai đang ở cơ sở và thời điểm họ đến và đi. Mã thông báo và thẻ có thể cung cấp một ID được tuân tự hóa cho mỗi người dùng, cho phép ghi nhật ký cho-từng-người-dùng-cụ-thể. Ban đầu được thiết kế để tăng cường thẻ chấm công tính lương, các ID điện tử này đã cải thiện tính bảo mật thông qua việc ghi

lại nhặt ký thời gian ra vào của nhân viên. Mã thông báo và thẻ cung cấp chức năng tương tự như khóa, nhưng hệ thống có thể được cập nhật từ xa để quản lý quyền truy cập theo thời gian thực và người dùng có thể bị thu hồi đặc quyền của họ mà không cần công ty hoặc quản trị viên phải khôi phục lại mã thông báo hoặc thẻ.

## Nhiệt độ

Các cảm biến *nhiệt độ* hoạt động chính xác như những gì bạn nghĩ: chúng cảm nhận nhiệt độ. Một phần của phương trình bảo mật vật lý là ngăn ngừa thiệt hại đối với cơ sở hạ tầng trong tổ chức và máy chủ có thể là một phần quan trọng của cơ sở hạ tầng đó. Phòng máy chủ là khu vực được kiểm-soát-nhiệt-độ-rất-cao, có cả hai thái cực nóng và lạnh, vì máy chủ có xu hướng tạo ra nhiệt và nhiệt đó cần phải được loại bỏ. Các lỗi đi có nhiệt độ nóng và lạnh sẽ được đề cập chi tiết hơn trong phần sau của chương này. Việc theo dõi nhiệt độ hiện tại trong các phòng máy chủ yêu cầu phải có các cảm biến nhiệt độ, được đặt đúng vị trí để đo nhiệt độ thực tế mà máy chủ phải trải qua. Sau đó, một giải pháp giám sát phân tích có thể cảnh báo cho nhân sự thích hợp khi các phạm vi nhiệt độ nhất định bị vượt quá. Trong các cơ sở nhỏ, một cảm biến cho toàn bộ căn phòng có thể là đủ, trong các khu vực máy chủ lớn hơn, có thể có một cảm biến trên mỗi tủ rack. Trong mọi trường hợp, ý tưởng là giống nhau: đo nhiệt độ và báo cáo về các trường hợp ngoại lệ.



**MÁCH NƯỚC CHO KỲ THI** Sử dụng các cảm biến như một phần của một giải pháp bảo mật vật lý tổng thể là điều quan trọng. Có rất nhiều thứ cần phải được giám sát, và sử dụng các cảm biến tự động hóa để hỗ trợ cho nhóm bảo mật trong việc tìm kiếm những điều kiện ngoại lệ là điều quan trọng. Mục tiêu là tìm hiểu tầm quan trọng của bảo mật vật lý,

và điều đó bao gồm những chi tiết cụ thể đã được đo lường bởi các cảm biến.

### **Thiết bị bay không người lái**

Việc sử dụng *thiết bị bay không người lái* đã tăng mạnh trong vài năm qua. Từ các kiểu máy gia đình/theo sở thích có thể mang theo một máy ảnh nhỏ, đến các giàn công nghiệp lớn hơn có thể mang những máy ảnh lớn hơn trong thời gian dài hơn, các thiết bị này đã tạo ra một cuộc cách mạng trong việc xem xét các đề mục từ xa. Thiết bị bay không người lái được các tuyến đường sắt sử dụng để kiểm tra đường ray và được các công ty điện lực sử dụng để kiểm tra đường dây điện. Khả năng đi đến hầu hết mọi nơi và kiểm tra mọi thứ một cách trực quan là một nguồn tài nguyên tuyệt vời. Những thiết bị này cung cấp các trường hợp sử dụng thú vị cho cả tội phạm và phòng thủ trong an ninh mạng vì chúng có thể được sử dụng để khảo sát cơ sở vật chất từ xa, cung cấp các mắt quan sát theo yêu cầu ở nhiều nơi mà bạn có thể sẽ không muốn một người đi đến đó và trong khung thời gian không thể được đáp ứng theo bất kỳ cách thức nào khác.

### **Nhật ký Khách viếng thăm**

*Nhật ký khách truy cập* bảo mật vật lý cung cấp tiện ích tương tự như các nhật ký máy tính để điều tra bảo mật. Chúng hoạt động như một hồ sơ ghi lại những gì đã quan sát được tại những thời điểm cụ thể. Việc có được các nhân viên bảo vệ lưu động kiểm tra tại các địa điểm khác nhau trong một ca làm việc thông qua một mục nhập nhật ký cung cấp hồ sơ giám sát thực tế. Các nhật ký của khách đến và đi, thiết bị được nhận vào và vận chuyển đi, v.v... đóng vai trò như một hồ sơ về những diễn biến thực tế trong một cơ sở.

Cảm biến từ xa về các huy hiệu và thiết bị bằng cách sử dụng thẻ RFID có thể tạo ra một nhật ký tự động về việc di chuyển của thiết bị, bao

gồm thông tin về thời gian, địa điểm, cái gì và ai. Những khả năng nâng cao như vậy giúp việc kiểm kê thiết bị có thể di chuyển được dễ dàng hơn, khi vị trí của thiết bị được theo dõi và có thể được quét từ xa.



**MÁCH NƯỚC CHO KỲ THI** Các camera, phát hiện IR, phát hiện chuyển động, và các nhặt ký là tất cả những phương pháp liên quan đến phát hiện – và thường xuyên phát hiện sau-khi-sự-việc-xảy-ra tại đó. Những thiết bị và phương pháp này cung cấp những hình mẫu thực tế phân bổ có giá trị, thậm chí ngay cả khi sự kiện thực tế đã diễn ra.

### Lồng Faraday

Nhiều điện từ (EMI) là một nhiễu loạn điện gây ảnh hưởng đến một mạch điện. EMI là do cảm ứng điện từ hoặc bức xạ phát ra từ nguồn bên ngoài, một trong hai nguồn này có thể tạo ra dòng điện đi vào các mạch nhỏ tạo nên hệ thống máy tính và gây ra rối loạn về mặt logic. EMI có thể gây hại cho bất kỳ loại thiết bị điện tử nào, nhưng mật độ của kết cấu mạch điện trong trung tâm dữ liệu điển hình có thể khiến cho nó trở thành nơi trú ẩn của EMI. Độ nhạy đối với trường EMI phụ thuộc vào một số yếu tố, bao gồm cả chiều dài của mạch, có thể hoạt động giống như một ăng-ten. EMI được nhóm thành hai loại chung: băng thông hẹp và băng thông rộng. Băng thông hẹp, về bản chất, là năng lượng điện từ có dải tần số nhỏ và do đó, thường có nguồn từ một thiết bị truyền có mục đích trong dải tần được chỉ định, chẳng hạn như điện thoại. Băng thông rộng bao gồm một dải tần số rộng hơn và thường được gây ra bởi một số kiểu sử dụng năng lượng điện thông thường như đường dây điện hoặc động cơ điện.

Một ví dụ về việc che chắn có thể được sử dụng là *lồng Faraday* hoặc *tấm chắn Faraday*, là một vỏ bọc bằng vật liệu dẫn điện được nối đất. Điều

này có thể có kích-cỡ-phòng hoặc được xây dựng trong một tòa nhà, yếu tố quan trọng là không có khe hở đáng kể trong vật liệu bao vây. Các biện pháp này có thể giúp che chắn EMI, đặc biệt là trong môi trường tần-số-vô-tuyến-cao. Lồng Faraday có thể có kích thước cụ thể theo từng hạng mục, vì vậy các hệ thống nhỏ hơn có thể chứa chỉ một chiếc điện thoại thông minh cũng đang có sẵn.



**MÁCH NƯỚC CHO KỲ THI** Khi nói đến che chắn, hãy tìm hiểu sự khác biệt giữa một lồng Faraday (như một không gian mở lớn) và lá chắn EMI trên các dây cáp (che chắn rất cụ thể) và loại nào phù hợp dựa trên những gì đang được bảo vệ khỏi EMI.

### Khe hở Không khí

*Khe hở không khí* là một thuật ngữ được sử dụng để mô tả sự tách biệt về mặt vật lý và luận lý của một mạng với tất cả các mạng khác. Sự tách biệt này được thiết kế để ngăn chặn việc truyền dữ liệu trái phép đến và đi từ mạng. Lỗi hỏng trong logic này là người dùng sẽ di chuyển dữ liệu bằng các phương tiện khác, chẳng hạn như ổ USB, để hoàn thành công việc của họ. Thường được gọi là “lưới giày thể thao”, hành vi vượt qua khe hở không khí trái phép này, mặc dù bề ngoài với mục đích hoàn thành nhiệm vụ, làm gia tăng rủi ro hệ thống vì nó cũng bỏ qua quá trình kiểm tra, ghi nhật ký và các quy trình khác quan trọng trong quá trình phát triển và triển khai.

### Mạng con được Sàng lọc

Khái niệm về một mạng con được sàng lọc (trước đây được gọi là khu phi quân sự [DMZ]) xuất phát từ cách nói quân sự, trong đó nó đại diện cho một khu vực không thuộc “sở hữu” của cả hai bên. Khái niệm này được sử dụng trong mạng để chỉ một khu vực mà kiểm soát truy cập không

chặt chẽ như bên trong hoặc mở như bên ngoài, là nơi hợp tác chung và rủi ro được kiểm soát. Khái niệm tương tự này hoạt động trong các cấu trúc vật lý, nơi tiền sảnh giống như thế giới bên ngoài và bất kỳ ai cũng có thể bước vào, sau đó là các hành lang chung để các nhân viên hòa nhập và cuối cùng là các văn phòng đặc biệt và phòng máy chủ, nơi truy cập được kiểm soát một cách chặt chẽ. Các khu vực làm việc chung cũng giống như DMZ - một khu vực nơi rủi ro được kiểm soát.

### **Phân phối Cáp được Bảo vệ**

Cáp chạy giữa các hệ thống cần phải được bảo vệ khỏi thiệt hại về mặt vật lý đối với cáp và các lõi giao tiếp sau đó. Điều này được thực hiện nhờ hệ thống *phân phối được bảo vệ/cáp được bảo vệ* trong quá trình lắp đặt cáp. Đây có thể đơn giản như ống kim loại hoặc ống bê tông phức tạp để chạy cáp ngầm. Mục tiêu là để ngăn chặn bất kỳ thiệt hại về mặt vật lý nào đối với phần lớp vật lý của hệ thống. Hệ thống phân phối được bảo vệ/cáp được bảo vệ cung cấp các biện pháp bảo vệ vật lý đối với hệ thống cáp giữa các hệ thống, khỏi tất cả các mối đe dọa vật lý, bao gồm cả việc đánh chặn và khai thác. Việc bọc che chắn cáp, chẳng hạn như cáp xoắn đôi được bảo vệ, được thiết kế để ngăn nhiễu điện từ ảnh hưởng đến tín hiệu trên các lõi trong cáp. Việc bảo vệ toàn bộ hệ thống đã được đề cập trong phần trước "Lồng Faraday".

### **Khu vực An ninh**

Những *khu vực an ninh* là những khu vực mà các biện pháp phòng ngừa cụ thể được triển khai để kiểm soát việc tiếp cận cả hai chiều đến và đi. Giống như nhiều cấu trúc bảo mật vật lý khác, có một loạt các cấp độ dành cho những khu vực an ninh. Từ những khu vực được tạo ra bởi một cánh cửa khóa đơn giản, đến những khu vực có thủ tục và bảo vệ đặc biệt, các khu vực an ninh có thể được điều chỉnh để phù hợp với nhu cầu an ninh của một doanh nghiệp. Ý tưởng tổng thể đằng sau một khu vực

an ninh là hạn chế thông tin và dòng người ra vào khu vực, và khi được phép, nó sẽ được kiểm soát ở mức độ thích hợp. Cơ quan Quản lý An ninh Giao thông vận tải (Transport Security Administration - TSA) tạo ra một khu vực an ninh khi bạn đến sân bay bằng cách chỉ cho phép một số vật liệu và người đi qua trạm kiểm soát.

### Khe hở Không khí

Như đã đề cập trước đây, thuật ngữ *khe hở không khí* được sử dụng để chỉ một hệ thống không có kết nối trực tiếp với các hệ thống bên ngoài. Mạng khe-hở-không-khí không có kết nối với các mạng bên ngoài. Một khe hở không khí cho một mạng mở rộng ra đến tất cả các kết nối vật lý, có dây và không dây, tồn tại để bảo vệ máy tính hoặc mạng khỏi các ảnh hưởng từ bên ngoài hoặc giữ cho dữ liệu không rời khỏi hệ thống. Về nguyên tắc thì trông có vẻ đơn giản nhưng thực tế lại khó hơn nhiều. Nếu một hệ thống bị cô lập, làm thế nào để dữ liệu được đi vào? Bạn sẽ làm gì với kết quả? Làm cách nào để bạn duy trì hệ thống, cung cấp các bản cập nhật, v.v...? Trong thực tế, khi các khe hở không khí được sử dụng, chúng phải theo dõi các kết nối xảy ra xung quanh chúng để đảm bảo hệ thống vẫn được cô lập.



### MÁCH NƯỚC CHO KỲ THI

CompTIA liệt kê khe hở không khí hai lần trong Mục tiêu 2.7, do đó hãy xem như bạn đã được cảnh báo. Một khe hở không khí là một biện pháp bảo mật được triển khai để đảm bảo rằng các hệ thống trong một mạng bảo mật được cách ly hoàn toàn (không được kết nối) khỏi một mạng không bảo mật như Internet.

### Hầm

*Hầm* là một khu vực an toàn được thiết kế để cung cấp một mức độ bảo mật cụ thể cho những gì được lưu trữ bên trong. Đây có thể là một không

gian vật lý, với các biện pháp bảo vệ cụ thể như tường không thể xâm nhập và các cửa có thể được bảo vệ. Hầm là một hạng mục lớn hơn hầu hết các két an toàn, thường có kích thước phòng. Ví dụ, một hầm tại ngân hàng được sử dụng để lưu trữ một lượng lớn tiền và các vật có giá trị khác.

### Két an toàn

*Két an toàn* là những thiết bị lưu trữ vật lý nhằm mục đích ngăn chặn truy cập trái phép vào những nội dung được bảo vệ của chúng. Két an toàn có hình dạng, kích thước và giá thành khác nhau. Mức độ bảo vệ khỏi môi trường vật lý càng cao thì mức độ bảo vệ chống lại sự truy cập trái phép càng tốt. Các két an toàn không hoàn hảo, trên thực tế, chúng được đánh giá dựa trên thời gian chúng có thể được kỳ vọng để bảo vệ nội dung bên trong khỏi trộm cắp hoặc hỏa hoạn trong bao lâu. Đánh giá càng tốt thì két sắt càng đắt tiền.

Đôi khi két sắt hoạt động quá mức cần thiết, cung cấp mức độ bảo mật cao hơn mức thực sự cần thiết. Một giải pháp đơn giản hơn là *tủ an toàn* và *hàng rào an toàn*. Tủ và hàng rào an toàn cung cấp cho chủ sở hữu hệ thống một địa điểm để cất giữ tài sản cho đến khi sử dụng chúng. Hầu hết các tủ/hàng rào an toàn không cung cấp tất cả các cấp độ bảo vệ mà người ta có được với két sắt, nhưng chúng có thể khá hữu ích, đặc biệt khi khối lượng lưu trữ an toàn là khá lớn.

Hàng rào an toàn có thể cung cấp mức bảo mật chống lại một số hình thức truy cập vật lý, như đối với người dùng, nhưng vẫn cung cấp các biện pháp kiểm soát môi trường thích hợp và cài đặt cần thiết cho hoạt động. Két an toàn thường không thể cung cấp các cấp kiểm soát này.

## Các gian Nóng và Lạnh

Xu hướng hướng tới các máy chủ nhỏ hơn, dày đặc hơn có nghĩa là nhiều máy chủ và thiết bị hơn được đặt trên mỗi tủ rack, gây ra tải trọng lớn hơn cho hệ thống làm mát. Điều này khuyến khích việc sử dụng bố trí lối đi nóng/lối đi lạnh. Một trung tâm dữ liệu được bố trí thành các *lối đi nóng và lạnh* quy định rằng tất cả các quạt hút trên tất cả các thiết bị đều hướng ra lối đi lạnh và các quạt đẩy đều hướng ra lối đi đối diện. Hệ thống HVAC sau đó được thiết kế để đẩy không khí mát bên dưới sàn nâng lên thông qua các tấm gạch đục lỗ trên lối đi lạnh. Không khí nóng từ lối đi nóng được thu nhận bằng các ống dẫn khí hồi cho hệ thống HVAC. Việc sử dụng cách bố trí này được thiết kế để kiểm soát luồng không khí, với mục đích không bao giờ giòi trộn lẫn không khí nóng và lạnh. Điều này đòi hỏi phải sử dụng các tấm chặn và tấm bên cạnh để đóng các khe mở trên tủ rack. Lợi ích của cách sắp xếp này là làm mát hiệu quả hơn và có thể xử lý mật độ cao hơn.



**LƯU Ý** Việc hiểu được luồng không khí cho phép bạn hiểu các lối đi nóng và lạnh. Không khí lạnh được tạo ra bởi thiết bị HVAC, và không khí lạnh này được gửi đến các máy chủ. Các máy chủ tỏa ra nhiệt, khiến cho không khí nóng hơn, điều này sẽ bị loại bỏ. Các lối đi giúp không khí nóng trộn lẫn với không khí lạnh, giúp làm mát hiệu quả. Bạn sẽ không mở cửa vào mùa hè với điều hòa không khí bật, phải không?



**MÁCH NƯỚC CHO KỲ THI** Hãy hiểu và có khả năng giải thích về tầm quan trọng của những khu vực bảo mật như khe hở không khí, hầm, két an toàn và lối đi lạnh.

## **Phá hủy Dữ liệu An toàn**

Khi dữ liệu đã không còn được sử dụng, cho dù là trên các bản in đã cũ, hệ thống cũ bị loại bỏ hoặc thiết bị đã bị hư hỏng, điều quan trọng là phải phá hủy dữ liệu trước khi mất quyền kiểm soát về vật lý đối với phương tiện mà nó đang sử dụng. Nhiều tội phạm đã học được giá trị của việc đào sâu trong thùng rác để khám phá thông tin có thể được sử dụng trong các hành vi trộm cắp danh tính, kỹ thuật xã hội và các hoạt động độc hại khác. Một tổ chức phải quan tâm không chỉ đến thùng rác giấy tờ, mà còn cả thông tin được lưu trữ trên các đồ vật bị loại bỏ như máy tính. Một số tổ chức chính phủ đã phải bối rối khi các máy tính cũ được bán cho những người cứu hộ đã được chứng minh là có chứa các tài liệu nhạy cảm trên ổ cứng của họ. Điều quan trọng đối với mọi tổ chức là phải có một chính sách xử lý và tiêu hủy mạnh mẽ và các thủ tục liên quan. Phần này bao gồm các phương pháp phá hủy dữ liệu và làm sạch phương tiện.

### **Đốt (Burning)**

*Đốt* được coi là một trong những phương pháp phá hủy dữ liệu tiêu-chuẩn-vàng. Một khi phương tiện lưu trữ được chuyển thành dạng có thể bị hỏa hoạn phá hủy, các quá trình hóa học của lửa là không thể đảo ngược được và khiến cho dữ liệu bị mất đi vĩnh viễn. Phương pháp điển hình là cắt nhỏ vật liệu, thậm chí cả đĩa nhựa và ổ cứng (bao gồm cả SSD), sau đó đưa vật liệu đó vào lò đốt và oxy hóa vật liệu trở lại dạng hóa học cơ bản. Khi vật liệu bị đốt cháy hoàn toàn, thông tin trên đó sẽ hoàn toàn biến mất.

### **Băm nhỏ (Shredding)**

*Băm nhỏ* là sự phá hủy về mặt vật lý bằng cách xé nhỏ một món đồ thành nhiều mảnh nhỏ, sau đó có thể trộn lẫn chúng lại với nhau, khiến việc tổ hợp lại sẽ rất khó khăn nếu không muốn nói là không thể. Các giấy tờ quan trọng nên được cắt nhỏ, và điểm *quan trọng* trong trường hợp này

có nghĩa là bất cứ thứ gì có thể hữu ích đối với kẻ xâm nhập tiềm ẩn hoặc kẻ đào bới thùng rác. Thật đáng kinh ngạc về những gì những kẻ xâm nhập có thể làm với những gì trông có vẻ dường như là những mẩu thông tin vô hại. Máy hủy có đủ loại kích cỡ, từ các kiểu máy tính để bàn nhỏ có thể xử lý một vài trang [tài liệu giấy tờ] cùng một lúc, hoặc một đĩa CD/DVD, đến các phiên bản công nghiệp có thể xử lý ngay cả danh bạ điện thoại và nhiều đĩa cùng một lúc. Máy hủy tài liệu công nghiệp tối ưu có thể hủy cả ổ đĩa cứng, vỏ kim loại và tất cả. Rất nhiều công ty tiêu hủy tài liệu có các máy hủy tài liệu lớn hơn trên xe tải mà họ mang đến địa điểm của khách hàng và hủy tài liệu tại-chỗ theo một lịch trình thường xuyên.

### **Nghiền nát (Pulping)**

*Nghiền nát bột giấy* là một quá trình mà khi đó các sợi giấy được trộn lẫn trong chất lỏng và kết hợp lại thành giấy mới. Nếu bạn có hồ sơ dữ liệu trên giấy và bạn đã cắt nhỏ giấy, quy trình nghiền nát sẽ loại bỏ dấu vết mực in bằng cách tẩy trắng và kết hợp tất cả các mảnh giấy đã cắt thành giấy mới, phá hủy hoàn toàn bối cảnh vật lý của giấy cũ.

### **Tán nhỏ (Pulverizing)**

*Tán nhỏ* là một quá trình vật lý để phá hủy bằng cách sử dụng lực vật lý quá mức để phá vỡ một vật phẩm thành những mảnh nhỏ không thể sử dụng được. Máy tán được sử dụng đối với các vật phẩm như ổ đĩa cứng, phá hủy đĩa cứng theo cách mà chúng không thể phục hồi được. Một phương pháp hiện đại hơn để tán nhỏ dữ liệu là sử dụng mã hóa. Dữ liệu trên ổ đĩa được mã hóa và chính bản thân khóa sẽ bị phá hủy. Điều này khiến cho dữ liệu trở nên không thể khôi phục được dựa trên độ mạnh của mã hóa. Phương pháp này có lợi thế duy nhất về quy mô, một doanh nghiệp nhỏ có thể nghiền nát dữ liệu của chính mình, trong khi đó, họ sẽ

cần thiết bị đắt tiền hoặc cần đến một bên-thứ-ba để tán nhỏ một vài đĩa mà họ cần tiêu hủy trong mỗi năm.

### **Khử từ (Degaussing)**

Một phương pháp an toàn hơn để phá hủy các tập tin trên các thiết bị lưu trữ từ tính (nghĩa là, các băng và đĩa cứng từ tính) là phá hủy dữ liệu về mặt từ tính, bằng cách sử dụng một từ trường mạnh để khử từ phương tiện. *Khử từ* sắp xếp lại các hạt từ tính, loại bỏ cấu trúc đã được tổ chức đại diện cho dữ liệu. Việc này phá hủy một cách hiệu quả tất cả những dữ liệu trên phương tiện lưu trữ. Một số loại thiết bị khử từ thương mại có sẵn cho mục đích này.

### **Thanh lọc (Purging)**

*Thanh lọc* dữ liệu là một thuật ngữ thường được sử dụng để mô tả các phương pháp xóa và loại bỏ vĩnh viễn dữ liệu ra khỏi không gian lưu trữ. Cụm từ khóa là “loại bỏ dữ liệu”, không giống như xóa (deletion) vốn chỉ hủy dữ liệu, thanh lọc được thiết kế để mở ra không gian lưu trữ để sử dụng lại. Một bộ nhớ đệm hình tròn là một ví dụ tuyệt vời về cơ chế tự động thanh lọc. Nó lưu trữ một lượng phần tử dữ liệu nhất định và sau đó không gian được sử dụng lại. Ví dụ, nếu một bộ đệm tròn chứa 64 MB, khi nó đầy, nó sẽ ghi đè lên tài liệu cũ nhất khi tài liệu mới được thêm vào bộ đệm.

### **Các giải pháp Bên-thứ-ba**

Cũng giống như nhiều thành phần khác của một chương trình bảo mật, có những nhà cung cấp bán việc phá hủy dữ liệu như một dịch vụ. Các nhà cung cấp này có thể tận dụng lợi thế của quy mô, gia tăng khả năng trong khi chia sẻ chi phí của thiết bị. Tuy nhiên, điều này cũng đưa ra một hình thức mất dữ liệu mới, thông qua việc sử dụng bên-thứ-ba có quyền truy cập vào dữ liệu trước khi phá hủy. Và, như với tất cả các mối quan hệ với bên-thứ-ba, những gì được tính đến là những gì có trong hợp

đồng. Do đó, việc xem xét điều kiện bảo mật tốt của các chi tiết trong hợp đồng cần được đảm bảo, không chỉ đối với các vấn đề pháp lý mà còn cả các vấn đề kỹ thuật.



### MÁCH NƯỚC CHO KỲ THI

Phần này đề cập đến một số phương pháp phá hủy dữ liệu/phương tiện lưu trữ, một số phương pháp được sử dụng cùng nhau. Hãy tìm hiểu về những chi tiết của từng phương pháp và tìm kiếm những lựa chọn đáp án bất hợp lý để thu hẹp phạm vi của những đáp án chính xác khả dĩ, chẳng hạn như những tùy chọn đề cập đến việc nghiền nát những vật phẩm không-phải-giấy-tờ hoặc khử từ những phương tiện phi từ tính.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các nguyên tắc về kiểm soát bảo mật vật lý, bao gồm cả kiểm soát môi trường. Chương này bắt đầu bằng cách thảo luận về rào cản/chướng ngại vật, biển báo, camera, CCTV và ngũ trang công nghiệp - tất cả những hạng mục được thiết kế để hạn chế, hướng dẫn hoặc giám sát chuyển động vật lý. Từ đó, chương chuyển sang các nhân viên bảo vệ, lính canh robot, khóa, chiếu sáng, cảm biến, thiết bị bay không người lái/UAV và phân phổi được bảo vệ đối với dây cáp. Các yếu tố này tinh chỉnh thêm các hạn chế về chuyển động và khả năng truy cập vào các thành phần hệ thống. Sau đó, chương này đã xem xét lồng Faraday, khe hở không khí và DMZ. Các khu vực an toàn bao gồm hầm, két, lối đi nóng và lối đi lạnh cũng được đề cập.

Chương này khép lại với việc kiểm tra các phương pháp phá hủy dữ liệu an toàn, bao gồm các giải pháp đốt, cắt nhỏ, khử từ và các giải pháp của bên-thứ-ba.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

- 1.** Tại sao bảo mật vật lý lại là điều quan trọng để bảo vệ dữ liệu?
  - A.** Quyền truy cập vật lý đến dữ liệu sẽ phủ nhận các lợi thế bảo mật của đám mây.
  - B.** Thông tin nằm trên tài sản vật lý, liên kết giữa bảo mật vật lý và bảo mật thông tin.
  - C.** Kỹ thuật xã hội có thể phủ nhận bất kỳ biện pháp kiểm soát bảo mật thông tin nào.
  - D.** Không có đáp án nào đúng.
- 2.** Tại sao ánh sáng nội và ngoại thất thích hợp lại quan trọng?
  - A.** Nó có thể phát hiện những người ở nơi mà đáng lẽ họ không thuộc về.
  - B.** Nó cho biết ai đang ở trong một khu vực không gian bị hạn chế.
  - C.** Nó cho phép quan sát được nhiều người và nhiều hoạt động hơn.
  - D.** Nó là điều cần thiết cho việc sử dụng máy ghi hình mạch-kín.
- 3.** Tổ chức của bạn đã gặp phải nhiều sự cố về việc gắn thẻ graffiti và mọi người lảng vảng trong bãi đậu xe bất chấp hàng rào liên-kết-chuỗi đang bao quanh nó. Giải pháp tốt nhất cho vấn đề là gì?
  - A.** Biển báo "Không xâm phạm"
  - B.** Thêm trạm gác bảo vệ
  - C.** Nguồn chiếu sáng bên ngoài bổ sung
  - D.** Thay đổi hàng rào liên-kết-chuỗi thành hàng rào chống quy mô.

4. Sau một sự cố bảo mật vật lý, nhân viên bảo vệ thường có thể cung cấp những dữ liệu quan trọng nào?
  - A. Thông tin ID nhân viên
  - B. Nhật ký truy cập của những người đã vào và ra khỏi tòa nhà
  - C. Mã báo động
  - D. Bản thiết kế hiển thị các khu vực không được giám sát của tòa nhà.
5. Báo động chỉ có hiệu lực nếu điều nào dưới đây là đúng?
  - A. Chúng cảnh báo về tình trạng bất thường.
  - B. Mọi lối vào đều được giám sát bằng cảm biến.
  - C. Chúng không bị ràng buộc với hệ thống thông tin.
  - D. Chúng được điều chỉnh để cung cấp các cảnh báo chính xác và hữu ích.
6. Bạn đang triển khai một phòng thí nghiệm thử nghiệm tại tổ chức của mình để phát triển một phần mềm alpha ban đầu. Để ngăn chặn bất kỳ mã phát triển nào vô tình được đưa vào máy tính sản xuất, bạn nên thực hiện những gì?
  - A. Khe hở không khí
  - B. Tường lửa nghiêm ngặt
  - C. Phân phối được bảo vệ
  - D. Quản lý bản vá lỗi.
7. Lợi ích bảo mật của lồng Faraday là gì?
  - A. Ngăn chặn cuộc tấn công bởi EMP
  - B. Ngăn chặn việc truy cập vào một thiết bị bằng mạng không dây hoặc kết nối di động
  - C. Hoạt động tốt hơn hàng rào chống quy mô
  - D. Ngăn chặn việc tràn ngasket bởi EMI.
8. Ví dụ về mạng con được sàng lọc dựa-trên-con-người (DMZ) là gì?

- A.** Sảnh của khách được nhân viên lễ tân ngăn cách với văn phòng công ty
- B.** Hành lang giữa tiền sảnh của công ty và các văn phòng
- C.** Một phòng máy chủ có cửa khóa
- D.** Các tủ mạng trong cơ sở
- 9.** Vấn đề chính với sinh trắc học là gì?
- A.** Về mặt kỹ thuật, sinh trắc học rất khó thực hiện.
- B.** Cơ thể con người thay đổi theo thời gian.
- C.** Sinh trắc học dễ bị làm giả.
- D.** Sinh trắc học không thể được cho mượn hoặc ủy quyền.
- 10.** Bạn nên làm gì để bảo vệ hệ thống CCTV dựa-trên-IP của mình khỏi cuộc tấn công DDoS?
- A.** Thiết lập cấu hình lại tường lửa của bạn.
- B.** Kết nối nó với một hệ thống phát hiện xâm nhập.
- C.** Yêu cầu xác thực đa yếu tố để truy cập hệ thống CCTV.
- D.** Đặt tất cả các thành phần camera quan sát trên một mạng riêng biệt.

## Đáp án

1. **B.** Thông tin nằm trên các tài sản vật lý, liên kết giữa bảo mật vật lý với bảo mật của thông tin.
2. **C.** Việc chiếu sáng thích hợp cho phép quan sát được nhiều người và hoạt động hơn.
3. **D.** Thay đổi từ hàng rào liên-kết-chuỗi sang hàng rào chống quy mô để ngăn những kẻ xâm nhập trèo qua hàng rào là giải pháp tốt nhất.
4. **B.** Các nhân viên bảo vệ thường có nhật ký về những ai đã vào và ra khỏi một tòa nhà.
5. **D.** Báo động chỉ có hiệu lực nếu chúng được điều chỉnh để cung cấp thông tin cảnh báo chính xác và hữu ích.
6. **A.** Môi trường phòng thí nghiệm có thể được tạo khe hở không khí với phần còn lại của mạng để ngăn phần mềm vô tình bị sao chép vào máy sản xuất.
7. **B.** Một chiếc lồng Faraday có thể ngăn chặn việc truy cập một thiết bị qua sóng tần số vô tuyến, từ mạng không dây hoặc vô tuyến điện thoại di động.
8. **B.** Tiền sảnh là một phần của môi trường bên ngoài, vì vậy các hành lang là sự lựa chọn tốt hơn. Phòng máy chủ và phòng mạng là những không gian được đảm bảo an toàn hơn.
9. **B.** Một số tính năng sinh trắc học có thể thay đổi theo thời gian hoặc tình trạng y tế có thể khiến chúng kém tin cậy hơn, do đó buộc phải thực hiện giai đoạn nhận-dạng-lại để đồng bộ hóa người dùng và sinh trắc học của họ.
10. **D.** Hệ thống CCTV nên nằm trên một mạng hoàn toàn riêng biệt, được tạo khe hở không khí nếu có thể, và chỉ có nhân viên an ninh mới có quyền truy cập.

## Chương 16 Các Khái niệm Mật mã học

---

### Các Khái niệm Mật mã học

Trong chương này bạn sẽ

- Nhận diện các kiểu mã hóa khác nhau,
  - Tìm hiểu về các phương pháp mã hóa hiện hành,
  - Tìm hiểu cách mã hóa được áp dụng đối với bảo mật,
  - Đưa ra một kịch bản, sử dụng các khái niệm mã hóa chung,
  - So sánh và đối chiếu các khái niệm về mã hóa.
- 

*Mật mã học (cryptography)* là khoa học về *mã hóa (encrypting)*, hoặc che giấu, thông tin - điều mà mọi người đã tìm cách thực hiện kể từ khi họ bắt đầu sử dụng ngôn ngữ. Mặc dù ngôn ngữ cho phép họ giao tiếp với nhau, nhưng những người nắm quyền đã cố gắng để che giấu thông tin bằng cách kiểm soát ai được cách đọc và viết. Cuối cùng, các phương pháp che giấu thông tin phức tạp hơn bằng cách dịch chuyển các chữ cái xung quanh để làm cho văn bản trở nên không thể đọc được đã được phát triển. Các phương pháp phức tạp này là các thuật toán mật mã, còn được gọi là mã hóa (cipher). Từ *mã hóa* xuất phát từ từ *sifr* trong tiếng Ả Rập, có nghĩa là trống hoặc số không (zero).

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 2.8 của kỳ thi CompTIA Security +: Tóm tắt các khái niệm cơ bản về mật mã.

## Những khái niệm Mật mã Tổng quát

Mật mã trong lịch sử rất dễ sử dụng và cũng dễ bị phá vỡ. Bởi vì việc ẩn giấu thông tin vẫn tiếp tục là điều quan trọng, nên các mật mã thay thế và chuyển vị tiên tiến hơn là điều cần thiết. Khi các hệ thống và công nghệ trở nên ngày càng phức tạp, mật mã thường được tự động hóa bằng một số thiết bị cơ hoặc điện. Một ví dụ nổi tiếng về mã hóa hiện đại là máy Enigma của Đức từ Thế chiến thứ hai. Cỗ máy này đã sử dụng một loạt các thay thế phức tạp để thực hiện việc mã hóa, và điều thú vị là nó đã làm này sinh ra những nghiên cứu sâu rộng về máy tính.

Khi thiết lập một lược đồ mật mã, điều quan trọng là phải sử dụng các công nghệ đã được chứng minh. Thư viện mật mã đã được chứng minh và trình tạo ra số ngẫu nhiên chính xác về mặt mật mã là những yếu tố nền tảng được liên kết với một chương trình vững chắc. Các yếu tố cây nhà lá vườn hoặc tùy chỉnh trong những lĩnh vực này có thể làm tăng đáng kể những rủi ro tương ứng với một hệ thống bị phá vỡ. Việc phát triển các thuật toán mật mã của riêng bạn nằm ngoài khả năng của hầu hết các nhóm. Các thuật toán rất phức tạp và rất khó để tạo ra. Bất kỳ thuật toán nào chưa được đánh giá công khai đều có thể sẽ có điểm yếu. Hầu hết các thuật toán tốt chỉ được phê duyệt để sử dụng sau một giai đoạn kiểm nghiệm kéo dài và xem xét công khai.

Khi tài liệu, được gọi là *văn bản rõ ràng* (*plaintext*), cần được bảo vệ khỏi sự can thiệp hoặc thay đổi trái phép, nó sẽ được mã hóa thành *văn bản mã hóa* (*ciphertext*). Điều này được thực hiện bằng cách sử dụng một thuật toán và một khóa, và sự phát triển của những máy tính kỹ thuật số đã cung cấp một loạt các thuật toán và các khóa ngày càng phức tạp hơn. Việc lựa chọn thuật toán cụ thể phụ thuộc vào một số yếu tố, sẽ được xem xét trong chương này.



**LƯU Ý** Chương này giới thiệu rất nhiều tên gọi, từ viết tắt và thông tin chi tiết, tất cả đều hoạt động cùng nhau để xác định các khái niệm cơ bản về mật mã. Bối cảnh của chương phù hợp với mục tiêu Security+, giúp việc tra cứu dễ dàng hơn, nhưng có nghĩa là một số thuật ngữ sẽ được mô tả sau trong chương. Bạn nên đọc nhanh qua chương để biết mọi thứ ở đâu và sau đó đọc lại một lần nữa để biết nội dung, biết chủ đề ở đâu nếu bạn cần tra cứu chúng.

### **Những Phương pháp Nền tảng**

Những hoạt động mã hóa hiện đại được thực hiện bằng cách sử dụng cả một thuật toán và một khóa. Việc lựa chọn thuật toán phụ thuộc vào kiểu hoạt động mã hóa đang được mong muốn. Việc lựa chọn khóa tiếp theo sau đó gắn liền với thuật toán cụ thể. Các hoạt động mã hóa bao gồm mã hóa để bảo vệ tính bảo mật, băm để bảo vệ tính toàn vẹn, các chữ ký kỹ thuật số để quản lý tính không khước từ, và và một loạt các hoạt động đặc biệt như trao đổi khóa.

Mặc dù các chi tiết toán học cụ thể của các hoạt động này có thể rất phức tạp và vượt quá phạm vi của cấp độ tài liệu này, nhưng kiến thức để sử dụng chúng một cách đúng đắn không phức tạp và là đối tượng phải được kiểm tra trong kỳ thi CompTIA Security+. Các hoạt động mã hóa được đặc trưng bởi số lượng và loại dữ liệu, cũng như mức độ và loại bảo vệ được tìm kiếm. Hoạt động bảo vệ tính toàn vẹn được đặc trưng bởi mức độ đảm bảo mong muốn. Dữ liệu được đặc trưng bởi cách sử dụng: dữ liệu đang truyền tải, dữ liệu ở trạng thái nghỉ hoặc dữ liệu đang được sử dụng. Nó cũng được đặc trưng ở cách nó có thể được sử dụng, ở dạng khối hoặc dạng luồng, như được mô tả tiếp theo.



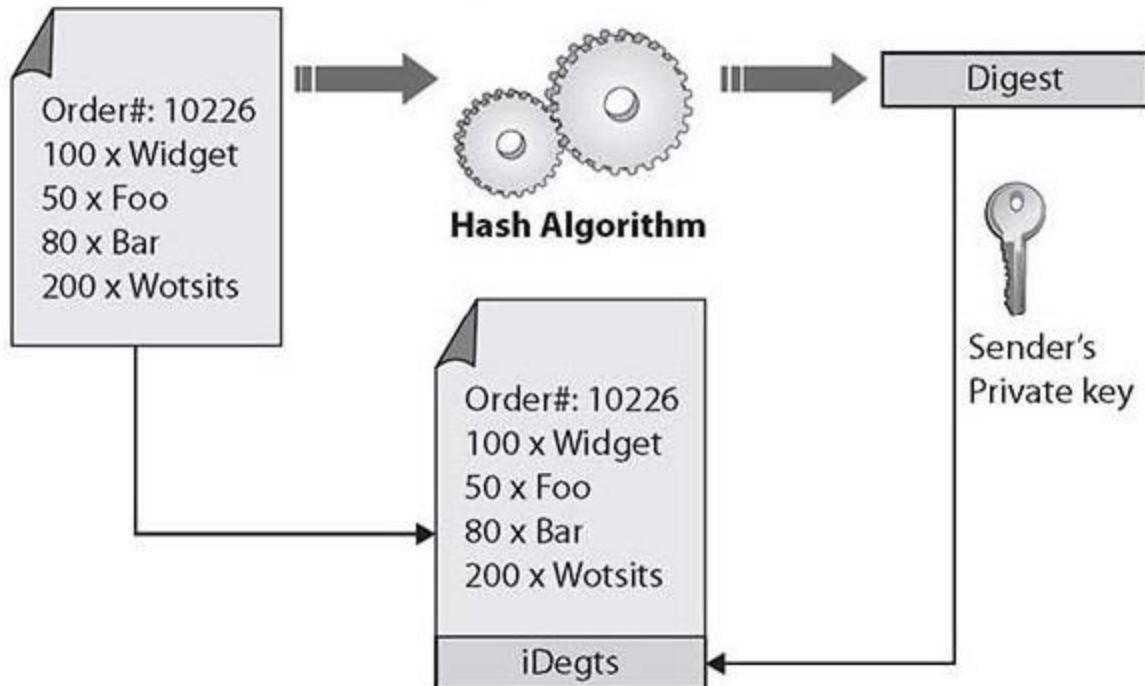
## MÁCH NƯỚC CHO KỲ THI

Các thuật ngữ *dữ liệu đang truyền tải, dữ liệu ở trạng thái nghỉ và dữ liệu đang sử dụng* là các thuật ngữ tiêu chuẩn của ngành. Trong các mục tiêu Security+, chẳng hạn như 2.1 trong "Bảo vệ dữ liệu", các thuật ngữ hơi khác được sử dụng. Security+ sử dụng các thuật ngữ [dữ liệu] *ở trạng thái nghỉ, đang truyền tải/chuyển động và đang xử lý*. Điều quan trọng là phải nhận ra và sử dụng các thuật ngữ dành-riêng-cho-kỳ thi trong kỳ thi.

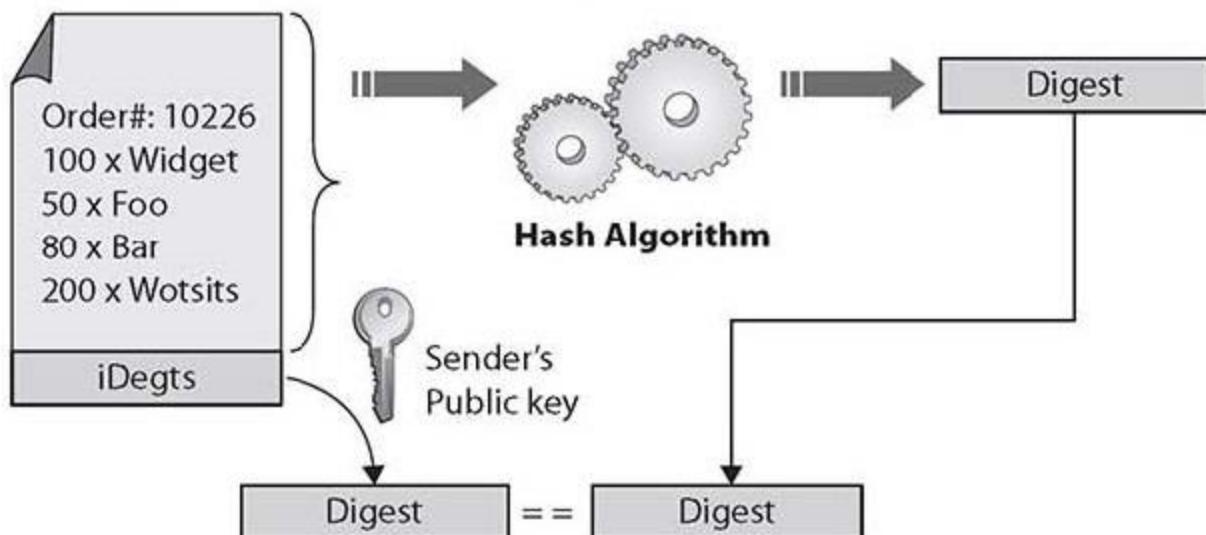
### Chữ ký Kỹ thuật số

*Chữ ký điện tử* là một triển khai mật mã được thiết kế để chứng minh tính xác thực và danh tính được liên kết với một thông điệp. Bằng cách sử dụng mật mã khóa công khai, một chữ ký điện tử cho phép truy xuất nguồn gốc của người đã ký thông điệp thông qua việc sử dụng khóa riêng tư của họ. Việc bổ sung mã băm cũng cho phép đảm bảo tính toàn vẹn của thông điệp. Hoạt động của chữ ký điện tử là sự kết hợp của các yếu tố mã hóa để đạt được một kết quả mong muốn. Các bước liên quan đến việc tạo ra và sử dụng chữ ký số được minh họa trong Hình 16-1. Thông điệp cần ký sẽ được băm và mã băm được mã hóa bằng khóa riêng của người gửi. Sau khi nhận, người nhận có thể giải mã băm bằng khóa công khai của người gửi. Nếu một lần băm tiếp theo của thông điệp tiết lộ một giá trị giống hệt nhau, hai điều được biết đến: Thứ nhất, thông điệp đã không bị thay đổi. Thứ hai, người gửi sở hữu khóa riêng của người gửi đã được xác định và do đó có lẽ là cùng một người.

### Digital Signature signing (send)



### Digital Signature verification (receive)



If the digests match, message authenticity and integrity are assured.

**Hình 16-1** Hoạt động của chữ ký số

Một chữ ký số bản thân nó không bảo vệ nội dung của thông điệp khỏi sự can thiệp. Thông điệp vẫn được gửi đi dưới hình thức rõ ràng, do đó, nếu tính bảo mật của thông điệp là một yêu cầu, các bước bổ sung phải được thực hiện để bảo vệ thông điệp khỏi bị nghe lén. Việc này có thể được thực hiện bằng cách mã hóa bản thân thông điệp, hoặc bằng cách mã hóa kênh mà thông điệp được truyền tải qua đó.



**MÁCH NƯỚC CHO KỲ THI** Hãy biết rằng một chữ ký số bảo đảm rằng nội dung của một thông điệp đã không bị thay đổi trong quá trình truyền tải.

### **Độ dài của Khóa**

Sức mạnh của chức năng mã hóa thường phụ thuộc vào sức mạnh của khóa, khi một khóa lớn hơn có mức độ mất trật tự (mức độ hỗn loạn) lớn hơn và bổ sung thêm nhiều sức mạnh hơn cho việc mã hóa. Vì các thuật toán khác nhau sử dụng các phương pháp khác nhau với một khóa, việc so sánh trực tiếp sức mạnh của khóa giữa các thuật toán khác nhau không thể được thực hiện một cách dễ dàng. Một số hệ thống mã hóa có độ dài khóa được cố định, chẳng hạn như Triple Digital Encryption Standard (3DES), trong khi những hệ thống khác, chẳng hạn như Advanced Encryption Standard (AES), có nhiều độ dài khóa khác nhau (ví dụ, AES-128, AES-192, và AES-256).

Một số thuật toán đưa ra các tùy chọn độ dài khóa: như một nguyên tắc chung, độ dài khóa dài hơn thì sẽ bảo mật hơn, nhưng cũng cần nhiều thời gian để tính toán hơn. Liên quan đến việc tìm kiếm sự cân bằng thích hợp giữa bảo mật và tính tiện dụng, dưới đây là một số khuyến cáo về độ dài khóa tối thiểu:

- Độ dài khóa đối xứng ít nhất từ 80 đến 112 bit.
  - Độ dài khóa đường cong eliptic ít nhất từ 160 đến 224 bit.
  - Độ dài hóa RSA ít nhất là 2048 bit. Đặc biệt, CA/Browser Forum Extended Validation (EV) Guidelines yêu cầu một độ dài khóa tối thiểu 2048 bit.
  - Độ dài khóa ĐƯỢC SỬ DỤNG ĐỂ ít nhất là 2048 bit.
- 



**LƯU Ý** Mật mã học là một ngành học chứa đầy các từ viết tắt, chúng được sử dụng cho các thuật toán, phương pháp và các quy trình. Điều này trông có vẻ đáng sợ, nhưng sau khi đã đọc qua chương này, chúng [các từ viết tắt] sẽ trở nên quen thuộc hơn với bạn.

### Kéo căng Khóa

*Kéo căng khóa* là một cơ chế lấy những gì sẽ là các khóa yếu và “kéo căng” chúng để làm cho hệ thống trở nên an toàn hơn trước các cuộc tấn công kiểu brute-force. Khi các máy tính đã có được đủ năng lực tính toán, các hàm băm có thể được tính toán một cách nhanh chóng, dẫn đến nhu cầu về cách thức tăng khối lượng công việc khi tính toán các hàm băm, nếu không, kẻ tấn công có thể chỉ đơn thuần là tính toán mọi thứ. Trong trường hợp sử dụng một khóa ngắn, cơ hội khớp ngẫu nhiên với hàm băm bằng cách sử dụng các cuộc tấn công đoán tính toán đã tăng lên. Để làm cho việc so khớp băm trở nên khó khăn hơn, người ta phải tăng không gian khóa hoặc làm chậm quá trình tính toán. Việc kéo căng khóa liên quan đến việc làm tăng độ phức tạp của tính toán bằng cách thêm các vòng tính toán lặp đi lặp lại - các vòng không thể thực hiện song song. Khi một người muốn sử dụng một cuộc tấn công kiểu brute-force, sự tăng khối lượng của công việc tính toán trở nên đáng kể khi được thực hiện hàng tỷ lần, làm cho hình thức tấn công này tốn kém hơn nhiều.

## "Trộn muối" (Salting)

Để cung cấp đủ mức độ hỗn loạn cho các đầu vào có mức độ hỗn loạn thấp cho các hàm băm, một phần dữ liệu có mức độ hỗn loạn cao có thể được liên kết với tài liệu được băm. Thuật ngữ *muối* đề cập đến phần dữ liệu ban đầu này. Muối đặc biệt hữu ích khi tài liệu được băm ngắn và ít hỗn loạn. Việc thêm muối mức độ hỗn loạn cao (ví dụ, 30- ký tự) vào mật khẩu ba-ký-tự sẽ làm tăng đáng kể mức độ hỗn loạn của hàm băm được lưu trữ.



### LƯU Ý

Mức độ hỗn loạn là một thuật ngữ quan trọng trong mật mã học, nó đề cập đến mức độ ngẫu nhiên. Mức độ hỗn loạn sẽ được đề cập chi tiết hơn trong phần sau của chương.

Một thuật ngữ khác được sử dụng trong văn đề này là *véc-tơ khởi tạo*, hoặc *IV* (*initialization vector*), và điều này được sử dụng trong một số mật mã, đặc biệt là trong không gian không dây, để đạt được tính ngẫu nhiên, ngay cả với các đầu vào xác định thông thường. Các IV có thể bổ sung thêm tính ngẫu nhiên và được sử dụng trong mật mã khôi để bắt đầu các chế độ hoạt động.



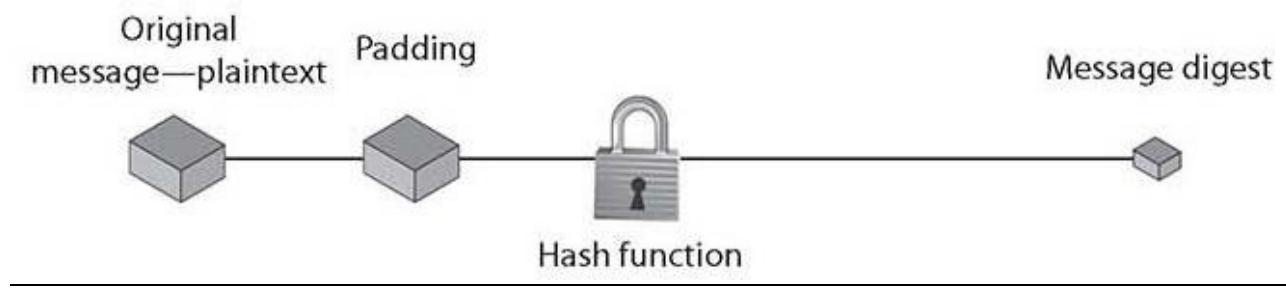
### LƯU Ý

Các vectơ khởi tạo sẽ được trình bày chi tiết hơn trong Chương 4, "Các Chỉ báo Tấn công Mạng". *Thời gian hiện tại* (*nonce*) là một số chỉ được sử dụng một lần và tương tự như một muối hoặc một IV. Tuy nhiên, vì nó chỉ được sử dụng một lần nên nếu cần dùng lại, một giá trị khác sẽ được sử dụng. Các nonce cung cấp mức độ hỗn loạn không xác định ngẫu nhiên cho các hàm mật mã và thường được sử dụng trong

mật mã dòng để phá vỡ các thuộc tính trạng thái khi khóa được tái sử dụng lại.

## Băm

Hàm băm là phương pháp mã hóa thường được sử dụng. *Hàm băm* là một hàm toán học đặc biệt thực hiện việc mã hóa một chiều, có nghĩa là khi thuật toán được xử lý, không có cách nào khả thi để sử dụng bản được mã hóa để lấy ra bản rõ (plaintext) đã được sử dụng để tạo ra nó. Ngoài ra, lý tưởng là không có cách nào khả thi để tạo ra hai bản rõ khác nhau tính theo cùng một giá trị băm. Hình 16-2 cho thấy một quy trình băm điển hình.



**Hình 16-2** Hàm băm hoạt động như thế nào

Những cách sử dụng phổ biến của thuật toán băm là để lưu trữ mật khẩu máy tính và đảm bảo tính toàn vẹn của thông điệp. Ý tưởng ở đây là băm có thể tạo ra một giá trị duy nhất tương ứng với dữ liệu đã nhập, nhưng giá trị băm cũng có thể được tái tạo bởi bất kỳ ai khác đang chạy cùng một thuật toán đối với dữ liệu. Vì vậy, bạn có thể băm một thông điệp để lấy *mã xác thực thông điệp* (*message authentication code - MAC*) và số tính toán của thông điệp sẽ cho thấy rằng không có người trung gian nào đã sửa đổi thông điệp. Quá trình này hoạt động vì các phương pháp băm thường là công khai và bất kỳ ai cũng có thể băm dữ liệu bằng phương pháp đã được chỉ định. Về mặt tính toán, việc tạo ra mã băm rất đơn

giản, do đó, việc kiểm tra tính hợp lệ hoặc tính toàn vẹn của một thứ gì đó bằng cách so khớp hàm băm đã cho với hàm băm được tạo [trên máy tính] cục bộ sẽ rất đơn giản. HMAC, hay *Mã Xác thực Thông điệp dựa-trên-Băm (Hash-based Message Authentication Code)*, là một tập hợp con đặc biệt của công nghệ băm. Đây là một thuật toán băm được áp dụng cho một thông điệp để tạo MAC, nhưng nó được thực hiện với một bí mật đã được chia sẻ trước đó. Vì vậy, HMAC có thể cung cấp tính toàn vẹn đồng thời với sự xác thực.

Một thuật toán băm có thể bị xâm phạm với cái được gọi là *tấn công xung đột*, trong đó kẻ tấn công tìm thấy hai thông điệp khác nhau có cùng giá trị băm. Kiểu tấn công này rất khó và đòi hỏi việc phải tạo ra một thuật toán riêng để cố gắng tìm được một văn bản sẽ băm thành cùng một giá trị của một hàm băm đã biết. Điều này phải diễn ra nhanh hơn so với việc chỉ chỉnh sửa các ký tự cho đến khi bạn băm về cùng một giá trị, đây là một kiểu tấn công brute-force. Hệ quả của một hàm băm bị xâm phạm là tính toàn vẹn sẽ bị mất. Nếu kẻ tấn công có thể cố ý tạo ra hai đầu vào khác nhau để băm thành cùng một giá trị, chúng có thể lừa mọi người chạy mã độc hại và gây ra các vấn đề khác. Các thuật toán băm phổ biến là loạt Thuật toán Băm An toàn (Secure Hash Algorithm - SHA), các thuật toán RIPEMD và Đóng hóa Thông điệp (Message Digest - MD) gồm các phiên bản khác nhau (MD2, MD4 và MD5).



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng một hàm băm là một hàm toán học đặc biệt để thực hiện mã hóa một-chiều.

Các hàm băm rất phổ biến, và chúng đóng một vai trò rất quan trọng trong cách thức mà thông tin, chẳng hạn như mật khẩu, được lưu trữ một cách an toàn và cách thức mà theo đó, thông điệp có thể được ký. Bằng

cách tính toán một mã đồng hóa (digest) của thông điệp, sẽ có ít dữ liệu hơn cần phải được ký bởi chức năng mã hóa không đồng bộ phức tạp hơn, và việc này vẫn duy trì được sự đảm bảo về tính toàn vẹn của thông điệp. Đây là mục đích chủ yếu mà theo đó các giao thức đã được thiết kế, và sự thành công của chúng sẽ cho phép sự tin tưởng nhiều hơn vào các giao thức điện tử và các chữ ký số.

### **Trao đổi Khóa**

Các cơ chế mật mã sử dụng cả một thuật toán lẫn một khóa, cùng với khóa yêu cầu giao tiếp giữa các bên. Trong mã hóa đối xứng, tính bí mật phụ thuộc vào tính bí mật của khóa, do đó việc truyền tải khóa không an toàn có thể dẫn đến thất bại trong việc bảo vệ thông tin đã được mã hóa bằng khóa. *Trao đổi khóa* là yếu tố nền tảng trung tâm của một hệ thống mã hóa đối xứng an toàn. Việc duy trì tính bí mật của khóa đối xứng là cơ sở của giao tiếp bí mật. Trong các hệ thống bất đối xứng, vẫn đề trao đổi khóa là một trong những vấn đề rất quan trọng. Bởi vì khóa công khai được thiết kế để chia sẻ nên vẫn đề được đảo ngược từ vấn đề về tính bí mật sang vấn đề về sự công khai.



**MÁCH NƯỚC CHO KỲ THI** Với mã hóa đối xứng, thông điệp cần được bảo vệ sẽ được mã hóa và giải mã bằng cách sử dụng cùng một khóa bí mật. Mã hóa bất đối xứng sử dụng hai khóa riêng biệt để mã hóa và giải mã thông điệp.

Các cuộc trao đổi khóa ban đầu đã được thực hiện bởi những người đưa thư đáng tin cậy. Mọi người mang chìa khóa từ người gửi đến người nhận. Người ta có thể coi hình thức trao đổi khóa này là phương thức tối ưu trong giao tiếp *ngoài-dải-tần (out-of-band)*. Với sự ra đời của các phương pháp kỹ thuật số và một số thuật toán toán học, người ta có thể truyền

khóa theo cách thức an toàn. Điều này có thể xảy ra ngay cả khi tất cả các gói đều bị đánh chặn. Trao đổi khóa Diffie-Hellman là một ví dụ về kiểu trao đổi khóa an toàn này. Việc trao đổi khóa Diffie-Hellman phụ thuộc vào hai số ngẫu nhiên, mỗi số do một trong các bên lựa chọn và được giữ bí mật. Trao đổi khóa Diffie-Hellman có thể được thực hiện *trong-dải-tần (in-band)* và thậm chí dưới sự quan sát từ bên ngoài, vì các số ngẫu nhiên bí mật không bao giờ bị lộ ra bên ngoài.

### **Mật mã Đường cong Elliptic**

*Mật mã đường cong elliptic (ECC)* hoạt động trên cơ sở đường cong hình elliptic. Một *đường cong elliptic* là một hàm đơn giản được vẽ dưới dạng một đường cong mảnh lặp lại trên mặt phẳng X, Y. Các đường cong elliptic được xác định bởi phương trình sau:

$$y^2 = x^3 + ax^2 + b$$

Các đường cong elliptic hoạt động vì chúng có một thuộc tính đặc biệt – bạn có thể bổ sung hai điểm trên đường cong cùng nhau và có được một điểm thứ ba trên đường cong.

Đối với mật mã học, đường cong elliptic hoạt động như một thuật toán khóa công khai. Người dùng thống nhất về một đường cong elliptic và một điểm đường cong cố định. Thông tin này không phải là bí mật được chia sẻ và những điểm này có thể được công khai mà không ảnh hưởng đến tính bảo mật của hệ thống. Vấn đề an toàn của hệ thống đường cong elliptic đã bị nghi ngờ, phần lớn là do thiếu sự phân tích. Tuy nhiên, tất cả các hệ thống khóa công khai đều dựa vào độ khó của một số bài toán nhất định. Sẽ cần một bước đột phá trong toán học để bắt kỳ hệ thống nào trong số các hệ thống đã được đề cập bị suy yếu một cách đáng kể, nhưng nghiên cứu đã được thực hiện về các vấn đề này và đã chỉ ra rằng bài toán đường cong elliptic có khả năng chống lại những tiến bộ ngày

càng gia tăng [có lẽ hàm ý của tác giả là đường cong elliptic có thể giải quyết những bài toán về mã hóa – người dịch]. Một lần nữa, như với tất cả các thuật toán mật mã khác, chỉ có thời gian mới cho biết việc triển khai ECC thực sự an toàn như thế nào.

Một lợi ích lớn lao của các hệ thống ECC là chúng đòi hỏi ít năng lực tính toán hơn cho một cường độ bit nhất định. Điều này khiến cho ECC trở nên lý tưởng để sử dụng trong các thiết bị di động có công-suất-thấp. Sự gia tăng kết nối di động đã mang đến các ứng dụng thoại, email và văn bản an toàn sử dụng thuật toán ECC và AES để bảo vệ dữ liệu của người dùng.



## MÁCH NƯỚC CHO KỲ THI

Mật mã đường cong elliptic có thể được sử dụng theo một số cách, bao gồm trong cả quá trình trao đổi khóa và một chữ ký điện tử. Security+ có 3 từ viết tắt mà bạn cần phải biết trong lĩnh vực này: ECC – mật mã đường cong elliptic (elliptic curve cryptography), ECDHE – Đường cong Elliptic Diffie-Helman Phù du (Elliptic Curve Diffie-Helman Ephemeral), và ECDSA – Thuật toán Chữ ký Số Đường cong Elliptic (Elliptic Curve Digital Signature Algorithm). Điều quan trọng là phải có được kiến thức thực tế về những thuật ngữ trong chú giải thuật ngữ Security+.

## Bí mật Chuyển tiếp Hoàn hảo

*Bí mật chuyển tiếp hoàn hảo (perfect forward secrecy – PFS)* là một thuộc tính của một hệ thống khóa công khai, theo đó, một khóa có nguồn gốc từ một khóa khác sẽ không bị xâm phạm, thậm chí ngay cả khi khóa khởi tạo bị xâm phạm trong tương lai. Điều này đặc biệt quan trọng trong quá trình tạo ra khóa phiên, nơi các phiên giao tiếp trong tương lai có thể bị

xâm phạm, nếu không có bí mật chuyển tiếp hoàn hảo thì những thông điệp trong quá khứ đã được ghi lại có thể bị giải mã.

### **Mật mã Lượng tử**

*Mật mã lượng tử* là việc sử dụng phần cứng máy tính lượng tử để thực hiện các quá trình mã hóa và giải mã. Phần cứng lượng tử vẫn đang trong giai đoạn phát triển ban đầu và sức mạnh tính toán to lớn trong những nền tảng này sẽ tạo ra một cuộc cách mạng về mật mã. Hầu hết các vấn đề liên quan đến mật mã lượng tử vẫn chỉ đang nằm trong lý thuyết, vì các máy tính [lượng tử] có đủ sức mạnh và khả năng lập trình vẫn chưa được xây dựng. Nhưng, giống như tất cả các cuộc đua công nghệ, khi khả năng tấn công mã hóa bằng máy lượng tử xuất hiện, các phương pháp mã hóa mới sử dụng cùng loại phần cứng sẽ khôi phục sự cân bằng giữa độ mạnh mã hóa và khả năng bẻ khóa nó.

Các nguyên tắc lượng tử đã thực sự được triển khai vào các trao đổi khóa liên-quan-đến-giao-tiếp thông qua phân phối khóa lượng tử (quantum key distribution - QKD). QKD không thực sự mã hóa giao tiếp mà thay vào đó, cung cấp một phương tiện để người dùng phân phối một cách an toàn các khóa được sử dụng để mã hóa kênh giao tiếp.



**LƯU Ý** Điện toán lượng tử sẽ làm thay đổi cả tính toán lẫn giao tiếp. Trong tính toán, các phương pháp lượng tử hứa hẹn các giải pháp cho những vấn đề vẫn chưa thể được giải quyết trong hiện hành. Trong truyền thông, các phương pháp lượng tử cung cấp các phương tiện bảo mật mới, bao gồm phân phối khóa, vốn đã sẵn sàng thông qua phân phối khóa lượng tử.

Điện toán lượng tử là một trong những biên giới của máy tính và liên quan đến việc tạo ra một loại máy tính hoàn toàn mới. Các máy tính lượng tử sử dụng một cấu trúc mới được gọi là *qubit*, cho phép thông tin được biểu diễn theo cách khác chứ không chỉ là "bật" hoặc "tắt" như các bit nhị phân. Nói cách khác, qubit cho phép nhiều đường dẫn của một vấn đề được tính toán một cách đồng thời. Điện toán lượng tử không chỉ là phần cứng, nó liên quan đến các dạng thức phần mềm mới và cũng đã có những phát triển đáng kể trong lĩnh vực này. Gần đây, các nhà khoa học đã tuyên bố vượt qua sức mạnh tính toán thông thường với một cỗ máy lượng tử, nhưng trước khi khiến bạn phấn khích, đây không phải là một cỗ máy đa năng, mà là một cỗ máy chỉ chuyên giải quyết một vấn đề cụ thể duy nhất. Bất chấp tất cả những hạn chế hiện tại, điện toán lượng tử sẽ mang lại những đột phá đáng kể trong lĩnh vực điện toán trong tương lai.

### Kỷ nguyên Hậu-Lượng tử

Khi điện toán lượng tử đang đặt ra một thách thức đối với rất nhiều thuật toán mật mã ngày nay, làm sụt giảm đáng kể sức mạnh của chúng, và vậy, có một phong trào phát triển các thuật toán không dễ giải quyết bằng phương pháp lượng tử. Đây không phải là một bài tập lý thuyết, vì các cơ quan chính phủ và các cơ quan khác đang nghiên cứu các giải pháp thực tế để tìm ra đáp án và các thuật toán thay thế nếu bất kỳ thuật toán hiện tại nào bị lỗi, cho dù bằng máy tính lượng tử hay các vấn đề khác.

Hiện tại có một số thuật toán mật mã đã được phát triển để ứng phó với các phương pháp lượng tử và được cho là có khả năng chống lại các phương pháp giải mã dựa-trên-tính-toán-lượng tử ở một mức độ hợp lý. Những phương pháp này sử dụng các tính chất toán học khác nhau, khiến cho các bộ giải pháp đồng thời không đạt hiệu quả cao, do đó hạn chế

được sức mạnh của tính toán lượng tử trong việc giải loại bài toán này. Như với tất cả các hệ thống, luôn có sự đánh đổi và trong trường hợp này, các phương pháp mới hơn có xu hướng sử dụng các khóa dài hơn và đòi hỏi nhiều sức mạnh tính toán hơn để sử dụng.

### **Khóa Phù du (Ephemeral)**

Khóa tạm thời là khóa mật mã chỉ được sử dụng một lần sau khi được tạo ra. Khi một khóa tạm thời được sử dụng như một phần của lược đồ Diffie-Hellman, nó tạo thành một trao đổi khóa Ephemeral Diffie-Hellman (EDH). EDH tạo một khóa tạm thời cho mỗi kết nối, không bao giờ sử dụng cùng một khóa hai lần. Điều này dành cho bí mật chuyển tiếp hoàn hảo. Nếu điều này được xây dựng bằng thuật toán đường cong elliptic, nó sẽ là ECDHE, viết tắt của Elliptic Curve Diffie-Helman Ephemeral, như đã được đề cập trước đây.



### **MÁCH NƯỚC CHO KỲ THI**

Các khóa phù du là các khóa mật mã được sử dụng chỉ sau khi đã tạo ra.

### **Chế độ Vận hành**

Trong các thuật toán đổi xứng hoặc thuật toán khối, cần phải xử lý nhiều khối dữ liệu giống hệt nhau để ngăn chặn nhiều khối văn bản mạng có thể xác định các khối dữ liệu đầu vào giống hệt nhau. Có nhiều phương pháp để giải quyết vấn đề này, được gọi là các *chế độ vận hành*. Tiềm đề cơ bản là sử dụng một số nguồn mức độ hỗn loạn trước khi mã hóa các khối tiếp theo để các khối văn bản rõ ràng giống hệt nhau tạo ra các khối văn bản mã hóa khác nhau. Các chế độ này có thể được chia thành ba nhóm: đã xác thực, chưa xác thực và bộ đếm.

## Đã được xác thực

Mã hóa xác thực với dữ liệu tương ứng (*authenticated encryption with associated data - AEAD*) là một hình thức mã hóa được thiết kế để cung cấp cả các dịch vụ bảo mật và xác thực. Một loạt các chế độ đã được xác thực đang sẵn có cho các nhà phát triển, bao gồm GCM, OCB và EAX.



### LƯU Ý

Tại sao bạn lại cần đến mã hóa đã được xác thực? Để bảo vệ trước các cuộc tấn công văn bản mã hóa đã chọn như POODLE, bạn cần một lớp thứ hai sử dụng triển khai MAC như HMAC-SHA. Điều này được thực hiện bằng các bước sau:

- Tính toán MAC trên bản mã hóa, không phải trên bản rõ ràng.
- Sử dụng các khóa khác nhau: một để mã hóa và một khóa khác cho MAC.

Phương thức cụ thể nhưng chung chung này bổ sung thêm các bước và rắc rối cho các nhà phát triển. Để giải quyết vấn đề này, các chế độ đặc biệt cho các mật mã khối được gọi là mã hóa đã được xác thực (*authenticated encryption - AE*) và mã hóa đã được xác thực với dữ liệu tương ứng (*authenticated encryption with associated data - AEAD*) đã được phát minh ra. Chúng cung cấp sự bảo vệ tương tự như kết hợp mật mã khối/MAC, nhưng trong một chức năng duy nhất với một phím duy nhất. Các chế độ AE (AD) đã được phát triển để giúp triển khai các giải pháp dễ dàng hơn, nhưng việc áp dụng còn tương đối chậm chạp.

OCB là *Offset Codebook Mode*, một phương pháp triển khai đã được cấp bằng sáng chế mang lại hiệu suất cao nhất, nhưng do có bằng sáng chế nên nó không được đưa vào bất kỳ tiêu chuẩn quốc tế nào. EAX giải quyết vấn đề bằng sáng chế, nhưng tương tự như vậy vẫn chưa được bất kỳ

tiêu chuẩn quốc tế nào áp dụng. Việc này được để lại cho GCM (Galois Counter Mode), được mô tả trong phần tiếp theo.

## Bộ đếm

*Chế độ bộ đếm (counter mode - CTM)* sử dụng một hàm “bộ đếm” để tạo ra một nonce được sử dụng cho mỗi mã hóa khối. Các khối khác nhau có các nonce khác nhau, cho phép xử lý song song và cải thiện tốc độ đáng kể. Trình tự hoạt động là lấy giá trị của hàm đếm (nonce), mã hóa nó bằng khóa, sau đó XOR nó bằng bản rõ ràng. Mỗi khối có thể được thực hiện một cách độc lập, dẫn đến khả năng xử lý đa luồng. Hãy lưu ý rằng CTM cũng được viết tắt là CTR trong một số vòng kết nối.

CCM là một chế độ hoạt động liên quan đến CBC (cipher block chaining - chuỗi khối mật mã, được mô tả trong phần tiếp theo) với MAC, hoặc CBC-MAC. Phương pháp này được thiết kế dành cho mật mã khối có độ dài 128 bit, trong đó độ dài của thông điệp và bất kỳ dữ liệu tương ứng nào phải được biết trước. Điều này có nghĩa là nó không phải là một dạng AEAD “trực tuyến”, vốn có đặc trưng là cho phép bất kỳ độ dài đầu vào nào.

Chế độ bộ đếm Galois (GCM) là một phần mở rộng của CTM trong đó có bổ sung thêm chế độ xác thực Galois. Điều này bổ sung thêm một chức năng xác thực cho chế độ mật mã và trường Galois được sử dụng trong quá trình này có thể được song song hóa, cung cấp các hoạt động hiệu quả. GCM được sử dụng trong rất nhiều tiêu chuẩn quốc tế, bao gồm IEEE 802.1ad và 802.1AE. NIST đã công nhận AES-GCM cũng như GCM và GMAC. Bộ mật mã AES GCM cho TLS được mô tả trong IETF RFC 5288.

## Chưa được xác thực

Chế độ chưa được xác thực sử dụng nguồn không-dựa-trên-danh-tính cho phần tử entropy cho các khối tiếp theo. Trong chuỗi khối mật mã (CBC), mỗi khối được XOR với khối bản mã hóa trước đó trước khi được mã hóa.

Để làm xáo trộn khối đầu tiên, một véc-tơ khởi tạo (IV) được XOR với  
CompTIA Security+ - All in One – Exam Guide

khôi đầu tiên trước khi được mã hóa. CBC là một trong những chế độ phổ biến nhất được sử dụng, nhưng nó có hai điểm yếu lớn. Thứ nhất, bởi vì có sự phụ thuộc vào các khối trước đó, thuật toán không thể được song song hóa về tốc độ và hiệu quả. Thứ hai, do bản chất của chuỗi, một khối văn bản rõ ràng có thể được khôi phục từ hai khối bản mã hóa liền kề. Một ví dụ về điều này là trong cuộc tấn công POODLE (Padding Oracle On Downgraded Legacy Encryption) trên TLS. Kiểu tấn công đệm này hoạt động vì sự thay đổi một-bit đối với bản mã hóa gây ra hư hỏng hoàn toàn khối văn bản rõ ràng tương ứng và đảo ngược bit tương ứng trong khối bản rõ ràng sau đó, nhưng phần còn lại của các khối vẫn nguyên vẹn.

## Blockchain

*Blockchains* là các danh sách các bản ghi, trong đó mỗi quá trình bổ sung vào danh sách được thực hiện bởi một thuật toán mật mã. Mặc dù điều này trông có vẻ phức tạp nhưng nó phục vụ cho một mục đích quan trọng: các bản ghi trong chuỗi khối có khả năng chống lại sự sửa đổi. Điều này cho phép một sổ cái phân tán có thể ghi lại các giao dịch và có cả xác minh các bổ sung và sự bảo vệ liên quan đến tính toàn vẹn. Sức mạnh của tính toàn vẹn đến từ cả việc ký hồ sơ và bản chất bị phân tán của blockchain. Mặc dù một bản ghi có thể được thay đổi, nó sẽ yêu cầu tất cả các bản ghi sau nó cũng phải được thay đổi và do đó sẽ có thể phát hiện được trên các bản sao trên hệ thống lưu trữ phân tán của chuỗi. Vì vậy, mặc dù bản ghi có thể thay đổi về mặt kỹ thuật, nhưng trên thực tế, hệ thống được bảo mật một cách rõ ràng.

Khái niệm blockchain được phát minh để tạo ra sổ cái giao dịch công khai của tiền điện tử. *Tiền điện tử* là một hệ thống tiền tệ được xây dựng trên một tập hợp hữu hạn các số “hiếm – rare” được khai thác và sau đó được “tạo ra - created”. Vì không có cơ quan trung ương, các số khi được khai thác sẽ được nhập vào sổ cái phân tán, đánh dấu việc tạo ra chúng. Mọi

giao dịch cũng được nhập vào sổ cái, ngăn chặn việc tiêu-tốn-gấp-đôi các mã thông báo. Việc sử dụng sổ cái công khai được phân tán mang lại các biện pháp bảo vệ mà mã thông báo vật lý cung cấp - chỉ một người có thể kiểm soát mã thông báo (token) tiền tệ nhất định tại bất kỳ thời điểm nào và tất cả các giao dịch là bất biến.

---



**LƯU Ý** Mặc dù các loại tiền điện tử như Bitcoin đã nhận được tiêu đề [*hàm ý được công bố rộng rãi trên trang đầu của báo chí và phương tiện truyền thông – người dịch*], người chiến thắng thực sự trong công nghệ blockchain là việc triển khai các sổ cái công khai phân tán. *Sổ cái công khai* đã được sử dụng để giải quyết nhiều vấn đề thách thức trong việc theo dõi các giao dịch tài chính, chuỗi cung ứng và các vấn đề khác dựa trên sổ cái. Ứng dụng cho các hạng mục như tiền bản quyền âm nhạc, hệ thống DNS và theo dõi thực phẩm từ trang trại đến bàn ăn là tất cả các ví dụ về các giải pháp công nghệ blockchain đang được phát triển.

---



**MÁCH NƯỚC CHO KỲ THI** Blockchain là công nghệ lưu giữ hồ sơ đứng sau Bitcoin. Nó là một hồ sơ phân tán và phi tập trung.

### Bộ Mật mã

Thuật ngữ *bộ mật mã* đề cập đến một tập hợp các thuật toán được sử dụng cùng nhau trong mật mã, nổi tiếng nhất là bộ mật mã TLS (xem <https://www.iana.org/assignments/tls-parameters/tls-parameter.xhtml>).

Các kết hợp này được xác định trước để tạo điều kiện dễ dàng áp dụng thông qua kết nối TLS, thay vì phải xác định và đồng ý về từng tham số, một số duy nhất có thể đại diện cho một bộ mật mã hoàn chỉnh. Bộ mật

mã sẽ liệt kê cơ chế trao đổi khóa, giao thức xác thực, mật mã khối/luồng và xác thực thông điệp.

## **Khối**

Mật mã khối hoạt động dựa trên dữ liệu đầu vào trong một chuỗi các khối. Trong bộ mật mã TLS, trong TLS 1.2, một vài mật mã khối có sẵn, bao gồm AES, 3DES và IDEA. Với sự ra đời của TLS 1.3, danh sách này đã được cắt giảm đáng kể để chỉ còn những mật mã có thể hỗ trợ hoạt động AEAD. Điều này loại bỏ các phiên bản CBC của AES. Việc triển khai các lược đồ AEAD đã đóng lại một loạt các lỗ hổng tiềm ẩn đã từng bị tấn công trong quá khứ.

## **Luồng**

Mật mã luồng hoạt động trên các luồng dữ liệu thay vì các khối. Các hoạt động luồng thường diễn ra trên một byte duy nhất tại một thời điểm, sử dụng hàm XOR và khóa giả ngẫu nhiên (pseudorandom). Thách thức là tạo ra một chuỗi byte giả ngẫu nhiên đủ dài có thể được sử dụng để mã hóa và giải mã luồng. Các thuật toán luồng cụ thể, chẳng hạn như A5 và RC4, đã được sử dụng trong nhiều năm, nhưng những điểm yếu đã dẫn đến các thuật toán mới hơn như ChaCha20 và việc sử dụng AES-GCM trong một chế độ luồng chính.



**MÁCH NƯỚC CHO KỲ THI** Một mật mã khối mã hóa văn bản rõ ràng theo từng khối một. Một mật mã luồng mã hóa từng byte.

## **Đối xứng so với Bất đối xứng**

Cả hai phương pháp mã hóa đối xứng và bất đối xứng đều có những ưu điểm và nhược điểm riêng. Mã hóa đối xứng có xu hướng nhanh hơn, ít liên quan đến tính toán hơn và tốt hơn cho việc truyền tải hàng loạt. Tuy

nhiên, nó gặp phải một vấn đề về quản lý khóa là các khóa phải được bảo vệ khỏi các bên trái phép. Các phương pháp bất đối xứng giải quyết vấn đề bí mật của khóa bằng khóa công khai, nhưng chúng làm tăng thêm đáng kể mức độ phức tạp trong tính toán, khiến chúng ít phù hợp hơn với mã hóa hàng loạt.

Mã hóa hàng loạt có thể được thực hiện bằng cách sử dụng những gì là tốt nhất của cả hai hệ thống, bằng cách sử dụng mã hóa bất đối xứng để chuyển khóa đối xứng. Bằng cách bổ sung thêm vào trao đổi khóa tạm thời, bạn có thể đạt được bí mật chuyển tiếp hoàn hảo, đã được thảo luận trước đó trong chương. Chữ ký điện tử, một công cụ có tính hữu ích cao sẽ không thực tế nếu không có các phương pháp bất đối xứng. Bảng 16-1 so sánh các phương pháp đối xứng và bất đối xứng.

<b>Biện pháp</b>	<b>Mã hóa Đối xứng</b>	<b>Mã hóa Bất đối xứng</b>
Sử dụng chủ yếu	Mã hóa hàng loạt với số lượng lớn	Trao đổi các khóa đối xứng
Số lượng khóa được sử dụng	1, cùng một khóa để mã hóa và giải mã	2, một khóa có thể mã hóa, và khóa còn lại để giải mã
Các thuật toán phổ biến	AES, 3DES, RCA, IDEA	DSA, RSA, El Gamal, ECC, Diffie-Helman
Ưu điểm	Nhanh. Có thể được sử dụng cho một lượng lớn dữ liệu	Có thể được sử dụng mà không cần chia sẻ bí mật chung. Được sử dụng để trao đổi các khóa cho mã hóa đối xứng
Nhược điểm	Khóa chung cần phải được chia sẻ, và nếu bị mất khóa, sự bảo vệ cũng mất theo	Chậm hơn, không thích hợp cho lượng lớn dữ liệu

**Bảng 16-1** So sánh Mã hóa Đối xứng và Mã hóa Bất đối xứng



**MÁCH NƯỚC CHO KỲ THI** Hãy hiểu sự khác biệt giữa mã hóa đổi xứng và mã hóa bất đối xứng. [Mã hóa] Đổi xứng sử dụng một khóa, và nó nhanh hơn nhưng ít bảo mật hơn. [Mã hóa] Bất đối xứng sử dụng hai khóa, chậm hơn nhưng an toàn hơn.

Mã hóa đổi xứng và bất đối xứng thường được sử dụng cùng với nhau. Ví dụ, khi bạn truy cập một trang web được bảo vệ bằng TLS (HTTPS), bạn cần trao đổi khóa đổi xứng với máy chủ web để bảo vệ kênh giao tiếp. Điều này được thực hiện thông qua các phương pháp mã hóa bất đối xứng, vì chúng có thể tạo ra một trao đổi khóa an toàn giữa các bên mà không cần một bí mật chung được xác định trước. Việc này được sử dụng để trao đổi khóa đổi xứng sau đó được sử dụng để mã hóa và giải mã dữ liệu, bảo vệ được kênh giao tiếp. Một cách sử dụng chung phổ biến khác của các phần tử mật mã là trong chữ ký điện tử. Các phần tử mã hóa bất đối xứng cung cấp dịch vụ xác thực (nghĩa là bằng chứng về việc người gửi là ai và không khước từ). Chìa khóa, kích thước nhỏ, được xử lý bằng phương pháp bất đối xứng. Thông điệp, có kích thước lớn, được xử lý bằng khóa đổi xứng và phương pháp đổi xứng, phù hợp với mã hóa hàng loạt. Việc hiểu được sự khác biệt và cách sử dụng của từng loại, bao gồm cả hàm băm, là điều quan trọng đối với cả kỳ thi và thực tiễn bảo mật.

### **Mật mã Hạng nhẹ**

Trong một thế giới mà các thiết bị máy tính đạt được sức mạnh với mỗi vòng lặp lại của CPU, thật khó để tưởng tượng nhu cầu về mật mã ít-đòi-hỏi-máy-tính hơn. Bước vào thế giới của Internet of Things (IoT), nơi có rất nhiều thiết bị nhỏ, di động, bị hạn-chẽ-năng-lượng và tài-nghiên-máy-tính. Những thiết bị này nhỏ, giá rẻ và số lượng lên tới hàng trăm triệu đến hàng tỷ. Chúng có nhu cầu giao tiếp an toàn và quản lý các

chức năng như xác thực. *Mật mã hạng nhẹ* là một bộ thuật toán mật mã chuyên biệt được thiết kế để hoạt động trong môi trường hạn chế về tài nguyên này.

Toàn bộ bộ thuật toán hạng nhẹ được thiết kế cho bộ xử lý 8-bit đã được phát triển, bao gồm các hàm băm, mật mã khối và luồng, và thậm chí cả các hàm bất đối xứng và các hàm ký. NIST đã thúc đẩy các nghiên cứu quan trọng trong những năm gần đây và một loạt tiêu chuẩn ISO/IEC, ISO/IEC 29192, đề cập đến các phương pháp và chi tiết.

### **Steganography**

*Steganography*, một nhánh của công nghệ mật mã, lấy nghĩa của nó từ từ *steganos* trong tiếng Hy Lạp, có nghĩa là bị che phủ. Mục vô hình được quét trên tài liệu và bị ẩn đi bởi văn bản vô hại là một ví dụ về thông điệp được che phủ. Một ví dụ khác là hình xăm được đặt trên đỉnh đầu của một người, chỉ hiển thị khi tóc của người đó được cạo sạch.

Ẩn đi những gì được viết trong thời đại máy tính dựa vào một chương trình để ẩn dữ liệu bên trong dữ liệu khác. Ứng dụng phổ biến nhất là ẩn tin nhắn văn bản trong một tập tin ảnh. Internet chứa hàng tỷ tập tin hình ảnh, cho phép một thông điệp ẩn được đặt ở hầu hết mọi nơi mà không bị phát hiện. Bản chất của các tập tin hình ảnh cũng làm cho một thông điệp được ẩn giấu trở nên khó bị phát hiện. Mặc dù ẩn thông điệp bên trong hình ảnh là phổ biến nhất nhưng chúng cũng có thể được ẩn trong các tập tin video và âm thanh.

Ưu điểm của kỹ thuật ẩn so với mật mã là các thông điệp không thu hút sự chú ý và điều khó khăn trong việc phát hiện ra thông điệp ẩn này tạo ra một rào cản bổ sung cho việc phân tích. Dữ liệu ẩn trong thông điệp ẩn thường cũng được mã hóa, vì vậy nếu bị phát hiện, thông điệp sẽ vẫn an toàn. Steganography có nhiều mục đích sử dụng, nhưng cách sử dụng

được công khai nhiều nhất là để che giấu tài liệu bất hợp pháp, thường là nội dung khiêu dâm, hoặc được cho là để truyền thông bí mật bởi các mạng lưới khủng bố. Mặc dù không có bằng chứng trực tiếp nào chứng minh rằng những kẻ khủng bố sử dụng kỹ thuật ẩn giấu, nhưng các kỹ thuật này đã được ghi lại trong một số tài liệu đào tạo của chúng.

Mã hóa Steganographic có thể được sử dụng theo nhiều cách và thông qua nhiều phương tiện khác nhau. Việc đề cập đến tất cả chúng vượt quá phạm vi của quyển sách này, nhưng chúng ta sẽ thảo luận về một trong những cách phổ biến nhất để mã hóa thành tập tin hình ảnh: *mã hóa LSB*. LSB, viết tắt của bit ít quan trọng nhất (less significant bit), là một phương pháp mã hóa thông tin thành một hình ảnh trong khi làm thay đổi hình ảnh trực quan thực tế càng ít càng tốt. Một hình ảnh máy tính được tạo thành từ hàng nghìn hoặc hàng triệu pixel, tất cả được xác định bởi các số 1 và 0. Nếu một hình ảnh bao gồm các giá trị RGB (Đỏ Xanh Lá Xanh lục), mỗi pixel có một giá trị RGB được biểu thị bằng số từ 0 đến 255. Ví dụ: 0, 0, 0 là màu đen và 255,255,255 là màu trắng, cũng có thể được biểu thị bằng 00000000, 00000000, 00000000 cho màu đen và 11111111, 11111111, 11111111 cho màu trắng. Với một pixel màu trắng, việc chỉnh sửa bit ít quan trọng nhất của pixel thành 11111110, 11111110, 11111110 sẽ làm thay đổi màu sắc. Mắt người không thể phát hiện được sự thay đổi màu sắc, nhưng trong một hình ảnh có một triệu pixel, điều này tạo ra một vùng 125KB để lưu trữ một thông điệp.

Nội dung đã được ẩn có thể được nhúng vào hầu như bất kỳ luồng dữ liệu đã được mã hóa nào, nơi mã hóa được sử dụng để thể hiện phiên bản kỹ thuật số của một hình ảnh, luồng âm thanh hoặc luồng video. Việc mã hóa thông tin ẩn trong các khía cạnh của tín hiệu thực theo cách thức làm thay đổi đáng kể độ trung thực của tín hiệu gốc là những gì đem đến các kênh bí mật. Để bảo vệ dữ liệu tốt hơn khỏi quá trình phân tích, một

mã mã hóa được thực hiện trên dữ liệu bí mật, khiến cho dữ liệu bí mật được nhúng trông giống như nhiễu, điều này càng bảo vệ kenh tránh khỏi bị phát hiện đơn giản.

### **Mã hóa Đồng hình**

Một trong những mục đích chính của mật mã là ngăn chặn sự truy cập trái phép vào dữ liệu. Điều này rất quan trọng đối với dữ liệu ở trạng thái nghỉ và dữ liệu đang truyền tải, nhưng có thể là một vấn đề đối với dữ liệu đang được sử dụng. Dữ liệu được mã hóa trong khi lưu trữ hoặc di chuyển được bảo vệ khỏi sự quan sát hoặc thay đổi của các bên trái phép. Tuy nhiên, điều này cũng buộc các bên đã được cấp phép phải thực hiện các bước giải mã trước khi thực hiện việc tính toán, tiếp theo là các bước mã-hóa-lại bổ sung sau khi tính toán, điều này thể hiện một hình phạt đáng kể cho việc sử dụng. Hãy bước vào thế giới mã hóa đồng hình. *Mã hóa đồng hình* là một tập hợp các thuật toán cho phép các hoạt động được tiến hành trên dữ liệu đã được mã hóa mà không cần giải mã và mã-hóa-lại. Khái niệm rất đơn giản: tạo ra một hệ thống cho phép các hoạt động trên bản mã hóa mà nếu được giải mã, sẽ có kết quả giống như khi hoạt động được thực hiện trên bản rõ ràng.

Hầu hết các hoạt động liên quan đến dữ liệu được mã-hóa-đồng-hình đều liên quan đến công việc trên các con số - cụ thể là các số nguyên dưới dạng phép cộng. Mặc dù điều này trông có vẻ giống như là một hạn chế nhưng đó là một tiến bộ rất lớn, vì phần lớn dữ liệu được "thay đổi" trong hệ thống thực tế là số hoặc giá trị trong cơ sở dữ liệu. Hơn thế nữa, nếu số có thể được thêm vào, thì cùng với nhiều vòng cộng, có thể đạt được phép nhân và bằng cách sử dụng số âm, có thể đạt được phép trừ. Điều này khiến cho việc sử dụng các phương pháp đồng hình trở nên có giá trị đối với nhiều hệ thống dựa-trên-giao-dịch.

## Những trường hợp Sử dụng Phổ biến

Các dịch vụ mật mã đang được sử dụng trong ngày càng nhiều hệ thống và rất nhiều trường hợp sử dụng phổ biến được liên kết với chúng. Các ví dụ bao gồm việc triển khai để hỗ trợ cho các tình huống như năng lượng thấp, độ trễ thấp và khả năng phục hồi cao, cũng như hỗ trợ các chức năng như bảo mật, toàn vẹn và không khước từ.

### Thiết bị Năng-lượng-Thấp

Các thiết bị năng-lượng-thấp, chẳng hạn như điện thoại di động và thiết bị điện tử cầm tay, rất phổ biến và những thiết bị này đều có những nhu cầu về các chức năng mật mã. Các chức năng mật mã có xu hướng sử dụng sức mạnh tính toán đáng kể và các chức năng mật mã đặc biệt, chẳng hạn như mật mã đường cong elliptic, rất thích hợp cho các ứng dụng công suất thấp.

### Hoạt động Độ trễ Thấp

Một số trường hợp sử dụng liên quan đến các hoạt động có độ-trễ-thấp, và điều này khiến cho các chức năng mật mã chuyên biệt trở nên cần thiết để hỗ trợ cho các hoạt động có những ràng buộc quá mức về thời gian. Mã hóa luồng là những ví dụ về hoạt động độ-trễ-thấp.

### Các Hệ thống có Khả-năng-phục-hồi-Cao

Các hệ thống có khả-năng-phục-hồi-cao có đặc trưng bởi các chức năng có khả năng khôi phục lại những điều kiện hoạt động bình thường sau một sự gián đoạn từ bên ngoài. Việc sử dụng các mô-đun mật mã có thể hỗ trợ khả năng phục hồi thông qua một triển khai được tiêu chuẩn hóa tính linh hoạt của mật mã.

### Hỗ trợ Tính bảo mật

Việc bảo vệ dữ liệu khỏi việc đọc trái phép là định nghĩa về tính bảo mật. Mật mã là phương tiện chủ yếu để bảo vệ tính bảo mật của dữ liệu – đang được lưu trữ, đang truyền tải, và đang sử dụng.

## Hỗ trợ Tính Toàn vẹn

Thời gian phát sinh khi tính toàn vẹn của dữ liệu là điều cần thiết (ví dụ: trong quá trình truyền tải). Tính toàn vẹn có thể chứng minh rằng dữ liệu đã không bị thay đổi. Mã xác thực thông điệp (MAC) được hỗ trợ bởi các hàm băm là một ví dụ về các dịch vụ mật mã hỗ trợ cho tính toàn vẹn.

## Hỗ trợ sự Xáo trộn

Đôi khi thông tin cần được làm xáo trộn - nghĩa là được bảo vệ khỏi sự quan sát liên quan đến nguyên nhân và kết quả. Trong trường hợp của một chương trình, sự xáo trộn có thể bảo vệ mã khỏi sự quan sát của các bên trái phép.

## Hỗ trợ Xác thực

Xác thực là một thuộc tính có liên quan đến danh tính của một bên - có thể là một người dùng, một chương trình hoặc một phần cứng. Các chức năng mật mã có thể được sử dụng để chứng minh sự xác thực, chẳng hạn như xác nhận rằng một thực thể có khóa cá nhân cụ thể được liên kết với khóa công khai đã được trình bày, do đó chứng minh được danh tính.

## Hỗ trợ Không khước từ

*Không khước từ* là một thuộc tính liên quan đến khả năng xác minh rằng một thông điệp đã được gửi và nhận để từ đó người gửi (hoặc người nhận) không thể từ chối việc gửi (hoặc nhận) thông tin. Ví dụ về điều này trong thực tế được thấy với mối quan hệ chủ sở hữu cá nhân. Giả định rằng khóa riêng không tư bao giờ rời khỏi quyền sở hữu của người nắm giữ khóa riêng tư. Nếu việc này xảy ra, chủ sở hữu có trách nhiệm thu hồi chìa khóa. Do đó, nếu khóa riêng tư được sử dụng, bằng chứng là khóa công khai thành công, thì người ta giả định rằng thông báo đã được gửi bởi người giữ khóa riêng tư. Vì vậy, các hành động đã được ký kết không thể bị từ chối bởi người giữ khóa.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng không khước từ là khả năng xác minh rằng một thông điệp đã được gửi và nhận để từ đó người gửi (hoặc người nhận) không thể từ chối việc gửi (hoặc nhận) thông tin.



**MÁCH NƯỚC CHO KỲ THI** Việc hiểu được sự khác biệt giữa các trường hợp sử dụng phổ biến và có khả năng xác định những trường hợp sử dụng có thể áp dụng cho một tình huống nhất định là một phần tử có thể kiểm tra được tương ứng với mục tiêu của phần này.

### Những hạn chế

Khi bạn đang xem xét các tùy chọn để triển khai các giải pháp mật mã, một loạt các ràng buộc hoặc giới hạn có thể sẽ trở thành một vấn đề. Năng lực xử lý bao nhiêu, bao nhiêu dữ liệu và định dạng dữ liệu nào (khối hoặc luồng), tất cả đều quan trọng và cần được xem xét. Cũng rất quan trọng khi xem xét cách thức mà những lựa chọn này tác động hoặc hạn chế hiệu quả của giải pháp của bạn như thế nào, chẳng hạn như giải pháp của bạn có thể bảo vệ dữ liệu trong bao lâu. Có một số vấn đề chính cần tìm hiểu, chẳng hạn như tốc độ, kích thước, tác động của khóa yếu và hơn thế nữa. Chúng được mô tả trong các phần sau.

### Tốc độ

Tốc độ mã hóa và giải mã có thể là một vấn đề với nhiều hình thức giao tiếp khác nhau. Thuật toán càng phức tạp, càng nhiều vòng được thực hiện và mã hóa càng mạnh hơn, nhưng thông lượng sẽ càng chậm. Hiệu quả tính toán là một điểm chuẩn quan trọng trong mật mã hiện đại và đã dẫn đến việc các thuật toán như ChaCha20 được ưa chuộng, vì nó có lợi thế về tốc độ đáng kể so với AES.

## Kích cỡ

Trong mật mã, kích thước có ý nghĩa quan trọng và điều này liên quan đến kích thước khóa. Khóa càng lớn thì càng có nhiều dữ liệu có thể được thông qua và mã hóa càng mạnh. Kích thước đi kèm với sự-đánh-đổi: tốc độ. Các khóa dài hơn mất nhiều thời gian hơn để được tạo ra và hệ thống hoạt động càng nhiều vòng, thời gian để mã hóa/giải mã càng lâu. Vì vậy, kích thước là một phương tiện đo sức mạnh tương đối, với chi phí là tốc độ. Sự-đánh-đổi này là một cân nhắc chính trong việc phát triển các thuật toán để triển khai trong thực tế.

## Các Khóa Yếu

Độ mạnh của mật mã là một hàm của độ mạnh của thuật toán và độ mạnh của khóa. Như đã đề cập trước đó, độ dài khóa có thể là một yếu tố quan trọng tạo nên sức mạnh của một giải pháp mật mã. Nhưng cũng có những vấn đề về các khóa yếu, hoặc các khóa, bất kể độ dài, đối với một thuật toán nhất định dẫn đến mã hóa yếu hơn.

Đối với một số thuật toán, có những trường hợp các giá trị khóa dẫn đến mã hóa yếu hơn. Một giá trị khóa bao gồm tất cả các số 0 hoặc tất cả các số 1 chỉ là một giá trị khóa khác trong tập hợp tất cả các giá trị khả dĩ, nhưng những số như số này hoặc những số có hình mẫu có thể gây ra những điểm yếu. Một thuật toán hoàn hảo sẽ không có các giá trị khóa yếu, nhưng không phải tất cả các thuật toán đều có chung đặc điểm được mong muốn này. Hiện tại các thuật toán DES, RC4, IDEA, Blowfish và GMAC có thể phải chịu đựng các khóa yếu. Việc hiểu được vấn đề và loại bỏ việc sử dụng các khóa yếu như một phần của việc triển khai một thuật toán cụ thể là một biện pháp bảo vệ quan trọng.

## Thời gian

Không có gì tồn tại mãi mãi, ngay cả trong mật mã. Nếu có đủ thời gian, bất kỳ mã hóa nào đều cũng có thể bị phá vỡ - người ta đơn giản chỉ cần

thử tất cả các khóa. Đây được coi là một cuộc tấn công brute-force. Vì vậy, mục tiêu của mật mã là bảo vệ dữ liệu trong một khoảng thời-gian-đủ-dài để giải mã brute-force không phải là một yếu tố trong phương trình bảo mật. Với các thuật toán mã hóa hiện đại như AES và điện toán quy ước (phi-lượng-tử), thời gian để xử lý vẫn đề vượt quá tuổi thọ của con người, vì vậy các hệ thống được coi là an toàn. Các phương pháp cũ hơn, chẳng hạn như DES, đã được chứng minh là không còn cung cấp thời gian bảo vệ đủ lâu nữa do tốc độ của năng lực tính toán hiện đại.

### Tuổi thọ

Tuổi thọ của một lược đồ mã hóa không phải được đo bằng năng lực tính toán ngày nay mà dựa trên sự gia tăng năng lực tính toán so với thời gian bảo vệ được kỳ vọng mà mã hóa mong muốn. Nếu chúng ta muốn bảo vệ tài liệu trong 25 năm tới, chúng ta cần xem xét xem sức mạnh tính toán nào sẽ sẵn sàng trong 25 năm tới - một thách thức đối với những tiến bộ trong tính toán lượng tử. Mặc dù chúng ta có thể dự đoán chính xác sức mạnh tính toán thô của các nền tảng máy tính hiện tại trong nhiều thập kỷ nhưng các phương pháp mới như điện toán lượng tử gọi những dự đoán này là một câu hỏi. Điều này đã dẫn đến động lực đằng sau các cơ quan chính phủ đang làm việc trên các chương trình mã hóa thế hệ tiếp theo sẽ chống lại các nỗ lực tính toán lượng tử.

### Tính có thể dự đoán

Một yếu tố quan trọng khiến cho các hàm mật mã trở nên mạnh mẽ là một hàm ngẫu nhiên loại bỏ bất kỳ hình thức dự đoán nào. Việc sử dụng mật mã các số ngẫu nhiên là điều quan trọng, vì nó loại bỏ vấn đề về khả năng dự đoán của các bộ tạo ra số giả ngẫu nhiên. Máy tính sẽ thực hiện các hoạt động theo cách có thể tái tạo: với các đầu vào giống nhau, bạn sẽ nhận được các đầu ra giống nhau. Khi nói đến việc tạo các số ngẫu nhiên, chuỗi các số ngẫu nhiên được tạo ra bởi một thuật toán thường sẽ

có thể tái tạo được và mặc dù nó có thể trông ngẫu nhiên, nhưng nếu nói về mặt thống kê, nó thực sự không phải ngẫu nhiên vì việc biết được một trong các con số sẽ cho phép bạn biết các số sau này trong chuỗi trình tự. Điều này khiến cho việc sử dụng trình tạo mật mã số ngẫu nhiên trở nên quan trọng đối với sự thành công của các giải pháp mật mã, vì nó loại bỏ yếu tố có thể dự đoán được.

### Tái sử dụng

Việc sử dụng lại các khóa mật mã là một cách chắc chắn sẽ dẫn đến thất bại. Càng nhiều tài liệu mà kẻ tấn công có thể nhận được bằng cách sử dụng cùng một khóa thì khả năng sử dụng các công cụ phân tích mật mã để phá vỡ lược đồ [mã hóa] càng lớn. Đây chính là cách mà các cỗ máy Enigma và Purple đã thất bại trong Thế chiến thứ hai. Có một số cơ chế tích-hợp để giúp ngăn chặn những vấn đề này. Trong mã hóa khối, việc đưa vào một biến số phần tử dữ liệu giữa các khối giống hệt nhau sẽ ngăn cản việc phân tích mật mã đơn giản. Một tên gọi được đặt cho điều này là véc-tơ khởi tạo (IV), là một phương pháp có cấu trúc để tạo ra tính ngẫu nhiên. Điều quan trọng là sử dụng giá trị IV đủ dài để nó không lặp lại, vì việc sử dụng lặp lại IV trong một loạt thông điệp là nguyên nhân chính dẫn đến lỗi WEP. Việc sử dụng các khóa tạm thời là một ví dụ khác về việc ngăn chặn việc tái sử dụng phần tử mật mã vì các khóa tạm thời chỉ được sử dụng một lần.

### Mức độ hỗn loạn (Entropy)

Mức độ hoặc số lượng ngẫu nhiên được gọi là *entropy*. Entropy là thước đo mức độ không chắc chắn liên quan đến một loạt các giá trị. Entropy hoàn hảo tương đương với tính ngẫu nhiên hoàn toàn, chẳng hạn với bất kỳ chuỗi bit nào, không có tính toán nào để cải thiện việc đoán bit tiếp theo trong chuỗi. Một "thước đo" entropy đơn giản là tính bằng bit, trong đó các bit là lũy thừa của 2, đại diện cho số lượng lựa chọn. Do đó, các

tùy chọn 2048 sẽ đại diện cho 11-bit của entropy. Theo cách này, người ta có thể tính toán entropy của mật khẩu và đo lường mức độ “khó” đoán của chúng. Có những công thức toán học cụ thể để có thể ước tính entropy và những công thức này cung cấp một phương tiện đo lường độ ngẫu nhiên thực sự liên quan đến một đề mục kỹ thuật số.



**MÁCH NƯỚC CHO KỲ THI** Việc thiếu đi một entropy thích hợp có thể khiến cho một hệ thống mật mã dễ bị tổn thương và không thể mã hóa dữ liệu một cách an toàn.

### **Chi phí Tính toán**

Các thuật toán khác nhau có các phương tiện khác nhau để tính toán mức độ phức tạp khiến cho các giải pháp mật mã trở nên an toàn. Một trong những hạn chế của hệ thống mật mã là mức chi phí dành cho việc tính toán cần thiết để tạo ra hệ thống. Khái niệm này đã thúc đẩy các hệ thống như hệ thống mật mã đường cong elliptic, trong đó các phép tính dựa trên phép cộng, trái ngược với hệ thống RSA, dựa trên phép nhân các số-lớn. Cũng như với mọi sự-đánh- đổi khác, mỗi hệ thống đều có những ưu điểm khác nhau, vì vậy chúng không thể hoán đổi cho nhau một cách phổ biến và chi phí tính toán là một trong nhiều yếu tố phải được xem xét khi phát triển một giải pháp.

### **Những ràng buộc Nguồn lực so với Bảo mật**

Khi sử dụng mật mã để bảo vệ dữ liệu, một số yếu tố cần được đưa vào kế hoạch triển khai. Một trong những quyết định đầu tiên là sự lựa chọn thuật toán. Bạn không chỉ nên tránh các thuật toán không còn được dùng nữa mà còn cần phải phù hợp thuật toán với mục đích sử dụng. Điều này bao gồm những thứ như tài nguyên có sẵn — đó là hệ thống nhúng với sức mạnh tính toán thấp hay máy chủ có phần cứng mật mã chuyên dụng?

Cần bảo vệ bao nhiêu? Tốc độ thông lượng dữ liệu là gì? Tất cả các yếu tố này cần được xem xét khi cân nhắc lựa chọn các giải pháp mật mã, vì tài nguyên hiếm khi không giới hạn và các cân nhắc về bảo mật có thể khác nhau rất nhiều.

### **Các Thuật toán Yếu/Bị phản kháng**

Theo thời gian, các thuật toán mật mã sẽ rơi vào các cuộc tấn công khác nhau hoặc chỉ là sức mạnh thô của năng lực tính toán. Thách thức đối với các thuật toán này là việc hiểu được những thuật toán nào đã rơi vào các cuộc tấn công nhưng vẫn có thể đang sẵn có để sử dụng trong thư viện phần mềm, dẫn đến việc sử dụng ứng dụng của chúng một cách không thích hợp. Mặc dù danh sách này vẫn sẽ tiếp tục phát triển, nhưng điều quan trọng là phải xem xét chủ đề này, bởi vì những thói quen cũ rất khó thay đổi. Việc sử dụng các thuật toán băm như MD5 nên được coi là không thích hợp, vì xung đột được tạo ra đã đạt được. Ngay cả các hàm băm mới hơn, chẳng hạn như SHA-1 và SHA-256, cũng có vấn đề vì chúng bị nghi ngờ là có xung đột cưỡng bức. Tiêu chuẩn Mã hóa Dữ liệu (DES) và dạng mạnh hơn thường được sử dụng của nó - 3DES, đã không còn được ưa chuộng. Tin tốt lành là các dạng mới của những chức năng này được phổ biến rộng rãi và trong rất nhiều trường hợp, chẳng hạn như với AES và ChaCha20, chúng hiệu quả hơn về mặt tính toán, mang lại hiệu suất tốt hơn.



### **MÁCH NƯỚC CHO KỲ THI**

Việc hiểu được những giới hạn khác nhau của các giải pháp mật mã và có khả năng xác định hàm ý của một kịch bản trường hợp sử dụng nhất định là một thành phần có thể kiểm tra được tương ứng với mục tiêu của phần này.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với những kiến thức cơ bản về mật mã. Chương mở đầu bằng một cuộc thảo luận về các khái niệm mật mã, sau đó là phần xem xét các chủ đề về chữ ký số, độ dài khóa, kéo căng khóa, muối, băm, trao đổi khóa, mật mã đường cong elliptic, bí mật chuyển tiếp hoàn hảo, tính toán lượng tử và kỹ nguyên hậu-lượng-tử. Chương này tiếp tục với các khái niệm về phần tử phù du, các chế độ hoạt động của mật mã khối, chuỗi khối và bộ mật mã. Một quá trình xem xét các lược đồ đối xứng và bất đối xứng, mật mã hạng nhẹ, steganography và mã hóa đồng hình cũng đã được trình bày. Chương này kết thúc với các chủ đề liên quan đến các trường hợp sử dụng phổ biến và những hạn chế của các hệ thống mật mã.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Nếu bạn cần thực hiện những hoạt động chẵng hạn như bổ sung các phần tử mã hóa, kiểu lược đồ mã hóa nào bạn sẽ sử dụng?

  - A. Bất đối xứng
  - B. Đồng hình
  - C. Luồng
  - D. Hạng nhẹ.
2. Điều nào sau đây không phải là giới hạn liên quan đến các giải pháp mật mã?

  - A. Tốc độ
  - B. Chi phí tính toán
  - C. Tuổi thọ
  - D. Entropy.
3. Bộ thuật toán nào được thiết kế dành cho các thiết bị tiêu thụ điện năng thấp như Internet of Things và các hệ thống nhúng?

  - A. Hạng Nhẹ
  - B. Băm
  - C. Luồng
  - D. Chuỗi khối.
4. Làm thế nào để bạn biến một bí mật ngắn, chẵng hạn như một mật khẩu, trở nên đủ dài để sử dụng?

  - A. Trộn muối
  - B. Kéo dài khóa
  - C. Kéo căng khóa
  - D. Hoạt động phù du.

5. Cách tốt nhất để lấy bản rõ ràng từ giá trị băm là gì?
  - A. Sử dụng phương pháp phân tích mật mã tuyến tính.
  - B. Sử dụng hàm băm ngược.
  - C. Bạn không thể lấy bản rõ ràng ra khỏi giá trị băm.
  - D. Sử dụng chìa khóa phù du.
6. Một muối cung cấp những gì?
  - A. Nó cho thuật toán biết có bao nhiêu chữ số của số nguyên tố để sử dụng.
  - B. Nó đánh dấu số nguyên tố của thuật toán bằng cách cung cấp cho nó dữ liệu ban đầu không phải là số nguyên tố.
  - C. Nó thêm các vòng bổ sung vào mật mã.
  - D. Nó cung cấp thêm entropi.
7. Điều gì khiến cho một thông điệp được ký điện tử khác với một thông điệp được mã hóa?
  - A. Thông điệp được ký điện tử có các biện pháp bảo vệ mã hóa cho tính toàn vẹn và không khước từ.
  - B. Thông điệp được ký điện tử sử dụng mã hóa mạnh hơn nhiều và khó phá vỡ hơn.
  - C. Thông điệp được mã hóa chỉ sử dụng mã hóa đối xứng.
  - D. Không có sự khác biệt.
8. Steganography thường được thực hiện bằng phương pháp nào?
  - A. Mã hóa
  - B. Véc-ctơ khởi tạo (IV)
  - C. Mã hóa LSB
  - D. Sự thay thế entropy.
9. Để tránh việc mất một thông điệp do việc giải mã ngẫu nhiên không gây ảnh hưởng đến các thông điệp đã được mã hóa khác, cần có thuộc tính nào sau đây?
  - A. Mã hóa luồng

- B.** Bí mật chuyển tiếp hoàn hảo
- C.** Entropy
- D.** Obfuscation.
- 10.** Với một lượng lớn dữ liệu dưới dạng tập tin video trực tuyến, loại phương pháp mã hóa nào tốt nhất để bảo vệ nội dung khỏi bị xem trực tiếp trái phép?
- A.** Khối đối xứng
- B.** Thuật toán băm
- C.** Mật mã luồng
- D.** Khối bất đối xứng.

## Đáp án

1. **B.** Các lược đồ đồng hình cho phép tính toán trên các phần tử đã được mã hóa.
2. **D.** Entropy là thước đo tính ngẫu nhiên, không phải là giới hạn của một giải pháp mật mã.
3. **A.** Các thuật toán mã hóa hạng nhẹ được thiết kế cho các hệ thống bị hạn chế tài nguyên.
4. **C.** Kéo dài khóa là một cơ chế lấy ra những gì có thể sẽ là khóa yếu và “kéo dài” chúng để làm cho hệ thống an toàn hơn.
5. **C.** Mật mã băm được thiết kế để giảm bớt rõ ràng xuống một giá trị nhỏ và được xây dựng để không cho phép trích xuất bản rõ. Đây là lý do tại sao chúng thường được gọi là các hàm “một chiều”.
6. **D.** Muối bổ sung thêm entropy, hoặc tính ngẫu nhiên, vào khóa mã hóa, đặc biệt cung cấp sự tách biệt giữa các đầu vào giống nhau, chẳng hạn như mật khẩu giống hệt nhau trên các tài khoản khác nhau.
7. **A.** Chữ ký điện tử bao gồm một hàm băm của thông điệp để cung cấp tính toàn vẹn của thông điệp và sử dụng mã hóa bất đối xứng để chứng minh tính không khước từ (thực tế là khóa riêng của người gửi đã được sử dụng để ký thông điệp).
8. **C.** LSB, hoặc bit ít quan trọng nhất, được thiết kế để đặt mã hóa vào trong hình ảnh theo cách ít quan trọng nhất để tránh làm thay đổi hình ảnh.
9. **B.** Bí mật chuyển tiếp hoàn hảo (PFS) là thuộc tính của một hệ thống khóa công khai, trong đó khóa bắt nguồn từ khóa khác không bị xâm phạm ngay cả khi khóa gốc bị xâm phạm trong tương lai.

**10. C.** Mã hóa luồng hoạt động tốt nhất khi dữ liệu ở dạng rất nhỏ cần được xử lý một cách nhanh chóng, chẳng hạn như video phát trực tiếp. Mật mã khôi tốt hơn khi nói đến khôi lưỡng lớn dữ liệu.

## Phần III

### Triển khai

- Chương 17 Các Giao thức Bảo mật
- Chương 18 Bảo mật Máy chủ và Ứng dụng
- Chương 19 Bảo mật Thiết kế Mạng
- Chương 20 Bảo mật Không dây
- Chương 21 Bảo mật các Giải pháp Di động
- Chương 22 Triển khai Bảo mật Đám mây
- Chương 23 Các Biện pháp kiểm soát Quản lý Tài khoản và Danh tính
- Chương 24 Triển khai Xác thực và Cấp phép
- Chương 25 Cơ sở hạ tầng Khóa Công khai

## Chương 17 Các Giao thức Bảo mật

### Các Giao thức Bảo mật

Trong chương này bạn sẽ

- Tìm hiểu cách triển khai các giao thức bảo mật đối với những tình huống nhất định,
- Khám phá các trường hợp sử dụng đối với các giao thức bảo mật.

Các giao thức cho phép giao tiếp giữa các thành phần, độc lập với nhà cung cấp và hoạt động như một ngôn ngữ để chỉ định cách thức giao tiếp được tiến hành và những gì có thể được truyền đạt. Đúng như nhiều công nghệ truyền thông, các giao thức có cả phiên bản an toàn lẫn phiên bản không an toàn. Chương này xem xét các giao thức phổ biến có thể được bảo mật và các trường hợp sử dụng của chúng.

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 3.1 của kỳ thi CompTIA Security+: Đưa ra một kịch bản, triển khai các giao thức bảo mật.

Mục tiêu của kỳ thi này là một ứng cử viên sáng giá cho các câu hỏi dựa-trên-hiệu-suất, có nghĩa là bạn nên dự kiến các câu hỏi trong đó bạn phải áp dụng kiến thức của mình về chủ đề cho một tình huống. Đáp án tốt nhất cho một câu hỏi sẽ phụ thuộc vào các chi tiết cụ thể trong tình huống trước câu hỏi, không chỉ riêng bản thân câu hỏi. Câu hỏi cũng có thể liên quan đến các nhiệm vụ khác ngoài việc chỉ chọn đáp án tốt nhất từ danh sách. Thay vào đó, nó có thể liên quan đến việc mô phỏng thực tế các bước cần thực hiện để giải quyết một vấn đề.

## Các Giao thức

*Các giao thức* hoạt động như một ngôn ngữ chung, cho phép các thành phần khác nhau nói chuyện với nhau bằng cách sử dụng một bộ các câu lệnh được chia sẻ đã biết. Giao thức bảo mật là những giao thức có cơ chế bảo mật được tích-hợp để theo mặc định, bảo mật có thể được thực thi thông qua giao thức. Nhiều giao thức khác nhau tồn tại, tất cả đều được sử dụng để đạt được các mục tiêu giao tiếp cụ thể.

---



**MÁCH NƯỚC CHO KỲ THI** Trong kỳ thi, bạn nên dự kiến sẽ được yêu cầu triển khai các giao thức và dịch vụ chung khi được cung cấp một tình huống cơ bản. Hãy chú ý nhiều đến các chi tiết giao thức và các số cổng được đề cập trong toàn bộ chương này!

## Domain Name System Security Extensions (DNSSEC)

Hệ thống Tên Miền (Domain Name System - DNS) là một giao thức để diễn dịch tên miền thành địa chỉ IP. Khi người dùng nhập một tên miền chẳng hạn như [www.example.com](http://www.example.com), DNS sẽ chuyển đổi tên này thành địa chỉ IP là các con số thực tế. Các bản ghi DNS cũng được sử dụng để gửi email. Giao thức DNS sử dụng UDP qua cổng 53 cho các truy vấn tiêu chuẩn, mặc dù TCP có thể được sử dụng cho các chuyển giao lớn như chuyển tiếp vùng. DNS là một hệ thống bao gồm các máy chủ được phân cấp, từ các bản sao cục bộ của các bản ghi thông qua các nhà cung cấp Internet đến các máy chủ cấp-root. DNS là một trong những giao thức nền tảng chủ yếu được sử dụng trên Internet và có liên quan đến hầu hết các tra cứu địa chỉ. Vấn đề với DNS là các yêu cầu và phản hồi được gửi đi dưới dạng văn bản rõ ràng và có thể bị giả mạo.

*DNSSEC (Phần mở rộng Bảo mật Hệ thống Tên Miền – Domain Name System Security Extensions)* là một tập hợp các phần mở rộng cho giao

thức DNS, thông qua việc sử dụng mật mã, cho phép xác thực nguồn gốc của dữ liệu DNS, xác thực từ chối sự tồn tại và tính toàn vẹn của dữ liệu nhưng không mở rộng đến tính sẵn sàng hoặc bảo mật. Các bản ghi DNSSEC được ký để tất cả các phản hồi DNSSEC được xác thực nhưng không được mã hóa. Điều này ngăn chặn việc các phản hồi DNS trái phép được hiểu là đúng. Sự từ chối về sự tồn tại đã được xác thực cũng cho phép trình phân giải xác thực rằng một tên miền nhất định hiện đang không tồn tại.

Truyền dữ liệu qua cổng UDP 53 có kích thước bị giới hạn ở 512-byte và các gói DNSSEC có thể lớn hơn. Vì lý do này, DNSSEC thường sử dụng cổng TCP 53 cho hoạt động của nó. Có thể mở rộng kích thước gói UDP lên 4096 để ứng phó với DNSSEC và điều này được đề cập trong RFC 2671.



**MÁCH NƯỚC CHO KỲ THI** DNSSEC xác thực dữ liệu DNS, từ đó mang lại tính toàn vẹn, nhưng nó không cung cấp các kiểm soát đối với tính sẵn sàng hoặc bảo mật.

## SSH

Giao thức *Secure Shell (SSH)* là một chương trình kết nối thiết bị đầu cuối từ xa được mã hóa được sử dụng cho các kết nối từ xa đến một máy chủ. SSH sử dụng mã hóa bắt đối xứng nhưng thường yêu cầu một nguồn tin cậy độc lập với một máy chủ để hoạt động, chẳng hạn như nhận một khóa của máy chủ bằng cách thủ công. SSH sử dụng cổng TCP 22 như là cổng mặc định của nó.



**MÁCH NƯỚC CHO KỲ THI** SSH sử dụng mật mã khóa công khai để truy cập thiết bị đầu cuối từ xa an toàn và đã được thiết kế như sự thay thế an toàn cho Telnet.

### **Phần mở rộng Thư Internet Đa mục đích/ Bảo mật (Secure/Multipurpose Internet Mail Extensions (S/MIME))**

MIME (Phần mở rộng Thư Internet Đa Mục đích) là một tiêu chuẩn để truyền dữ liệu nhị phân thông qua email. Các email được gửi đi dưới dạng tập tin văn bản rõ ràng và bất kỳ tập tin đính kèm nào cũng cần được mã hóa để phù hợp với định dạng văn bản rõ ràng. MIME chỉ định cách thức điều này được thực hiện với mã hóa Base64. Bởi vì nó là dạng văn bản rõ ràng và không có bảo mật liên quan đến các tập tin đính kèm nên chúng có thể được nhìn thấy bởi bất kỳ máy nào giữa người gửi và người nhận. S/MIME (*Tiện ích mở rộng Thư Internet An toàn/Đa mục đích*) là một tiêu chuẩn để mã hóa khóa công khai và ký dữ liệu MIME trong email. S/MIME được thiết kế để cung cấp các biện pháp bảo vệ mật mã đối với email và được tích hợp vào phần lớn phần mềm email hiện đại để tạo điều kiện thuận lợi cho khả năng tương tác lẫn nhau.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng S/MIME là tiêu chuẩn để mã hóa email. Nó cung cấp sự xác thực, tính toàn vẹn thông điệp và không khước từ trong email.

### **Giao thức Truyền tải Thời-gian-thực Bảo mật (Secure Real-time Transport Protocol (SRTP))**

*Giao thức Truyền tải Thời-gian-thực Bảo mật (SRTP)* là một giao thức mạng để bảo mật việc cung cấp âm thanh và hình ảnh qua các mạng IP. SRTP sử dụng mật mã để cung cấp mã hóa, xác thực và toàn vẹn thống

điệp, và bảo vệ phát lại cho dữ liệu Giao thức Truyền tải Thời-gian-thực (RTP).

### **Giao thức Truy cập Danh bạ Hạng nhẹ qua SSL (Lightweight Directory Access Protocol over SSL (LDAPS))**

Giao thức Truy cập Danh bạ Hạng nhẹ (LDAP) là giao thức chính để truyền thông tin danh bạ. Các dịch vụ danh bạ có thể cung cấp bất kỳ tập hợp bản ghi có tổ chức nào, thường có cấu trúc phân cấp và được sử dụng trong một loạt các trường hợp, bao gồm cả tập dữ liệu Active Directory (AD). Theo mặc định, lưu lượng LDAP được truyền là không an toàn. Bạn có thể làm cho lưu lượng LDAP trở nên an toàn bằng cách sử dụng nó với SSL/TLS, được gọi là *LDAP qua SSL (LDAPS)*. Thông thường, LDAP được chophép qua SSL/TLS bằng cách sử dụng chứng chỉ từ tổ chức phát hành chứng chỉ đáng tin cậy (CA).

LDAPS sử dụng đường hầm SSL/TLS để kết nối các dịch vụ LDAP. Về mặt kỹ thuật, phương pháp này đã được gỡ bỏ với LDAPv2 và được thay thế bằng Lớp Bảo mật và Xác thực Đơn giản (Simple Authentication and Security Layer - SASL) trong LDAPv3. SASL (không được liệt kê trong mục tiêu của kỳ thi) là một phương pháp tiêu chuẩn sử dụng TLS để bảo mật các dịch vụ trên Internet.



**MÁCH NƯỚC CHO KỲ THI** Giao tiếp LDAPS diễn ra thông qua cổng TCP 636. Giao tiếp LDAPS với một máy chủ danh mục toàn cầu diễn ra thông qua cổng TCP 3269. Khi kết nối đến cổng 636 hoặc 3269, SSL/TLS được thương lượng trước khi bất kỳ lưu lượng LDAP nào được trao đổi.

## **Giao thức Truyền tải Tập tin An toàn (File Transfer Protocol, Secure (FTPS))**

*Giao thức Truyền tải Tập tin An toàn (SFTP)* là sự triển khai FTP qua một kênh được bảo mật bằng SSL/TLS. Giao thức này hỗ trợ khả năng tương thích FTP hoàn toàn, nhưng vẫn cung cấp các biện pháp bảo vệ mã hóa được hỗ trợ bởi SSL/TLS. FTPS sử dụng cổng TCP 989 (cổng kết nối dữ liệu) và cổng 990 (cổng kết nối kiểm soát). Vì SSL không còn được tán thành nữa, theo RFC 7568, giờ đây TLS được sử dụng trong FTPS.

## **Giao thức Truyền tải Tập tin SSH (SSH File Transfer Protocol (SFTP))**

*Giao thức Truyền tải Tập tin SSH (SFTP)* là sử dụng FTP qua một kênh SSH. Giao thức này tận dụng các biện pháp bảo vệ mã hóa của SSH để bảo mật truyền tải FTP. Vì nó phụ thuộc vào SSH nên SFTP sử dụng cổng TCP 22.

## **Giao thức Quản lý Mạng Đơn giản, Phiên bản 3 (Simple Network Management Protocol, Version 3 (SNMPv3))**

*Giao thức Quản lý Mạng Đơn giản, phiên bản 3 (SNMPv3)* là một tiêu chuẩn để quản lý các thiết bị trên mạng dựa-trên-IP. SNMPv3 được phát triển đặc biệt để giải quyết các mối lo ngại và lỗ hổng bảo mật của SNMPv1 và SNMPv2. SNMP là một giao thức lớp-ứng-dụng, một phần của bộ giao thức IP và có thể được sử dụng để quản lý và giám sát các thiết bị, bao gồm các thiết bị mạng, các máy tính và các thiết bị khác được kết nối với mạng IP. Tất cả các phiên bản SNMP đều yêu cầu các cổng 161 và 162 phải được mở trên tường lửa.



**MÁCH NƯỚC CHO KỲ THI** Nếu được giới thiệu một kịch bản quản lý mạng, hãy nhớ rằng phiên bản bảo mật của SNMP chỉ có SNMPv3.

## Giao thức Truyền tải Siêu văn bản qua SSL/TLS (Hypertext Transfer Protocol over SSL/TLS (HTTPS))

*Giao thức Truyền tải Siêu văn bản Bảo mật (HTTPS)* là sử dụng SSL hoặc TLS để mã hóa kênh mà lưu lượng HTTP đang được truyền tải qua đó. Do các vấn đề với tất cả các phiên bản SSL, chỉ có TLS được khuyến nghị sử dụng. HTTPS sử dụng cổng TCP 443 và là phương pháp được sử dụng rộng rãi nhất để bảo mật cho lưu lượng HTTP.

*Lớp Cổng Bảo mật (Secure Socket Layer - SSL)* là một ứng dụng không sử dụng nữa của công nghệ mã hóa đã được phát triển cho các giao thức lớp-truyền-tải trên Web. Giao thức này đã sử dụng các phương pháp mã hóa khóa công khai để trao đổi khóa đối xứng dành cho việc sử dụng trong bảo vệ tính bảo mật và toàn vẹn cũng như xác thực. Phiên bản cuối cùng, v3, đã lỗi thời, đã được thay thế bằng TLS tiêu chuẩn IETF. Tất cả các phiên bản SSL đã không còn được sử dụng nữa do các vấn đề bảo mật và trong phần lớn các máy chủ thương mại sử dụng SSL/TLS, SSL đã ngừng hoạt động. Do sự phổ biến của việc sử dụng thuật ngữ SSL, nó sẽ tồn tại trong một thời gian khá dài, nhưng bề mặt chức năng, mã hóa hiện đang được thực hiện thông qua TLS.

*Bảo mật Lớp Truyền tải (Transport Layer Security - TLS)* là một tiêu chuẩn IETF cho việc sử dụng công nghệ mã hóa và thay thế cho SSL. Sử dụng các nguyên tắc cơ bản giống nhau, TLS cập nhật các cơ chế được sử dụng bởi SSL. Mặc dù đôi khi được gọi là SSL nhưng nó là một tiêu chuẩn riêng biệt. Cổng tiêu chuẩn cho SSL và TLS không được xác định vì nó phụ thuộc vào giao thức đang được bảo vệ sử dụng, ví dụ: cổng 80 cho HTTP trở thành cổng 443 khi nó là cho HTTPS.



**MÁCH NƯỚC CHO KỲ THI** HTTPS được sử dụng để bảo mật giao tiếp web. Sử dụng cổng 443, nó cung cấp tính toàn vẹn và bảo mật.

## IPSec

IPSec là một tập hợp các giao thức do IETF phát triển để trao đổi các gói tin một cách an toàn ở lớp mạng (lớp 3) của mô hình OSI (RFCs 2401 - 2412). Mặc dù các giao thức này chỉ hoạt động cùng với mạng IP nhưng khi một khi kết nối IPSec được thiết lập, có thể tạo một đường hầm qua các mạng khác ở các mức thấp hơn của mô hình OSI. Tập hợp các dịch vụ bảo mật do IPSec cung cấp diễn ra ở lớp mạng của mô hình OSI, vì vậy các giao thức lớp cao hơn, chẳng hạn như TCP, UDP, Giao thức Kiểm soát Thông điệp Internet (ICMP), Giao thức Cửa ngõ Ranh giới (Border Gateway Protocol - BGP), và các giao thức tương tự, không có chức năng bị thay thế bởi việc triển khai các dịch vụ IPSec.

Loạt giao thức IPSec có một loạt các dịch vụ mà nó được thiết kế để cung cấp, bao gồm nhưng không giới hạn ở kiểm soát truy cập, tính toàn vẹn không kết nối, tính bảo mật của luồng-lưu-lượng, từ chối các gói được phát lại, bảo mật dữ liệu (mã hóa) và xác thực nguồn gốc dữ liệu. IPSec có hai chế độ xác định – truyền tải và đường hầm – cung cấp các mức độ bảo mật khác nhau. IPSec cũng có ba chế độ kết nối: host-to-server, server-to-server và host-to-host.

Có thể sử dụng đồng thời cả hai phương pháp, chẳng hạn như sử dụng phương thức truyền tải trong mạng của chính mình để đi đến một máy chủ IPSec, sau đó là phương thức đường hầm đi đến mạng của máy chủ đích, kết nối với máy chủ IPSec ở đó, rồi lại sử dụng phương thức truyền tải từ máy chủ IPSec của mạng được nhắm mục tiêu đến máy chủ đích. IPSec sử dụng thuật ngữ *liên kết bảo mật (SA)* để mô tả sự kết hợp duy

nhất một chiều giữa thuật toán cụ thể và lựa chọn khóa để cung cấp một kênh được bảo vệ. Nếu lưu lượng truy cập là hai chiều, hai SA là cần thiết và trên thực tế có thể là khác nhau.

### **Tiêu đề Xác thực (Authentication Header – AH)/Tải trọng Bảo mật Đóng gói (Encapsulated Security Payload – ESP)**

IPSec sử dụng hai giao thức để cung cấp bảo mật cho lưu lượng:

- Tiêu đề xác thực (AH)
- Đóng gói khối lượng bảo mật (ESP)

IPSec không xác định các thuật toán bảo mật cụ thể, cũng như không yêu cầu các phương pháp triển khai cụ thể. IPSec là một khuôn khổ mở cho phép các nhà cung cấp triển khai các thuật toán theo tiêu-chuẩn-ngành hiện có thích hợp với các nhiệm vụ cụ thể. Tính linh hoạt này là chìa khóa trong khả năng của IPSec trong việc cung cấp một loạt các chức năng bảo mật. IPSec cho phép một số công nghệ bảo mật được kết hợp thành một giải pháp toàn diện để bảo mật, toàn vẹn và xác thực dựa-trên-mạng. IPSec sử dụng những điều dưới đây:

- Trao đổi khóa Diffie-Hellman (RFC 3526) và ECDH (RFC 4753) giữa các máy ngang hàng trên mạng công cộng
- Ký khóa công khai của các trao đổi khóa Diffie-Hellman để đảm bảo danh tính và tránh các cuộc tấn công người-trung-gian
- Các thuật toán mật mã được xác định để sử dụng với IPsec:
  - HMAC-SHA1/SHA2 để bảo vệ tính toàn vẹn và tính xác thực
  - TripleDES-CBC để bảo mật
  - AES-CBC để bảo mật
  - AES-GCM để cung cấp tính bảo mật và xác thực cùng nhau một cách hiệu quả

- ChaCha20 + Poly1305 để cung cấp tính bảo mật và xác thực cùng nhau một cách hiệu quả
- Các thuật toán xác thực:
  - RSA
  - ECDSA (RFC 4754)
  - PSK (RFC 6617)
- Chứng chỉ kỹ thuật số để hoạt động như thẻ ID kỹ thuật số giữa các bên

Để cung cấp bảo mật lưu lượng, hai phần mở rộng tiêu đề đã được xác định cho các sơ đồ IP. *AH*, khi được thêm vào một sơ đồ IP, sẽ đảm bảo tính toàn vẹn của dữ liệu và cũng như tính xác thực của nguồn gốc dữ liệu. Bằng cách bảo vệ các phần tử không thay đổi trong tiêu đề IP, AH bảo vệ địa chỉ IP, cho phép xác thực nguồn gốc dữ liệu. *ESP* chỉ cung cấp các dịch vụ bảo mật cho phần giao thức cấp-cao-hơn của gói tin chứ không phải cho tiêu đề IP.



**MÁCH NƯỚC CHO KỲ THI**      IPSec *AH* bảo vệ tính toàn vẹn, nhưng nó không cung cấp quyền riêng tư bởi vì chỉ có tiêu đề được bảo mật. IPSec *ESP* cung cấp tính bảo mật, nhưng không bảo vệ tính toàn vẹn của gói tin. Để bao hàm cả quyền riêng tư lẫn tính toàn vẹn, cả hai tiêu đề đều có thể được sử dụng cùng một lúc.

AH và ESP có thể được sử dụng một cách riêng biệt hoặc kết hợp, tùy thuộc vào mức độ và kiểu bảo mật mong muốn. Cả hai cũng hoạt động với các chế độ truyền tải và đường hầm của các giao thức IPSec.

## Đường hầm/Truyền tải

Chế độ *truyền tải* chỉ mã hóa phần dữ liệu của một gói tin, do đó cho phép một người bên ngoài nhìn thấy được các địa chỉ IP nguồn và đích. Chế độ truyền tải bảo vệ các giao thức cấp-cao-hơn được liên kết với một gói tin và bảo vệ dữ liệu đang được truyền nhưng cho phép biết được chính bản thân quá trình truyền tải. Bảo vệ phần dữ liệu của gói được gọi là bảo vệ nội dung.

Chế độ *đường hầm* cung cấp mã hóa các địa chỉ IP nguồn và đích cũng như chính bản thân dữ liệu. Điều này cung cấp khả năng bảo mật cao nhất, nhưng nó chỉ có thể được thực hiện giữa các máy chủ IPSec (hoặc bộ định tuyến) vì đích cuối cùng cần phải được biết để phân phối [các gói tin]. Bảo vệ thông tin tiêu đề còn được gọi là bảo vệ ngữ cảnh.



**MÁCH NƯỚC CHO KỲ THI** Trong *chế độ truyền tải* (từ-đầu-đến-cuối), bảo mật lưu lượng gói tin được cung cấp bởi các máy tính đầu cuối. Trong *chế độ đường hầm* (từ-cổng-đến-cổng) bảo mật lưu lượng gói tin được cung cấp giữa các máy nút đầu cuối trong từng mạng và không phải tại các máy chủ đầu cuối.

### **Giao thức Bưu điện (Post Office Protocol (POP))/Giao thức Truy cập Thư Internet (Internet Message Access Protocol (IMAP))**

*Giao thức Bưu điện (POP)/Giao thức Truy cập Thư Internet (IMAP)* tương ứng để cập đến POP3 và IMAP4, sử dụng cổng 110 cho POP3 và 143 cho IMAP. Khi POP và IMAP được gửi qua một phiên SSL/TLS, POP3 bảo mật sử dụng cổng TCP 995 và IMAP4 bảo mật sử dụng cổng TCP 993. Dữ liệu đã được mã hóa từ ứng dụng email được gửi đến máy chủ email qua phiên SSL/TLS. Với việc SSL ngừng sử dụng, TLS là giao thức được ưa chuộng hiện nay. Nếu các kết nối email được khởi động ở chế độ không bảo mật, chỉ thị STARTTLS sẽ yêu cầu các máy khách thay đổi sang các cổng bảo mật.

Giao thức thư khác, Giao thức Truyền tải Thư Đơn giản (SMTP), sử dụng nhiều cổng khác nhau, tùy thuộc vào cách sử dụng. Cổng mặc định của máy chủ SMTP là cổng TCP 25. Máy khách thư thường chỉ sử dụng SMTP khi giao tiếp với máy chủ chuyển tiếp thư và sau đó họ sử dụng cổng TCP 587 hoặc khi được mã hóa SSL/TLS, cổng TCP 465 (RFC 8314).

---



**MÁCH NƯỚC CHO KỲ THI** IMAP sử dụng cổng 143, nhưng IMAP4 bảo mật sử dụng cổng 993. POP3 sử dụng cổng 110 nhưng POP3 bảo mật sử dụng cổng 995.

---



**MÁCH NƯỚC CHO KỲ THI** SMTP giữa các máy chủ là cổng TCP 25, nhưng khi các máy khách có liên quan, đó là cổng TCP 587 hoặc, nếu được mã hóa, là cổng TCP 465.

### Các Trường hợp Sử dụng

Các giao thức cho phép các bên có được hiểu biết chung về cách thức giao tiếp sẽ được xử lý như thế nào và chúng xác định những kỳ vọng cho từng bên. Vì các trường hợp sử dụng khác nhau có các nhu cầu giao tiếp khác nhau nên các giao thức khác nhau sẽ được sử dụng trong các trường hợp sử dụng khác nhau. Nhiều nhóm công tác của IETF đã và đang làm việc để chuẩn hóa một số giao thức bảo mật có mục-đích-chung, những giao thức có thể được sử dụng lại nhiều lần thay vì phát minh ra những giao thức mới cho từng trường hợp sử dụng. SASL, được giới thiệu trước đó trong chương, là một ví dụ về nỗ lực như vậy, SASL là một phương pháp đã được tiêu chuẩn hóa để viện dẫn một đường hầm TLS để bảo mật một kênh truyền thông. Phương pháp này đã được chứng minh

là hoạt động với nhiều loại dịch vụ - hiện có hơn 15 và đang ngày càng gia tăng.

Phần này sẽ xem xét một số trường hợp sử dụng phổ biến và các giao thức bảo mật tương ứng được sử dụng trong các trường hợp sử dụng đó.

---



**MÁCH NƯỚC CHO KỲ THI** Phần này đề cập đến cách thức mà các giao thức khác nhau được sử dụng trong các trường hợp sử dụng khác nhau như thế nào. Với một trường hợp sử dụng trong đề thi, bạn cần phải có khả năng xác định chính xác (các) giao thức cũng như có khả năng thực hiện chính xác điều ngược lại: xác định các trường hợp sử dụng đối với một giao thức nhất định.

### **Âm thanh và Phim ảnh**

*Âm thanh thoại và phim ảnh* thường xuyên là phương tiện truyền trực tuyến và do vậy, sẽ có các giao thức riêng để mã hóa các luồng dữ liệu. Để truyền những tài liệu này một cách an toàn, bạn có thể sử dụng Giao thức Truyền tải Thời-gian-thực Bảo mật (Secure Real-time Transport Protocol - SRTP), vốn sẽ truyền tải âm thanh và phim ảnh qua mạng IP một cách an toàn. SRTP được đề cập đến trong RFC 3711 (<https://tools.ietf.org/html/rfc3711>).

---



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng SRTP là một phiên bản bảo mật của RTP. Nó thường được sử dụng cho VoIP cũng như cho việc phát ứng dụng đa phương tiện.

## Đồng bộ Thời gian

Giao thức Thời gian Mạng (NTP) là tiêu chuẩn để *đồng bộ hóa thời gian* giữa các máy chủ và máy khách. NTP được truyền qua cổng UDP 123. NTP không có gì đảm bảo để chống lại một cuộc tấn công người-trung-gian và mặc dù điều này đã làm dấy lên những lo ngại về hệ quả, cho đến nay, vẫn chưa có gì được thực hiện để bảo mật NTP một cách trực tiếp hoặc để thiết kế cơ chế kiểm tra bảo mật ngoài-băng-tần. Nếu bạn quá nhạy cảm với rủi ro này, bạn có thể gửi tất cả giao tiếp mọi thời điểm băng cách sử dụng đường hầm TLS, mặc dù đây không phải là một thực tiễn trong ngành.

## Email và Web

*Email* và *Web* đều là hệ thống dựa-trên-bản-rõ-ràng bẩm sinh. Như đã thảo luận ở phần trước đây cũng trong chương này, HTTPS, dựa trên SSL/TLS, được sử dụng để bảo mật các kết nối web. Việc sử dụng HTTPS khá phổ biến và rộng rãi. Hãy nhớ rằng SSL không còn được coi là an toàn nữa. Email phức tạp hơn một chút để bảo mật, và lựa chọn tốt nhất là thông qua S/MIME, cũng đã được thảo luận trước đây trong chương này.

## Truyền tải Tập tin

*Truyền tải tập tin* an toàn có thể được thực hiện thông qua rất nhiều phương pháp, đảm bảo tính bảo mật và toàn vẹn của việc truyền tập tin qua mạng. FTP không an toàn, nhưng như đã thảo luận trước đây, SFTP và FTPS là những lựa chọn thay thế an toàn có thể được sử dụng.

## Dịch vụ Danh bạ

Các *dịch vụ danh bạ* sử dụng LDAP làm giao thức chính. Khi bảo mật là bắt buộc thì LDAPS là một tùy chọn phổ biến, như đã được mô tả trước đây. Các dịch vụ danh bạ thường được tìm thấy ở hậu trường liên quan đến thông tin đăng nhập.

## Truy cập Từ xa

*Truy cập từ xa* là phương tiện mà người dùng có thể truy cập tài nguyên máy tính qua một mạng. Việc bảo mật truy cập từ xa có thể được thực hiện thông qua rất nhiều phương tiện - một số để đảm bảo quá trình xác thực và những phương tiện khác cho chính bản thân việc truy cập dữ liệu thực tế. Cũng như trong nhiều tình huống yêu cầu việc bảo mật các kênh giao tiếp hoặc bảo mật dữ liệu khi truyền, các tổ chức thường sử dụng SSL/TLS để bảo mật truy cập từ xa. Tùy thuộc vào thiết bị đang được truy cập sẽ có nhiều giao thức bảo mật khác nhau. Đối với thiết bị mạng, chẳng hạn như bộ định tuyến và thiết bị chuyển mạch, SSH là giải pháp thay thế an toàn cho Telnet. Đối với các máy chủ và các kết nối máy tính khác, truy cập thông qua VPN hoặc sử dụng IPSec là phổ biến.

## Phân giải Tên Miền

*Việc phân giải tên miền* được thực hiện chủ yếu bởi giao thức DNS. DNS là một giao thức văn bản rõ ràng và phiên bản bảo mật, DNSSEC, vẫn chưa được triển khai rộng rãi. Đối với triển khai cục bộ, DNSSEC đã có sẵn trong các miền Windows Active Directory từ năm 2012. Xét từ góc độ hoạt động, cả TCP và cổng UDP 53 đều có thể được sử dụng cho DNS, với nhu cầu bảo vệ tường lửa giữa Internet và cổng TCP 53 để ngăn chặn những kẻ tấn công truy cập vào vùng chuyển (transfer zone).

## Định tuyến và Chuyển mạch

*Việc định tuyến và chuyển mạch* là các chức năng xương sống của kết nối mạng trong hệ thống. Quản lý dữ liệu liên kết với mạng là địa hạt của SNMPv3. SNMPv3 cho phép các ứng dụng quản lý dữ liệu được liên kết với mạng và các thiết bị. Việc truy cập cục bộ vào các hộp có thể được thực hiện bởi Telnet, mặc dù vì lý do bảo mật nên SSH nên được sử dụng để thay thế.

## Phân bổ Địa chỉ Mạng

Việc quản lý các chức năng *phân bổ địa chỉ mạng* trong một hệ thống mạng đòi hỏi nhiều tiêu chí quyết định, bao gồm cả việc giảm thiểu độ phức tạp và quản lý tên và vị trí của thiết bị. SNMPv3 có nhiều chức năng có thể được sử dụng để quản lý các luồng dữ liệu của thông tin này tới các ứng dụng quản lý để có thể hỗ trợ quản trị viên trong việc phân bổ [tài nguyên] mạng.

Địa chỉ IP có thể được cấp phát tĩnh, có nghĩa là cấu hình thủ công địa chỉ IP cố định cho từng thiết bị hoặc thông qua DHCP, cho phép tự động hóa việc gán địa chỉ IP. Trong một số trường hợp, sự kết hợp giữa tĩnh và DHCP được sử dụng. Phân bổ địa chỉ IP là một phần của thiết kế mạng thích hợp, vốn là điều rất quan trọng đối với hiệu suất và khả năng mở rộng của mạng. Hãy tìm hiểu cách phân bổ đúng địa chỉ IP cho một mạng mới - và biết các tùy chọn của bạn nếu bạn hết địa chỉ IP.



## MÁCH NƯỚC CHO KỲ THI

Một số trường hợp sử dụng trong quá khứ có liên quan nhưng khác nhau. Hãy chú ý một cách cẩn thận đến từ ngữ chính xác của câu hỏi khi bạn phải chọn trong số các tùy chọn như phân giải tên miền, định tuyến và phân bổ địa chỉ. Tất cả chúng đều được liên kết với mạng IP, nhưng chúng thực hiện các chức năng riêng biệt.

## Các Dịch vụ Thuê bao

Các *dịch vụ thuê bao* liên quan đến việc quản lý các luồng dữ liệu đến và đi từ một hệ thống dựa trên mô hình đẩy (xuất bản) hoặc kéo (đăng ký). Việc quản lý các phần tử dữ liệu nào là cần thiết bởi các nút nào là một vấn đề mà bạn có thể giải quyết bằng cách sử dụng các dịch vụ danh bạ như LDAP.

Một cách sử dụng khác của các dịch vụ thuê bao là mô hình Phần mềm như một Dịch vụ (SaaS), trong đó phần mềm được cấp phép trên cơ sở đăng ký. Phần mềm thực tế được lưu trữ tập trung, thường là trên đám mây và quyền truy cập của người dùng dựa trên đăng ký thuê bao. Điều này đang trở thành một mô hình kinh doanh phần mềm rất phổ biến.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các giao thức bảo mật được sử dụng trong doanh nghiệp và các trường hợp sử dụng mà chúng áp dụng. Cụ thể, bạn đã kiểm tra các giao thức sau: DNSSEC, SSH, S/MIME, SRTP, LDAPS, FTPS, SFTP, SNMPv3, HTTPS (SSL/TLS), IPSec, Authentication Header (AH)/Encapsulated Security Payload (ESP), đường hầm/truyền tải và Bảo mật POP3 / IMAP4. Chương này sau đó chuyển sang tìm hiểu các giao thức nào áp dụng trong các trường hợp sử dụng liên quan đến thoại và video, đồng bộ hóa thời gian, e-mail và Web, truyền tập tin, dịch vụ danh bạ, truy cập từ xa, phân giải tên miền, định tuyến và chuyển mạch, phân bổ địa chỉ mạng và các dịch vụ đăng ký thuê bao. Yếu tố quan trọng của chương này là nó đã chuẩn bị cho bạn để chọn các giao thức bảo mật chính xác cho các trường hợp sử dụng khi đưa ra một tình huống trong kỳ thi CompTIA Security+.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Một người dùng báo cáo cho bộ phận hỗ trợ kỹ thuật rằng anh ấy đang nhận được thông báo lỗi “không thể phân giải địa chỉ” từ trình duyệt của mình. Cổng nào có khả năng là một vấn đề trên tường lửa của anh ấy?

A. 22.  
B. 53  
C. 161  
D. 162.
2. Đâu là điểm yếu của giao thức DNS?

A. Yêu cầu và phản hồi đều được gửi dưới dạng văn bản rõ ràng.  
B. Nó không cung cấp tiêu chuẩn hóa thanh toán trong cơ sở hạ tầng đám mây.  
C. TCP có thể được sử dụng cho các truyền tải lớn như chuyển vùng.  
D. Năng lực mã hóa của nó chậm.
3. DNSSEC có những lợi ích nào dưới đây?

A. Khả năng mở rộng  
B. Các khoản chi tiêu thấp hơn từ các khoản chi tiêu vốn hoạt động (operations capital - OpsCap)  
C. Cho phép xác thực nguồn gốc, xác thực từ chối sự tồn tại và tính toàn vẹn của dữ liệu  
D. Tính sẵn sàng và tính bảo mật.
4. Giao thức Secure Shell (SSH) là gì?

- A.** Đây là một chương trình kết nối đầu cuối từ xa được mã hóa được sử dụng cho các kết nối từ xa tới máy chủ.
- B.** Nó cung cấp diễn dịch địa chỉ mạng động.
- C.** Nó cung cấp Phần mềm như một Dịch vụ (SaaS).
- D.** Nó cung cấp ảnh chụp nhanh của các máy vật lý tại một thời điểm.
- 5.** Mục đích của giao thức Mở rộng Thư Internet Bảo mật/Đa năng (S/MIME) là gì?
- A.** Được sử dụng trong mã hóa âm thanh.
- B.** Tối ưu hóa việc sử dụng các cổng 80 và 443.
- C.** Mã hóa lưu lượng HTTP.
- D.** Cung cấp các biện pháp bảo vệ mật mã cho các email.
- 6.** Mục đích của Giao thức Truy cập Danh bạ Hạng nhẹ (LDAPS) là gì?
- A.** Tận dụng các biện pháp bảo vệ mã hóa SSH để bảo mật truyền tải FTP.
- B.** Sử dụng một đường hầm SSL/TLS để kết nối các dịch vụ LDAP.
- C.** Ký kỹ thuật số các bản ghi DNS.
- D.** Cung cấp cả mã hóa đối xứng và bất đối xứng.
- 7.** FTPS sử dụng cổng nào?
- A.** 53
- B.** 83
- C.** 990
- D.** 991.
- 8.** Bạn là quản trị viên bảo mật cho công ty XYZ. Bạn nghi ngờ rằng các email của công ty sử dụng các giao thức và cổng email POP và IMAP mặc định đang bị chặn khi đang chuyển tiếp. Bạn nên cân nhắc sử dụng cổng nào sau đây?
- A.** Các cổng 995 và 993

- B.** Các cổng 53 và 22
  - C.** Các cổng 110 và 143
  - D.** Các cổng 161 và 16240.
- 9.** Mục đích của Giao thức Quản lý Mạng Đơn giản phiên bản 3 (SNMPv3) là gì?
- A.** Cung cấp các giá trị mã hóa bất đối xứng.
  - B.** Đạt được các mục tiêu giao tiếp cụ thể.
  - C.** Cung cấp một ngôn ngữ chung cho các nhà phát triển.
  - D.** Được sử dụng để quản lý một cách bảo mật các thiết bị trên mạng dựa-trên-IP.
- 10.** Mục đích của HTTPS là gì?
- A.** Để cho phép liệt kê và giám sát các tài nguyên mạng
  - B.** Sử dụng SSL hoặc TLS để mã hóa kênh mà lưu lượng HTTP được truyền qua đó
  - C.** Để triển khai Đăng nhập một lần
  - D.** Để tăng cường các giao thức truyền thông.

## Đáp án

1. **B.** Hệ thống Tên Miền (DNS) sử dụng cổng TCP và UDP 53 cho các truy vấn và phản hồi tiêu chuẩn. Cổng này sẽ được mở trên tường lửa trong trường hợp này. Secure Shell (SSH) sử dụng cổng TCP 22 làm cổng mặc định của nó. Tất cả các phiên bản SNMP đều yêu cầu cổng 161 và 162 phải mở trên tường lửa.
2. **A.** Một điểm yếu chính của giao thức DNS là các yêu cầu và phản hồi được gửi ở dạng bản rõ ràng.
3. **C.** Một lợi ích chính của DNSSEC là nó cho phép xác thực nguồn gốc, từ chối xác thực sự tồn tại và tính toàn vẹn của dữ liệu.
4. **A.** Giao thức SSH là một chương trình kết nối đầu cuối từ xa được mã hóa được sử dụng cho các kết nối từ xa tới máy chủ.
5. **D.** Mục đích của giao thức S/MIME là cung cấp các biện pháp bảo vệ mật mã cho email và tập tin đính kèm.
6. **B.** LDAPS sử dụng đường hầm SSL/TLS để kết nối các dịch vụ LDAP.
7. **C.** FTPS sử dụng cổng 990.
8. **A.** Cổng POP3 và IMAP4 mặc định lần lượt là 110 và 143. Những cổng này không bảo mật. Với tư cách là quản trị viên bảo mật, bạn nên cân nhắc sử dụng POP bảo mật bằng cổng 995 và IMAP bảo mật bằng cổng 993.
9. **D.** Mục đích của SNMPv3 là quản lý một cách bảo mật các thiết bị trên mạng dựa-trên-IP.
10. **B.** HTTPS sử dụng SSL hoặc TLS để mã hóa kênh mà lưu lượng HTTP được truyền qua đó.

## Chương 18    Bảo mật Máy vật chủ và Ứng dụng

---

### Bảo mật Máy vật chủ và Ứng dụng

Trong chương này bạn sẽ

- Xem xét cách thức triển khai các giải pháp bảo mật dựa-trên-máy-vật-chủ,
  - Khám phá các giải pháp bảo mật ứng dụng.
- 

Điện toán liên quan đến việc xử lý dữ liệu bằng các máy móc và ứng dụng. Việc đảm bảo rằng cả máy móc và những ứng dụng chạy trên chúng càng an toàn càng tốt là một phần quan trọng của một chương trình bảo mật doanh nghiệp. Chương này khám phá các bước được sử dụng để bảo mật cả phần cứng và các ứng dụng chạy trên nó nhằm quản lý rủi ro hệ thống tổng thể.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 3.2 của kỳ thi CompTIA Security+: Đưa ra một kịch bản, triển khai các giải pháp bảo mật máy vật chủ hoặc ứng dụng.

## Bảo vệ Điểm đầu cuối

*Bảo vệ điểm đầu cuối* là khái niệm mở rộng phạm vi bảo mật đến các thiết bị đang kết nối với mạng. Có thể sử dụng nhiều giải pháp bảo vệ điểm đầu cuối, bao gồm các giải pháp chống vi-rút/chống phần mềm độc hại, giải pháp phát hiện và ứng phó tại điểm đầu cuối, giải pháp ngăn chặn mất dữ liệu và tường lửa. Các giải pháp phát hiện và ngăn chặn xâm nhập dựa-trên-máy-vật-chủ cũng có thể được triển khai tại các điểm đầu cuối. Không phải tất cả các điểm đầu cuối đều giống nhau về khả năng hoặc rủi ro từ cuộc tấn công và các giải pháp điểm đầu cuối nên được điều chỉnh để tính đến các yếu tố đó.

### Chống Vi-rút

Các sản phẩm *chống vi-rút (AV)* cố gắng xác định, vô hiệu hóa hoặc loại bỏ các chương trình, macro và tập tin độc hại. Những sản phẩm này ban đầu được thiết kế để phát hiện và loại bỏ vi-rút máy tính, mặc dù rất nhiều sản phẩm chống vi-rút hiện đã được đóng gói với các sản phẩm và tính năng bảo mật bổ sung. Hầu hết các gói phần mềm chống vi-rút hiện tại đều cung cấp khả năng bảo vệ chống lại một loạt các mối đe dọa, bao gồm vi-rút, sâu, Trojan và các phần mềm độc hại khác. Việc sử dụng gói chống vi-rút cập-nhật là điều cần thiết trong môi trường có nhiều mối đe dọa hiện nay.

Mặc dù các sản phẩm chống vi-rút đã có hơn hai thập kỷ để cải tiến năng lực của chúng nhưng mục đích của các sản phẩm chống vi-rút vẫn như cũ: phát hiện và loại bỏ vi-rút máy tính và các phần mềm độc hại. Hầu hết các sản phẩm chống vi-rút đều kết hợp các phương pháp sau khi quét vi-rút:

- **Quét dựa-trên-chữ-ký** Giống như một hệ thống phát hiện xâm nhập (IDS), các sản phẩm chống vi-rút cũng quét các chương trình, tập tin, macro, e-mail và dữ liệu khác để phát hiện sâu, vi-rút và

phần mềm độc hại đã biết. Sản phẩm chống vi-rút có chứa một từ điển vi-rút với hàng nghìn ký hiệu vi-rút đã biết phải được cập nhật thường xuyên, vì vi-rút mới được phát hiện hàng ngày. Cách tiếp cận này sẽ bắt được các loại vi-rút đã biết nhưng bị giới hạn bởi từ điển vi-rút - những gì nó không biết thì sẽ không thể bắt được.

- **Quét theo phương pháp heuristic** (hoặc **phân tích**) Tính năng quét theo phương pháp heuristic không dựa vào từ điển virus. Thay vào đó, nó tìm kiếm hành vi đáng ngờ — bất kỳ hành vi nào không phù hợp với hình mẫu hành vi “bình thường” đối với hệ điều hành (OS) và các ứng dụng đang chạy trên hệ thống đang được bảo vệ.

Vì quét dựa-trên-chữ-ký là một khái niệm quen thuộc, chúng ta hãy xem xét quá trình quét theo phương pháp heuristic một cách chi tiết hơn. Tính năng quét theo phương pháp heuristic thường tìm kiếm các câu lệnh hoặc hướng dẫn thường không được tìm thấy trong các chương trình ứng dụng, chẳng hạn như những nỗ lực truy cập vào thanh ghi bộ nhớ dành riêng. Hầu hết các sản phẩm chống vi-rút sử dụng hệ thống dựa-trên-trọng-số hoặc hệ thống dựa-trên-quy-tắc trong quá trình quét theo phương pháp heuristic của chúng (các sản phẩm hiệu quả hơn sử dụng kết hợp cả hai kỹ thuật). Một *hệ thống dựa-trên-trọng-số* đánh giá mọi hành vi đáng ngờ dựa trên mức độ của mỗi đe dọa liên quan đến hành vi đó. Nếu ngưỡng đã đặt bị vượt qua dựa trên một hành vi đơn lẻ hoặc kết hợp các hành vi, sản phẩm chống vi-rút sẽ coi tiến trình, ứng dụng, macro, v.v... đang thực hiện (các) hành vi như một mối đe dọa đối với hệ thống. *Hệ thống dựa-trên-quy-tắc* so sánh hoạt động với một tập hợp các quy tắc có ý nghĩa nhằm phát hiện và xác định phần mềm độc hại. Nếu một phần của phần mềm khớp với một quy tắc hoặc nếu một tiến trình, ứng dụng, macro, v.v... thực hiện một hành vi khớp với quy tắc, phần mềm chống vi-rút sẽ coi đó là một mối đe dọa đối với hệ thống cục bộ.

Một số sản phẩm heuristic rất tiên tiến và có các khả năng kiểm tra việc sử dụng và đánh giá chỉ bộ nhớ, một trình phân tích cú pháp để kiểm tra mã thực thi, trình phân tích luồng logic và trình tháo gỡ/giả lập để chúng có thể "đoán" mã được thiết kế để làm gì và nó có độc hại hay không.



**MÁCH NƯỚC CHO KỲ THI** Quét theo phương pháp heuristic là một phương pháp phát hiện hành vi độc hại tiềm ẩn hoặc có khả năng "giống-vi-rút" bằng cách kiểm tra những gì một chương trình hoặc một phần của mã thực hiện. Bất kỳ thứ gì "đáng ngờ" hoặc có khả năng là "độc hại" đều được kiểm tra chặt chẽ để xác định xem nó có phải là mối đe dọa đối với hệ thống hay không. Sử dụng tính năng quét theo phương pháp heuristic, một sản phẩm chống vi-rút cố gắng xác định các vi-rút mới hoặc các phiên bản đã sửa đổi đáng kể của vi-rút hiện có trước khi chúng có thể làm hỏng hệ thống của bạn.

Cũng giống như các sản phẩm IDS/IPS, mã hóa và xáo trộn gây ra một vấn đề đối với các sản phẩm chống vi-rút: bất kỳ thứ gì không đọc được đều không thể được khớp với các từ điển hoặc mô hình hoạt động của vi-rút hiện tại. Để chống lại việc sử dụng mã hóa trong phần mềm độc hại và vi-rút, nhiều máy quét heuristic tìm kiếm các vòng lặp mã hóa và giải mã. Vì phần mềm độc hại thường được thiết kế để chạy một mình và không bị giám sát, nếu nó sử dụng mã hóa, nó phải chứa tất cả các hướng dẫn để mã hóa và giải mã chính nó, khi cần. Máy quét heuristic tìm kiếm các hướng dẫn như khởi tạo con trỏ với địa chỉ bộ nhớ hợp lệ, thao tác với bộ đếm hoặc điều kiện rẽ nhánh dựa trên giá trị bộ đếm. Mặc dù những hành động này không phải lúc nào cũng chỉ ra sự hiện diện của vòng lặp mã hóa/giải mã, nhưng nếu công cụ heuristic có thể tìm thấy vòng lặp, nó có thể giải mã phần mềm trong không gian bộ nhớ được bảo

vệ, chẳng hạn như trình giả lập và đánh giá phần mềm chi tiết hơn. Nhiều loại vi-rút chia sẻ các quy trình mã hóa/giải mã chung có thể giúp các nhà phát triển chống vi-rút.

Các sản phẩm chống vi-rút hiện tại có cấu hình cao và hầu hết các sản phẩm đều sẽ có các khả năng sau:

- **Cập nhật tự động** Có lẽ tính năng quan trọng nhất của một giải pháp chống vi-rút tốt là khả năng tự cập nhật chính nó bằng cách tự động tải xuống các chữ ký vi-rút mới nhất một cách thường xuyên. Điều này thường yêu cầu hệ thống phải được kết nối với Internet theo một cách nào đó và các cập nhật phải được thực hiện hàng ngày (hoặc thường xuyên hơn).
- **Quét tự động** Hầu hết các sản phẩm chống vi-rút đều cho phép lập lịch quét tự động để bạn có thể chỉ định khi nào sản phẩm chống vi-rút sẽ kiểm tra hệ thống cục bộ để tìm kiếm các tập tin đã bị nhiễm. Các quá trình quét tự động này thường có thể được lập lịch cho những ngày và giờ cụ thể và các thông số quét có thể được định cấu hình để chỉ định những ổ đĩa, thư mục và loại tập tin nào sẽ được quét.
- **Quét phương tiện** Phương tiện có thể di động vẫn là một phương pháp phổ biến để lây lan vi-rút và phần mềm độc hại và hầu hết các sản phẩm chống vi-rút đều có thể được định cấu hình để tự động quét phương tiện quang, ổ USB, thẻ nhớ hoặc bất kỳ loại phương tiện di động nào khác ngay khi chúng được kết nối với hoặc được truy cập bởi hệ thống cục bộ.
- **Quét thủ công** Nhiều sản phẩm chống vi-rút cho phép người dùng quét ổ đĩa, tập tin hoặc thư mục (thư mục) "theo yêu cầu".
- **Quét thư điện tử** Thư điện tử vẫn là một phương thức lây lan chính của vi-rút và phần mềm độc hại. Nhiều sản phẩm chống vi-rút cung

cấp cho người dùng khả năng quét cả thư đến và thư đi cũng như bất kỳ tập tin đính kèm nào.

- **Giải pháp** Khi sản phẩm chống vi-rút phát hiện ra một tập tin hoặc ứng dụng đã bị nhiễm, nó thường có thể thực hiện một trong một số vài hành động. Sản phẩm chống vi-rút có thể cô lập tập tin, khiến cho tập tin trở nên không thể truy cập được. Nó có thể cố gắng sửa chữa tập tin bằng cách xóa đoạn mã lây nhiễm hoặc vi phạm hoặc có thể xóa tập tin bị nhiễm. Hầu hết các sản phẩm chống vi-rút cho phép người dùng chỉ định hành động mong muốn và một số cho phép hành động leo thang, chẳng hạn như làm sạch tập tin bị nhiễm trước nếu có thể và tiếp tục cách ly tập tin nếu không thể làm sạch.

Các giải pháp chống vi-rút thường được cài đặt trên các hệ thống riêng lẻ (máy tính để bàn, máy chủ và thậm chí cả thiết bị di động), nhưng khả năng chống vi-rút dựa-trên-mạng cũng có sẵn trong nhiều sản phẩm cửa ngõ (gateway) thương mại. Các sản phẩm cửa ngõ này thường kết hợp tường lửa, IDS/IPS và khả năng chống vi-rút vào một nền tảng được tích hợp duy nhất. Hầu hết các tổ chức cũng sẽ sử dụng các giải pháp chống vi-rút trên máy chủ email, vì đây vẫn tiếp tục là một phương pháp lây lan rất phổ biến của vi-rút.



**LƯU Ý** Ý định của những kẻ viết vi-rút máy tính đã thay đổi qua nhiều năm - từ việc chỉ đơn giản là muốn phát tán vi-rút để gây được sự chú ý, sang việc tạo ra các mạng botnet lén lút như một hoạt động tội phạm. Một phương pháp ẩn vẫn còn tồn tại là tạo ra các loại vi-rút có thể biến đổi để giảm tỷ lệ phát hiện của chúng bằng các chương trình chống vi-rút tiêu chuẩn. Số lượng các biến thể của một số loại virus đã tăng từ ít hơn 10 đến hơn 10.000. Sự bùng nổ về chữ ký này đã gây ra

hai vấn đề: Một, người dùng phải liên tục (đôi khi nhiều hơn hàng ngày) cập nhật tập tin chữ ký của họ. Hai và quan trọng hơn, các phương pháp phát hiện sẽ phải thay đổi khi số lượng chữ ký trở nên quá lớn để có thể quét nhanh. Đối với người dùng cuối, điểm mấu chốt rất đơn giản: cập nhật chữ ký một cách tự động và ít nhất hàng ngày.

Mặc dù việc cài đặt một sản phẩm chống vi-rút tốt vẫn được coi là thực tiễn tốt nhất cần thiết, nhưng ngày càng có nhiều mối lo ngại về hiệu quả của các sản phẩm chống vi-rút trong việc chống lại các mối đe dọa vẫn đang không ngừng phát triển. Các vi-rút ban đầu thường trưng ra các hành vi phá hoại, chúng là những tập tin được viết và sửa đổi kém và ít quan tâm đến việc che giấu sự hiện diện của chúng hơn là với việc lan truyền. Chúng ta đang chứng kiến sự xuất hiện của vi-rút và phần mềm độc hại được tạo ra bởi các chuyên gia, đôi khi được tài trợ bởi các tổ chức tội phạm hoặc chính phủ, nhằm che giấu sự hiện diện của chúng. Những vi-rút và phần mềm độc hại này thường được sử dụng để đánh cắp thông tin nhạy cảm hoặc biến máy tính bị nhiễm thành một phần của mạng botnet lớn hơn để sử dụng trong các hoạt động gửi thư rác hoặc hoạt động tấn công.



## MÁCH NƯỚC CHO KỲ THI

Chống vi-rút là một ứng dụng bảo mật thiết yếu trên mọi nền tảng. Có rất nhiều chương trình tuân thủ bắt buộc triển khai việc chống vi-rút, bao gồm Tiêu chuẩn Bảo mật Dữ liệu Ngành Thẻ Thanh toán (PCI DSS) và Bảo vệ Cơ sở hạ tầng Tối quan trọng của Hội đồng Độ tin cậy Điện Bắc Mỹ (North American Electric Reliability Council Critical Infrastructure Protections - NERC CIP)

## Chống Mã độc

Trong những ngày đầu sử dụng máy tính, các mối đe dọa vẫn còn khá hạn chế: hầu hết người dùng gia đình không được kết nối Internet 24/7 thông qua các kết nối băng thông rộng và mối đe dọa phổ biến nhất là vi-rút lan truyền từ máy tính này sang máy tính khác qua một đĩa mềm đã bị nhiễm vi-rút (giống như y học định nghĩa, một vi-rút máy tính là thứ có thể lây nhiễm sang máy vật chủ và có thể tự nhân bản chính nó). Tuy nhiên, mọi thứ đã thay đổi một cách đáng kể kể từ những ngày đầu tiên đó, và các mối đe dọa hiện tại đang gây ra những rủi ro lớn hơn bao giờ hết. Các đầu dò tự động từ botnet và sâu máy tính không phải là mối đe dọa duy nhất khi lang thang trên Internet - còn có cả vi-rút và phần mềm độc hại lây lan qua email, lừa đảo, các trang web bị nhiễm sẽ thực thi mã trên hệ thống của bạn khi bạn truy cập chúng, phần mềm quảng cáo, phần mềm gián điệp, v.v... Phần mềm chống lại phần-mềm-độc-hại (anti-malware) là tên gọi của một sản phẩm được thiết kế để bảo vệ máy của bạn khỏi phần mềm mã độc hoặc phần mềm độc hại. Ngày nay, hầu hết các giải pháp chống phần mềm độc hại đều được kết hợp với các giải pháp chống vi-rút thành một sản phẩm duy nhất. May mắn thay, khi các mối đe dọa ngày càng phức tạp và có khả năng, các sản phẩm được thiết kế để ngăn chặn chúng cũng vậy. Một trong những dạng phần mềm độc hại nguy hiểm nhất là ransomware, nó lây lan nhanh chóng, mã hóa các tập tin của người dùng và khóa nó cho đến khi người dùng trả tiền chuộc. Để biết thêm thông tin chi tiết về các sản phẩm chống phần mềm độc hại, hãy đọc lại phần "Chống vi-rút" trước đó và nhận ra rằng phần mềm độc hại là một mối đe dọa khác với vi-rút, nhưng biện pháp phòng vệ thì giống nhau.

## Nhận diện và Ứng phó tại Điểm đầu cuối (EDR)

Các giải pháp *nhận diện và ứng phó tại điểm đầu cuối (EDR)* là các giải pháp được tích hợp kết hợp các chức năng bảo mật điểm cuối riêng lẻ

thành một gói hoàn chỉnh. Việc có được giải pháp đóng gói giúp cho việc cập nhật trở nên dễ dàng hơn, và thường thì các sản phẩm này được thiết kế để tích hợp vào giải pháp cấp doanh nghiệp với nền tảng quản lý tập trung. Một số thành phần EDR phổ biến bao gồm giải pháp chống vi-rút, chống phần mềm độc hại, vá lỗi phần mềm, tường lửa và DLP. Quản lý điểm cuối thống nhất (unified endpoint management - UEM) là một mô hình bảo mật mới hơn tập trung vào việc quản lý và bảo mật các thiết bị trong doanh nghiệp như máy tính để bàn, máy tính xách tay, điện thoại thông minh và các thiết bị khác từ một vị trí duy nhất. UEM được đề cập trong Chương 22.

## DLP

Các giải pháp *ngăn chặn mất mát dữ liệu* (DLP) đóng vai trò ngăn chặn dữ liệu nhạy cảm rời khỏi mạng mà không được chú ý. Còn nơi nào tốt hơn để kiểm tra ngoài các điểm đầu cuối? Vâng, điều quan trọng là phải hiểu được điểm đầu cuối là gì. Đối với email, điểm đầu cuối thực sự chính là máy chủ và điều này cung cấp một vị trí có thể mở rộng đối với nhiều hộp thư. Việc áp dụng DLP trên các thiết bị đầu cuối để theo dõi các mục như tải dữ liệu qua USB có thể là một bài tập với việc duy trì nhiều bộ quy tắc DLP, các ứng dụng máy khách nặng nề ảnh hưởng đến hiệu suất của điểm đầu cuối và thiếu sự phân biệt có thể gây ra các vấn đề về năng suất. Điều này đã dẫn đến việc giám sát DLP tại điểm đầu cuối, nơi hoạt động tập tin được báo cáo cho các hệ thống tập trung và các dịch vụ DLP chuyên biệt như DLP nội dung đang được Microsoft triển khai trên môi trường Microsoft 365. Các giải pháp điểm đầu cuối này không cung cấp mức độ bao phủ hoàn chỉnh hoặc toàn diện nhưng khi kết hợp với nhau có thể đạt được nhiều mục tiêu với chi phí và độ phức tạp ít hơn.

## Tường lửa Thẽ hệ Kế tiếp (NGFW)

*Tường lửa thẽ-hệ-kế-tiếp (NGFW)* hoạt động bằng cách kiểm tra lưu lượng truy cập thực tế đi qua tường lửa - không chỉ xem xét địa chỉ và cổng nguồn và đích mà còn xem xét nội dung thực tế đang được gửi đi. Điều này khiến cho tường lửa thẽ-hệ-kế-tiếp trở thành một công cụ đắc lực trong việc săn lùng nội dung độc hại trên đường vào và bí mật của công ty trên đường thoát ra. Như với tất cả các nền tảng dựa trên quy tắc này, điều thách thức là duy trì các bộ quy tắc phù hợp để bắt được lưu lượng xấu mong muốn.

## Hệ thống Phát hiện Xâm nhập Dựa trên Máy vật chủ (HIDS)

*Hệ thống phát hiện xâm nhập dựa-trên-máy-vật-chủ (HIDS)* hoạt động để phát hiện các phần tử không mong muốn trong lưu lượng mạng đến và đi từ máy vật chủ. Bởi vì hệ thống phát hiện xâm nhập được gắn với máy vật chủ, nó có thể rất cụ thể đối với các mối đe dọa đối với hệ điều hành máy vật chủ và bỏ qua những mối đe dọa không có tác dụng. Được triển khai tại một điểm đầu cuối cụ thể, nó có thể được điều chỉnh theo các chi tiết cụ thể của điểm đầu cuối và các ứng dụng tại điểm đầu cuối, cung cấp mức độ phát hiện cụ thể cao hơn. Nhược điểm của HIDS là nó chỉ phát hiện các vấn đề, nó phải dựa vào một thành phần khác, thường thông qua một số cơ chế ghi nhật ký hoặc báo cáo, để ứng phó với mối đe dọa. Điều này được giải quyết trong một hệ thống ngăn chặn xâm nhập dựa-trên-máy-vật-chủ, sẽ được thảo luận trong phần tiếp theo.

## Hệ thống Ngăn chặn Xâm nhập Dựa trên Máy vật chủ (HIPS)

*Hệ thống ngăn chặn xâm nhập dựa-trên-máy-vật-chủ (HIPS)* là một HIDS với các thành phần bổ sung để cho phép nó tự động ứng phó với điều kiện đe dọa. Biện pháp ứng phó có thể chỉ đơn giản như chặn một gói tin cho đến việc ngắt kết nối. HIPS có tất cả các đặc tính của HIDS nền tảng, với lợi thế bổ sung là có thể thực hiện các hành động được xác định trước để đối phó với một mối đe dọa.

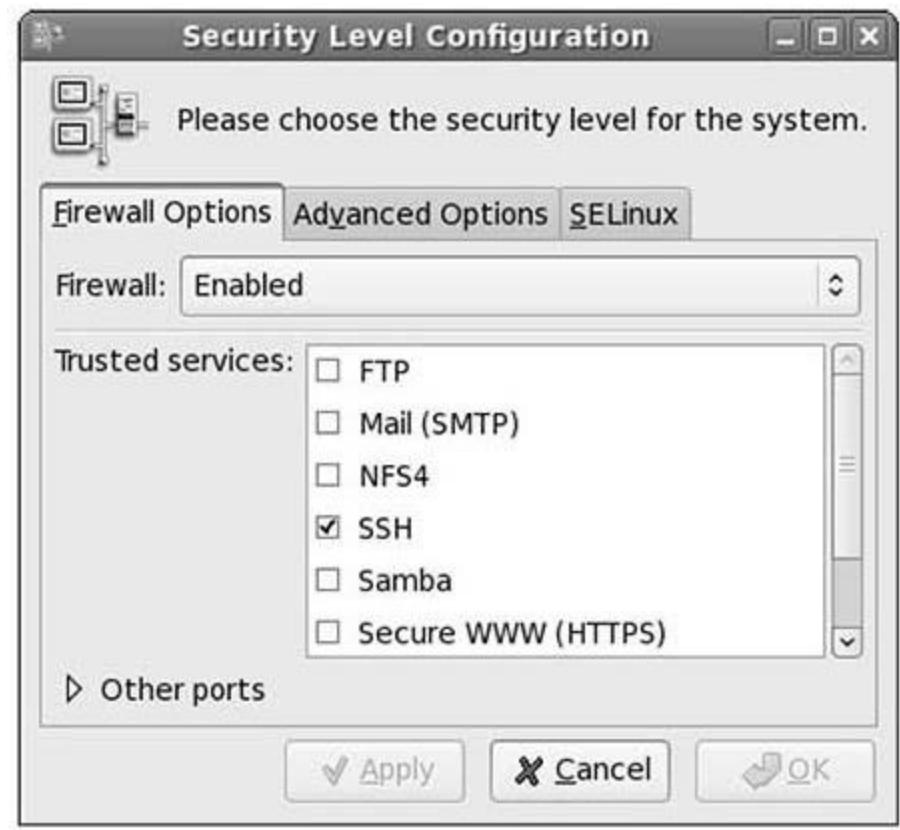


**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng HIDS chỉ có thể phát hiện ra các hoạt động độc hại và gửi cảnh báo. HIPS, nói cách khác, có thể phát hiện và ngăn chặn các cuộc tấn công.

### Tường lửa Dựa trên Máy vật chủ

Tường lửa cá nhân, hoặc *tường lửa dựa-trên-máy-vật-chủ*, là các cơ chế bảo vệ dựa trên máy vật chủ để giám sát và kiểm soát lưu lượng truy cập vào và ra khỏi một hệ thống. Được thiết kế cho người dùng cuối, tường lửa phần mềm thường có chính sách bảo mật có thể định cấu hình cho phép người dùng xác định lưu lượng nào là "tốt" và được phép vượt qua và lưu lượng nào là "xấu" và sẽ bị chặn lại. Quyết định "tốt" hay "xấu" dựa trên các địa chỉ đang được chuyển, cả địa chỉ IP lẫn kết hợp các cổng. Tường lửa phần mềm cực kỳ phổ biến - đến nỗi hầu hết các hệ điều hành hiện đại đều có một số loại tường lửa cá nhân đi kèm theo. Việc có được tường lửa trên hệ điều hành vật chủ đem đến khả năng điều chỉnh tường lửa theo kiểu sử dụng của điểm cuối cụ thể.

Hệ điều hành dựa-trên-Linux đã có tường lửa dựa-trên-phần-mềm được tích-hợp trong nhiều năm, bao gồm TCP Wrapper, ipchains và iptables. Ví dụ về tường lửa Linux được minh họa trong Hình 18-1.



**Hình 18-1** Tường lửa Linux

TCP Wrapper là một chương trình đơn giản giới hạn các kết nối mạng gửi đến dựa trên số của cổng, miền hoặc địa chỉ IP và được quản lý bằng hai tập tin văn bản được gọi là hosts.allow và hosts.deny. Nếu kết nối đến từ một địa chỉ IP đáng tin cậy và dành cho một cổng mà nó được phép kết nối, thì kết nối đó được chấp thuận.

Ipchains là một tường lửa phần mềm dựa-trên-quy-tắc và được nâng cao hơn, cho phép lọc lưu lượng, Diễn dịch Địa chỉ Mạng (NAT) và chuyển hướng. Ba “chuỗi” có thể định cấu hình được sử dụng để xử lý lưu lượng mạng: đầu vào, đầu ra và chuyển tiếp. Chuỗi đầu vào chứa các quy tắc đối với lưu lượng truy cập vào hệ thống cục bộ. Chuỗi đầu ra chứa các quy tắc dành cho lưu lượng truy cập rời khỏi hệ thống cục bộ. Chuỗi chuyển tiếp chứa các quy tắc dành cho lưu lượng đã được hệ thống cục

bộ nhận nhưng không phải dành cho hệ thống cục bộ. Iptables là sự phát triển mới nhất của ipchains. Iptables sử dụng ba chuỗi giống nhau cho các quy tắc chính sách và xử lý lưu lượng giống như ipchains, nhưng với iptables, mỗi gói tin chỉ được xử lý bởi chuỗi thích hợp. Dưới ipchains, mỗi gói đi qua cả ba chuỗi để xử lý. Với iptables, các gói đến chỉ được xử lý bởi chuỗi đầu vào và các gói rời khỏi hệ thống chỉ được xử lý bởi chuỗi đầu ra. Điều này cho phép kiểm soát chi tiết hơn lưu lượng mạng và nâng cao được hiệu suất.

Ngoài tường lửa “miễn phí” đi kèm với hệ điều hành, nhiều gói tường lửa cá nhân thương mại cũng có sẵn. Rất nhiều tường lửa phần mềm thương mại hạn chế lưu lượng đến và đi, chặn cửa sổ bật lên, phát hiện phần mềm quảng cáo, chặn cookie và các tiến trình độc hại, đồng thời quét lưu lượng tin nhắn tức thời. Mặc dù bạn vẫn có thể mua hoặc thậm chí tải xuống một tường lửa cá nhân dựa-trên-phần-mềm miễn phí, hầu hết các nhà cung cấp thương mại đều đang cung cấp chức năng tường lửa với những năng lực bổ sung như chống vi-rút và chống phần mềm gián điệp.

Microsoft Windows đã có tường lửa phần mềm cá nhân kể từ Windows XP SP2. Ngày nay, Tường lửa của Windows được gọi là Tường lửa của Bộ bảo vệ Windows (Windows Defender Firewall) (xem Hình 18-2). Nó được bật theo mặc định và đưa ra cảnh báo khi bị vô hiệu hóa. Tường lửa của Bộ bảo vệ Windows khá dễ thiết lập cấu hình, nó có thể được thiết lập để chặn tất cả lưu lượng truy cập, tạo ngoại lệ cho lưu lượng truy cập bạn muốn cho phép và ghi nhật ký lại lưu lượng truy cập bị từ chối để phân tích sau này.



**Hình 18-2** Tường lửa của Bộ bảo vệ Windows mặc định đã được bật

Trong Windows 10, Microsoft đã sửa đổi Tường lửa của Bộ bảo vệ Windows để làm cho nó có nhiều năng lực hơn và có thể thiết lập cấu hình tốt hơn. Nhiều tùy chọn hơn đã được thêm vào để cho phép kiểm soát lưu lượng mạng chi tiết hơn cũng như khả năng phát hiện khi một số thành phần nhất định không hoạt động như mong đợi. Ví dụ, nếu ứng dụng khách Microsoft Outlook của bạn đột nhiên cố gắng kết nối với máy chủ web từ xa, Tường lửa của Bộ bảo vệ Windows có thể phát hiện điều này là sai lệch so với hành vi bình thường và chặn lưu lượng truy cập không mong muốn đó.



**MÁCH NƯỚC CHO KỲ THI** Khi xem xét các giải pháp bảo mật điểm đầu cuối, bạn sẽ nhận thấy rằng một trong những điểm khác biệt chính nằm ở những gì hệ thống phát hiện được. Có các hệ thống mục-đích-đơn, chẳng hạn như chống vi-rút, chống phần-mềm-độc-hại và DLP. Các hệ thống đa mục đích như EDR, tường lửa và HIDS / HIPS có thể tìm kiếm nhiều loại mục khác nhau. Chìa khóa của tất cả điều này nằm ở việc định nghĩa các quy tắc cho từng sản phẩm.

## Toàn vẹn Khởi động

Khởi động một hệ thống là quá trình bật nguồn khởi động hệ thống và tải đúng phần mềm để chuyển hệ thống đến điều kiện hoạt động thích hợp. *Tính toàn vẹn khởi động* là đặc trưng của tải phần cứng/firmware/phần mềm dự kiến cho hệ thống tuân thủ theo trạng thái được mong đợi. Việc có một phương tiện để đảm bảo tính toàn vẹn khởi động là một phương tiện để đảm bảo rằng phần cứng, firmware và quá trình tải ban đầu của phần mềm không chịu bất kỳ sự can thiệp nào. Thuật ngữ *khởi động nền tảng được tin cậy* bao gồm phần cứng và bất kỳ phần mềm BIOS, firmware và hypervisor liên quan nào.

## Bảo mật Khởi động/Giao diện Firmware Có thể mở rộng được Hợp nhất (UEFI)

UEFI đưa ra giải pháp cho vấn đề toàn vẹn khởi động, được gọi là *Khởi động An toàn (Secure Boot)*, đây là một chế độ mà khi được kích hoạt, chỉ cho phép các trình điều khiển đã được ký và trình tải hệ điều hành được gọi lên. Khởi động an toàn yêu cầu các bước thiết lập cụ thể, nhưng sau khi đã được bật, nó sẽ ngăn chặn phần mềm độc hại đang cố gắng thay đổi quá trình khởi động. Khởi động an toàn cho phép *chứng thực* rằng các trình điều khiển và bộ tải hệ điều hành đang được sử dụng đã không bị thay đổi kể từ khi chúng được chấp thuận để sử dụng. Khởi động an toàn được hỗ trợ bởi Microsoft Windows và tất cả các phiên bản chính của Linux.

Một trong những đặc điểm chính của UEFI BIOS so với BIOS cũ là UEFI BIOS được thiết kế để hoạt động với nền tảng phần cứng để đảm bảo rằng bộ nhớ flash chứa BIOS sẽ không thể thay đổi nếu không có thông tin đăng nhập mật mã thích hợp. Việc này tạo nên Gốc Tin cậy (Root of Trust) trong nội dung của bộ nhớ flash, cụ thể là trong UEFI BIOS. Chìa khóa được sử dụng để ký BIOS do nhà sản xuất thiết bị kiểm soát, do đó ngăn chặn những thay đổi trái phép đối với BIOS. BIOS thực hiện kiểm

tra đổi với tất cả các bản cập nhật trước khi tải chúng, sử dụng khóa riêng được lưu trữ trên BIOS, đảm bảo tất cả các bản cập nhật đều đã được nhà sản xuất ký xác nhận. Các bước này tạo ra Gốc Tin cậy cho hệ thống.

Khởi động An toàn hoạt động bằng cách xác minh chữ ký số trên tất cả các bước trong quá trình khởi động. BIOS kiểm tra bộ tải và bộ tải kiểm tra các đối tượng nhân, mỗi đối tượng này là chữ ký số kiểm tra bằng các khóa do nhà sản xuất kiểm soát. Điều này đảm bảo rằng tất cả các thành phần không bị giả mạo và có tính toàn vẹn của thành phần ban đầu.

### **Khởi động được Đo lường**

*Khởi động được đo lường* cũng là một phương pháp phụ thuộc vào Gốc Tin cậy khi khởi động một hệ thống, nhưng thay vì sử dụng các chữ ký để xác minh các thành phần tiếp theo, một quá trình khởi động được đo lường sẽ băm các tiến trình tiếp theo và so sánh các giá trị băm với các giá trị tốt đã biết. Điều này có lợi thế là nó có thể được mở rộng vượt quá các hạng mục đã được bảo đảm bởi các nhà sản xuất, vì chữ ký đến từ nhà sản xuất và do đó chỉ giới hạn ở các hạng mục cụ thể. Các giá trị băm tốt đã biết phải được lưu trữ ở một vị trí an toàn và các đăng ký cấu hình nền tảng (PCR) Mô-đun Nền tảng đáng Tin cậy (TPM) bao gồm vị trí an toàn được sử dụng.

### **Chứng thực Khởi động**

Một trong những thách thức trong việc bảo mật một hệ điều hành là vô số trình điều khiển và các tiện-ích-bổ-sung (add-on) khác kết nối với hệ điều hành và cung cấp chức năng bổ sung cụ thể. Nếu các chương trình bổ sung này không được kiểm tra một cách đúng đắn trước khi cài đặt thì đường dẫn này có thể cung cấp một phương tiện mà phần mềm độc hại có thể tấn công vào máy tính. Và bởi vì các cuộc tấn công này có thể xảy ra tại thời điểm khởi động, ở cấp độ thấp hơn các ứng dụng bảo mật

như phần mềm chống vi-rút, chúng có thể sẽ rất khó để bị phát hiện và đánh bại.

*Chứng thực khởi động* là báo cáo về trạng thái của hệ thống đối với các thành phần và mối quan hệ của chúng với Gốc Tin cậy. Một phần của đặc tả UEFI/Gốc Tin cậy là phương tiện báo cáo thông qua chữ ký số về tính toàn vẹn đã được xác minh của các thành phần hệ thống. Máy chủ có thể sử dụng thông tin này từ xa để xác định xem hệ điều hành có đúng hay không và có mức độ bản vá chính xác trước khi cho phép sử dụng VPN của công ty, cũng như cho các hoạt động kết nối mạng khác.



## MÁCH NƯỚC CHO KỲ THI

*Chứng thực* có nghĩa là xác nhận tính xác thực của một nền tảng hoặc thiết bị dựa trên một hồ sơ về bằng chứng đáng được tin cậy. Bảo mật Khởi động, ví dụ, đảm bảo hệ thống đang khởi động đúng một cấu hình đáng tin cậy bằng cách có các bằng chứng về tính xác thực của từng bước đã được xác minh.

## Cơ sở dữ liệu

Các công cụ *cơ sở dữ liệu* lớn có khả năng mã hóa được tích-hợp. Ưu điểm của các lược đồ mã hóa này là chúng có thể được điều chỉnh để phù hợp với cấu trúc dữ liệu, bảo vệ các cột thiết yếu trong khi không gây ảnh hưởng đến các cột không nhạy cảm. Việc sử dụng mã hóa cơ sở dữ liệu một cách đúng đắn đòi hỏi lược đồ dữ liệu và các yêu cầu bảo mật của nó phải được thiết kế trong việc triển khai cơ sở dữ liệu. Ưu điểm là ở khả năng bảo vệ tốt hơn chống lại bất kỳ sự xâm phạm cơ sở dữ liệu nào và hiệu suất thường không đáng kể so với các lựa chọn thay thế khác.

## **Tokenization**

*Tokenization* là quá trình thay thế một giá trị đại diện, được gọi là mã thông báo, cho một phần tử dữ liệu nhạy cảm. Điều này cho phép xử lý dữ liệu, bao gồm tính toàn vẹn mang tính tham chiếu mà không làm tiết lộ giá trị nhạy cảm. Khái niệm tokenization được sử dụng rộng rãi trong các ngành như tài chính và chăm sóc sức khỏe để giúp giảm thiểu nguy cơ tiết lộ các phần tử dữ liệu nhạy cảm trong khi dữ liệu được sử dụng và để giảm thiểu nguy cơ dữ liệu nhạy cảm bị lộ qua các hệ thống không cần đến nó. Hãy nghĩ đến việc một ngân hàng kiểm tra hồ sơ tín dụng của mọi người và có được các yếu tố như số An sinh Xã hội của mọi người. Giá trị dữ liệu này, mặc dù nhạy cảm, là điều thiết yếu để có được thông tin tín dụng chính xác từ các văn phòng tín dụng, nhưng nó cũng không có nhiều ý nghĩa đối với nhân viên cho vay. Việc sử dụng giá trị thực để liên kết với văn phòng tín dụng nhưng sử dụng mã thông báo để đại diện cho nó trong các báo cáo tiếp theo sẽ bảo vệ giá trị khi không cần thiết.

## **“Trộn muối” (Salting)**

*Trộn muối* là quá trình bổ sung thêm một phần tử ngẫu nhiên vào một giá trị trước khi thực hiện một phép toán như băm. Việc này được thực hiện để bổ sung thêm tính ngẫu nhiên và cũng để ngăn ngừa việc các giá trị ban đầu giống hệt nhau được băm thành một hàm băm giống hệt nhau, điều này sẽ chỉ ra rằng hai người dùng có cùng giá trị [băm]. Băm được sử dụng để bảo vệ mật khẩu khi được lưu trữ. Việc trộn muối các hàm băm bảo vệ các đầu vào giống hệt nhau khỏi việc tạo ra các đầu ra giống hệt nhau và do đó tiết lộ rằng hai người dùng có mật khẩu giống hệt nhau.

## **Băm**

*Băm* là một phương pháp toán học để giảm một phần tử dữ liệu thành một dạng ngắn không thể đảo ngược về dạng ban đầu. Việc băm những dữ liệu nhạy cảm có tác động đến việc tạo ra một mã thông báo, và các

băm có thể được sử dụng như các mã thông báo trong các cấu trúc dữ liệu.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy nhận biết sự khác biệt giữa tokenization, trộn muối và băm. *Tokenization* là quá trình thay thế một giá trị thay thế, được gọi là mã thông báo, cho một phần tử dữ liệu nhạy cảm. *Trộn muối* là quá trình thêm một phần tử ngẫu nhiên vào một giá trị trước khi thực hiện một phép toán như băm. *Băm* là một phương pháp toán học để giảm một phần tử dữ liệu thành một dạng ngắn không thể đảo ngược trở về dạng ban đầu.

### **Bảo mật Ứng dụng**

Các ứng dụng là lý do của các thiết bị máy tính, nó là các ứng dụng để thực hiện công việc. Bởi vì các nhà sản xuất hệ điều hành và phần mềm cơ sở hạ tầng đã giải quyết các vấn đề với số lượng lớn các lỗ hổng trong quá khứ, mục tiêu hàng đầu của những kẻ tấn công ngày nay là các ứng dụng. Các ứng dụng có hai loại: phần mềm thương mại và phần mềm được xây dựng trong nội bộ. Các ứng dụng nội bộ ít có khả năng được đánh giá bảo mật nghiêm túc như một phần trong quá trình xây dựng của chúng và có nhiều khả năng có lỗ hổng bảo mật hơn. Chi tiết về việc phát triển ứng dụng an toàn được đề cập chi tiết trong Chương 11.

### **Xác thực Đầu vào**

Cách thức để một kẻ tấn công truy cập vào một ứng dụng là thông qua các đầu vào của nó. Việc xác nhận toàn diện và nghiêm ngặt các đầu vào trước khi xử lý chúng là điều thiết yếu để lọc ra các cuộc tấn công cụ thể. Nếu đầu vào sẽ được đưa vào tra cứu SQL thì việc đảm bảo đầu vào sạch không chứa các mã SQL không mong muốn là điều cần thiết. *Xác thực đầu vào* rất dễ giải thích: kiểm tra mọi thứ trước khi sử dụng. Nhưng

trong thực tế, đây là một công việc chi tiết và tiêu-tốn-nhiều-thời-gian thường bị bỏ qua hoặc các góc bị cắt [*hàm ý rằng có thể công việc cũng vẫn được thực hiện nhưng không đầy đủ*].

---



**MÁCH NƯỚC CHO KỲ THI** Xác thực đầu vào đúng cách ngăn chặn được rất nhiều kiểu tấn công khác nhau bằng cách đảm bảo rằng đầu vào đã được tính toán một cách đúng đắn.

### Bảo mật Cookies

Cookie là các tập tin văn bản được gửi theo mọi yêu cầu đến một trang web. Chúng đã được sử dụng cho rất nhiều chức năng, bao gồm duy trì trạng thái, tùy chọn, thông số sử dụng, v.v... Một thuộc tính trong cookie được gọi là *thuộc tính bảo mật*, khi được đặt, sẽ hướng dẫn cho trình duyệt và máy chủ chỉ vận chuyển cookie qua các kênh HTTPS. Vì cookie được truyền dưới dạng văn bản rõ ràng trên Web nên nếu chúng nằm ngoài kênh HTTPS được bảo vệ, chúng có thể được đọc bởi các bên trái phép. Việc đặt thuộc tính bảo mật sẽ ngăn trình duyệt gửi cookie cụ thể đó qua kết nối không-bảo-mật. Điều này không kết thúc tất cả rủi ro bởi vì nếu kẻ tấn công giả mạo cookie được lưu trữ trên máy điểm đầu cuối, thuộc tính có thể được thay đổi trở lại để cho phép cookie được gửi qua một kết nối không-bảo-mật.

### Tiêu đề Giao thức Truyền tải Siêu văn bản (HTTP)

Trình duyệt là cửa sổ cho rất nhiều ứng dụng, hoạt động như một phương tiện cung cấp thông tin đầu vào của người dùng và nhận phản hồi của hệ thống. HTTP có một số lượng lớn các tùy chọn và tính năng có thể được thao túng thông qua trình duyệt để cải thiện khả năng sử dụng của một trang web, nhưng trong một số trường hợp thao túng, chúng có thể dẫn đến những rủi ro về bảo mật. Trang web có thể cố gắng thực hiện một

số biện pháp kiểm soát đối với các hành vi của trình duyệt thông qua các tiêu đề phản hồi truyền tải các chỉ thị đến trình duyệt. Việc sử dụng một tập hợp các tiêu đề phản hồi liên quan đến bảo mật có thể làm giảm bớt các rủi ro như tấn công hạ cấp giao thức, tấn công bằng nhấp chuột, chiếm quyền điều khiển cookie và các cuộc tấn công khác. Một ví dụ là chỉ thị Bảo mật Truyền tải Nghiêm ngặt HTTP (HTTP Strict Transport Security - HSTS):

```
Strict-Transport-Security: max-age 3600; includeSubDomains
```

Lệnh này tuyên bố rằng các trình duyệt chỉ được tương tác qua HTTPS, không bao giờ là HTTP, với thời gian tối đa là 3600 giây và tất cả các miền con đều được bao gồm trong lệnh này. Có rất nhiều tiêu đề phản hồi bổ sung được sử dụng trong HTTP và nơi tốt nhất để tìm hiểu chi tiết, mặc dù chúng nằm ngoài phạm vi của kỳ thi Security+, là trên trang web của dự án OWASP.

## Ký Mã nguồn

Một yếu tố quan trọng trong việc đảm bảo rằng phần mềm là chính hãng và đã không bị thay đổi là phương pháp kiểm tra tính toàn vẹn của phần mềm. Theo quan điểm cứng-cő-đường-cơ-sở, làm thế nào để bạn có thể chắc chắn rằng mã phần mềm bạn đang sử dụng là chính hãng và không bị giả mạo? Câu trả lời là một quá trình được gọi là *ký mã phần mềm* (*code signing*), bao gồm việc áp dụng chữ ký điện tử vào mã, cung cấp một cơ chế mà người dùng đầu cuối có thể xác minh tính toàn vẹn của mã. Ngoài việc xác minh tính toàn vẹn của mã, chữ ký điện tử cung cấp bằng chứng về nguồn gốc của phần mềm.

Mã được ký bởi nhà sản xuất, nhà cung cấp thương mại hoặc nhóm nội-bộ. Chữ ký điện tử này chứa hàm băm của mã, cho phép xác minh tính toàn vẹn của nó vào bất cứ lúc nào. Nếu hàm băm của mã và mã trên hồ

sơ trùng khớp và các chữ ký hợp lệ, thì mã đó là đáng tin cậy đối với dòng dõi của nó.

---



**MÁCH NƯỚC CHO KỲ THI** Ký mã phần mềm đảm bảo rằng mã phần mềm đã không bị thay đổi kể từ khi được ký.

### Danh sách Chấp thuận (Allow List)

Các ứng dụng có thể được kiểm soát tại hệ điều hành tại thời điểm bắt đầu thông qua các danh sách khôi hoặc danh sách chấp phép. *Danh sách chấp thuận* là danh sách các ứng dụng được phép chạy trên Hệ điều hành. Việc chấp thuận danh sách dễ sử dụng hơn từ khía cạnh xác định các ứng dụng được phép chạy - các giá trị băm có thể được sử dụng để đảm bảo rằng các tập tin thực thi không bị hư hỏng. Thách thức trong việc chấp thuận danh sách là số lượng ứng dụng tiềm năng được chạy trên một máy thông thường. Đối với một máy đơn-mục-đích (single-purpose), chẳng hạn như một máy chủ cơ sở dữ liệu, danh sách chấp thuận có thể tương đối dễ sử dụng. Đối với máy đa-mục-đích, nó có thể phức tạp hơn.

### Danh sách bị Khóa (Block List)/Danh sách bị Từ chối (Deny List)

*Danh sách bị khóa/danh sách bị từ chối* về thực chất là một danh sách lưu ý về những ứng dụng không được phép chạy trên máy. Về cơ bản, đây là loại khả năng “bỏ qua” hoặc “khóa cuộc gọi” vĩnh viễn. Việc chặn theo kiểu này rất khó sử dụng để chống lại các mối đe dọa động (dynamic), vì việc xác định một ứng dụng cụ thể có thể dễ dàng tránh được bằng cách thông qua những thay đổi nhỏ.

---



**MÁCH NƯỚC CHO KỲ THI** Một *danh sách chấp thuận* là một danh sách các ứng dụng đã được phê duyệt. Một *danh sách bị khóa/danh sách*

bị từ chối là một danh sách các ứng dụng không nên được phép chạy trên máy.

### **Thực tiễn Lập trình Bảo mật**

Bảo mật ứng dụng bắt đầu bằng mã an toàn và không có lỗ hổng bảo mật. Thật không may, tất cả mã phần mềm đều có điểm yếu và lỗ hổng bảo mật, vì vậy việc khởi tạo mã theo cách có khả năng bảo vệ hiệu quả để ngăn chặn việc khai thác các lỗ hổng có thể duy trì mức độ bảo mật mong muốn. Tạo ra phần mềm là một loại quy trình sản xuất cần được định hướng và quản lý bởi các chính sách và thủ tục. Việc khởi tạo các bước cần thiết để đảm bảo mã bảo mật đang được tạo ra đòi hỏi sự tuân thủ một tập hợp các phương pháp mã hóa an toàn, bao gồm việc xử lý thích hợp các cấu hình, các lỗi và ngoại lệ và các đầu vào, để có thể hỗ trợ cho việc tạo ra ứng dụng an toàn. Việc kiểm tra ứng dụng trong suốt vòng đời phát triển phần mềm có thể xác định hồ sơ rủi ro bảo mật thực tế của một hệ thống.

Có nhiều yếu tố riêng lẻ trong một phương pháp luận vòng đời phát triển phần mềm (SDLM) để có thể hỗ trợ một nhóm trong việc phát triển mã an toàn. Các quy trình SDLM chính xác, chẳng hạn như xác thực đầu vào, xử lý lỗi và ngoại lệ thích hợp, cũng như giảm thiểu việc giả mạo yêu cầu chéo-trang và tập lệnh chéo-trang, có thể cải thiện tính bảo mật của mã. Các yếu tố của quy trình như kiểm tra bảo mật, quản lý mờ và quản lý vá lỗi cũng giúp đảm bảo các ứng dụng đáp ứng được cấu hình rủi ro mong muốn.

Hai danh sách chính về các lỗi phần mềm phổ biến là danh sách 25 lỗi Hàng đầu do MITRE duy trì và danh sách 10 Lỗi phần mềm Hàng đầu của OWASP dành cho các ứng dụng web. Tùy thuộc vào loại ứng dụng đang được đánh giá, những danh sách này cung cấp một điểm khởi đầu vững chắc để phân tích bảo mật về các loại lỗi đã biết. MITRE là kho lưu trữ

danh sách tiêu chuẩn ngành dành cho các chương trình tiêu chuẩn và danh sách OWASP dành cho các ứng dụng web. Bởi vì nguyên nhân của các lỗi thông thường không thay đổi một cách nhanh chóng nên các danh sách này không được cập nhật hàng năm.

## **Phân tích Mã Tĩnh**

*Phân tích mã tĩnh* là khi mã được kiểm tra mà không cần phải được thực thi. Quá trình phân tích này có thể được thực hiện trên cả cơ sở mã nguồn và mã đối tượng. Thuật ngữ *mã nguồn* thường được sử dụng để chỉ định mã ngôn ngữ cấp-cao, mặc dù về mặt kỹ thuật, mã nguồn là cơ sở mã gốc dưới mọi hình thức, từ ngôn ngữ cấp-cao đến mã máy. Phân tích tĩnh có thể được thực hiện bởi con người hoặc bằng công cụ, mặc dù con người bị giới hạn ở ngôn ngữ cấp-cao, trong khi các công cụ có thể được sử dụng để đổi đầu hầu như bất kỳ hình thức cơ sở mã nào.

Phân tích mã tĩnh thường được thực hiện bằng các công cụ được tự động hóa. Các công cụ này được đặt nhiều tên gọi khác nhau nhưng thường được gọi là bộ phân tích mã tĩnh hoặc bộ phân tích mã nguồn. Đôi khi, các cụm từ bổ sung, chẳng hạn như “máy quét nhị phân” và “máy quét mã byte”, được sử dụng để phân biệt các công cụ. Các công cụ tĩnh sử dụng nhiều cơ chế khác nhau để tìm kiếm các điểm yếu và các lỗ hổng. Các công cụ tự động có thể đem lại lợi thế khi kiểm tra cú pháp, sử dụng các lệnh gọi hàm/thư viện đã được phê duyệt và kiểm tra các quy tắc và ngữ nghĩa liên quan đến logic và các lệnh gọi. Chúng có thể ghi nhận được các yếu tố mà con người có thể bỏ qua.

## **Xem xét Mã Thủ công**

Mã cũng có thể được xem xét một cách thủ công. Việc *xem xét mã thủ công* có thể được thực hiện theo một trong hai kiểu: được định hướng hoặc vô hướng. Trong một quá trình xem xét vô hướng, một lập trình viên kiểm tra mã để xem nó thực hiện điều gì và nó hoạt động như thế nào.

Điều này giống như việc đọc lại một bài báo, mặc dù việc xem xét mã thường là một nỗ lực của cả nhóm. Đánh giá có định hướng là đánh giá mà tác giả mã chạy thử mã, giải thích từng dòng cho những người còn lại trong nhóm. Điều này đảm bảo có nhiều quan sát hơn trong việc kiểm tra cú pháp và cấu trúc để tìm ra lỗi và điểm yếu.

### **Phân tích Mã Động**

*Phân tích mã động* được thực hiện trong khi phần mềm được thực thi, trên hệ thống nhằm mục tiêu hoặc hệ thống giả lập. Hệ thống được cung cấp các đầu vào thử nghiệm cụ thể đã được thiết kế để tạo ra các dạng hành vi cụ thể. Phân tích động có thể đặc biệt quan trọng đối với các hệ thống chằng hạn như hệ thống nhúng, nơi được kỳ vọng là sẽ có mức độ tự chủ hoạt động cao. Như một trường hợp điển hình, việc không thực hiện kiểm tra đầy đủ phần mềm của chương trình tên lửa Ariane đã dẫn đến việc mất bộ tăng áp Ariane 5 trong quá trình cất cánh. Các phân tích sau đó cho thấy rằng nếu thực hiện kiểm tra phần mềm thích hợp, các điều kiện lỗi đã có thể được phát hiện và sửa chữa mà không làm mất phương tiện bay. Nhiều lần, bạn có thể kiểm tra phần mềm đang sử dụng mà không cần phần còn lại của hệ thống, và đối với một số trường hợp sử dụng, khi chi phí của hỏng hóc là cao thì việc kiểm tra với phạm vi rộng rãi trước khi sử dụng thực tế là thông lệ tiêu chuẩn.

Phân tích động yêu cầu tự động hóa được chuyên biệt hóa để thực hiện thử nghiệm cụ thể. Trong số các công cụ có sẵn có các bộ kiểm tra động được thiết kế để giám sát hoạt động của các chương trình có mức độ cao của các chức năng song song, các thủ tục kiểm-trá-luồng để đảm bảo bộ xử lý đa lỗi và phần mềm đang quản lý các luồng một cách chính xác và các chương trình được thiết kế để phát hiện các điều kiện cạnh tranh và các lỗi đánh-địa-chỉ-bộ-nhỏ.



**MÁCH NƯỚC CHO KỲ THI** Phân tích mã tính là khi mã được kiểm tra mà không cần phải được thực thi. Phân tích mã động phân tích mã đang trong quá trình thực thi.

### Thám tử

*Thám tử* (hoặc *fuzz testing*) là một phương pháp cưỡng bức (brute force) để xác định các vấn đề và lỗ hổng xác thực đầu vào. Cơ sở cho việc kiểm tra thám tử một chương trình là việc áp dụng số lượng lớn các yếu tố đầu vào để xác định những đầu vào nào gây ra lỗi và đầu vào nào có thể dễ bị khai thác. Kiểm tra fuzz có thể được áp dụng tại bất kỳ nơi nào dữ liệu được trao đổi để xác minh rằng xác thực đầu vào đang được thực hiện một cách đúng đắn. Các giao thức mạng có thể được kiểm tra, các giao thức tập tin có thể được kiểm tra và các giao thức web có thể được kiểm tra. Phần lớn các lỗi trình duyệt được tìm thấy thông qua fuzzing. Kiểm tra fuzz hoạt động tốt trong các môi trường đã biết, môi trường chưa biết và môi trường đã biết một phần, vì nó có thể được thực hiện mà không cần biết về các chi tiết cụ thể của ứng dụng đang được kiểm tra.

### Tăng cường bảo mật (Hardening)

Vấn đề quản lý quan trọng đằng sau việc vận hành một thiết lập hệ thống bảo mật là xác định các nhu cầu cụ thể của hệ thống để hệ thống hoạt động đúng cách và chỉ kích hoạt các hạng mục cần thiết cho các chức năng đó. Việc giữ tất cả các dịch vụ và người dùng khác khỏi hệ thống sẽ cải thiện được thông lượng hệ thống và gia tăng tính bảo mật. Giảm diện tích bề mặt tấn công liên quan đến hệ thống làm giảm các lỗ hổng bảo mật hiện tại và trong tương lai khi các bản cập nhật là cần thiết.

## Các Cổng và Dịch vụ Mở

Các dịch vụ trên máy được truy cập thông qua cổng TCP hoặc UDP. Đối với các dịch vụ đang được sử dụng, điều quan trọng là cổng phải được mở và không bị chặn bởi tường lửa, vì điều này sẽ chặn lưu lượng truy cập vào dịch vụ. Nhưng đối với bảo mật, bất kỳ dịch vụ nào không được sử dụng trên hệ thống sẽ bị vô hiệu hóa và các cổng sẽ bị chặn bởi tường lửa. Điều này có tác dụng giảm bề mặt tấn công vào mục tiêu và loại bỏ mọi rủi ro dựa trên lỗ hổng bảo mật từ các dịch vụ không cần thiết. Việc chặn các cổng mở không cần thiết và tắt các dịch vụ không sử dụng đều khá dễ dàng và nên được áp dụng cho hầu hết mọi máy. Đây là một trong những cách phòng thủ rẻ tiền nhất và nên được áp dụng đầu tiên vì phạm vi rộng của các vấn đề mà nó gây ra.

Những kẻ tấn công sử dụng thăm dò tích cực và các công cụ như Nmap để quét và xem các cổng đang mở. Là một nhà phân tích bảo mật, bạn cũng có thể sử dụng các công cụ tương tự, bao gồm netstat, để nhanh chóng xác định các cổng đang lắng nghe và các kết nối đang hoạt động. Tất cả những thứ này phải được ánh xạ tới các dịch vụ cần thiết nếu không sẽ bị tắt và bị chặn.



## MÁCH NƯỚC CHO KỲ THI

Bất kỳ dịch vụ nào không được dự định sẽ sử dụng trên một hệ thống nên được vô hiệu hóa, và bất kỳ cổng không cần thiết nào nên được chặn lại bởi tường lửa.

## Registry

Registry trong các hệ thống Microsoft Windows hoạt động như một kho lưu trữ tất cả thông tin liên quan đến cấu hình [của hệ thống]. Các tùy chọn cấu hình cho Hệ điều hành nằm trong Registry. Các tùy chọn cấu hình cho các ứng dụng cũng được đặt trong Registry. Việc sử dụng mô

hình phân cấp cấu trúc để quản lý tất cả các thông số này ở một nơi giúp giải quyết tình trạng lộn xộn trong công việc quản gia khi thông tin cấu hình nằm rải rác trên toàn hệ thống, với các vấn đề kiểm soát truy cập cho từng vị trí.

Windows Registry không phải là một cấu trúc có thể được sửa đổi hoặc thay đổi một cách ngẫu nhiên. Một nhiệm vụ bảo mật bạn có thể thực hiện là tạo bản sao lưu Registry định kỳ vào một vị trí an toàn, vì điều này sẽ rất quan trọng trong trường hợp có điều gì đó làm thay đổi Registry hiện tại. Mặc dù Windows có các cơ chế để bảo vệ Registry, nhưng đây là một phần quan trọng của giao diện ứng dụng - hệ điều hành, nếu bị mất, các ứng dụng sẽ phải được tải lại và cấu hình lại. Các công cụ chỉnh-sửa-registry cũng có thể bị giới hạn bởi các chính sách nhóm trong hệ thống dựa-trên-miền.

## **Mã hóa ổ đĩa**

Tăng cường bảo mật (hardening) một hệ thống cũng có nghĩa là bảo vệ những thông tin trong hệ thống. *Mã hóa đĩa* có thể bảo vệ dữ liệu thậm chí ngay cả khi đĩa bị lấy ra khỏi hệ thống này và đặt vào hệ thống khác. Dữ liệu được mã hóa trên đĩa khiến nó trở nên không thể sử dụng được nếu không có các khóa thích hợp. Các giải pháp tốt nhất để mã hóa đĩa hiện nay đã được tích hợp sẵn trong hệ điều hành và sử dụng mã hóa phần cứng trên chính bản thân đĩa và lưu trữ các khóa trong TPM PCR. Điều này giúp cho hệ điều hành dễ dàng truy cập dữ liệu khi được khởi động và đăng nhập đúng cách, nhưng gần như không thể bị vượt qua, ngay cả khi tháo đĩa ra và lắp nó vào một máy khác.

## **OS**

Nhiều hệ thống khác nhau có nhu cầu đối với một *hệ điều hành (OS)*. Phần cứng trong mạng đòi hỏi một hệ điều hành để thực hiện chức năng kết nối mạng. Máy chủ và máy trạm yêu cầu hệ điều hành để hoạt động

như giao diện giữa các ứng dụng và phần cứng. Các hệ thống chuyên dụng như ki-ốt và thiết bị (appliance), cả hai đều là dạng hệ thống đa năng tự động, yêu cầu phải có hệ điều hành giữa phần mềm ứng dụng và phần cứng.

Máy chủ đòi hỏi một hệ điều hành để thu hẹp khoảng cách giữa phần cứng máy chủ và các ứng dụng đang được vận hành. Hiện tại, các Hệ điều hành máy chủ bao gồm Microsoft Windows Server, nhiều phiên bản Linux và ngày càng nhiều môi trường VM/hypervisor. Vì lý do hiệu suất, Linux có một thị phần đáng kể trong lĩnh vực Hệ điều hành máy chủ, mặc dù Windows Server với công nghệ Active Directory (AD) của nó đã xâm nhập đáng kể vào thị phần đó.

Hệ điều hành trên các máy trạm tồn tại để cung cấp một không gian hoạt động chức năng để người dùng tương tác với hệ thống và các ứng dụng khác nhau của nó. Do mức độ tương tác cao của người dùng trên các máy trạm nên việc nhận thấy Windows đang đóng vai trò này là rất phổ biến. Trong các doanh nghiệp lớn, khả năng quản lý người dùng, cấu hình và cài đặt dễ dàng của Active Directory trên toàn bộ doanh nghiệp đã mang lại cho các máy khách Windows một lợi thế hơn so với Linux.

Appliance là các thiết bị độc lập, được kết nối vào mạng và được thiết kế để chạy một ứng dụng nhằm thực hiện một chức năng cụ thể về lưu lượng truy cập. Các hệ thống này hoạt động như các máy chủ không đầu, được cấu hình sẵn với các ứng dụng hoạt động và thực hiện một loạt các dịch vụ bảo mật trên lưu lượng mạng mà chúng nhìn thấy. Vì lý do kinh tế, tính di động và chức năng, phần lớn các appliance được xây dựng dựa trên hệ thống dựa trên Linux. Do đây thường là các bản phân phối tùy chỉnh, nên việc giữ cho chúng được vá lỗi sẽ trở thành vấn đề của nhà cung cấp vì loại công việc này nằm ngoài phạm vi hoặc khả năng quản lý đúng cách của hầu hết nhân viên CNTT.

Ki-ốt là các máy độc lập, thường vận hành một phiên bản trình duyệt bên trên hệ điều hành Windows. Những máy này thường được thiết lập để tự động đăng nhập vào một phiên trình duyệt được khóa vào một trang web cho phép tất cả các chức năng mong muốn. Ki-ốt thường được sử dụng cho các ứng dụng dịch vụ khách hàng tương tác, chẳng hạn như các trang web thông tin tương tác, menu, v.v... Hệ điều hành trên ki-ốt cần có khả năng bị khóa ở các mức chức năng tối thiểu, có các yếu tố như đăng nhập tự động và cung cấp một cách thức dễ dàng để xây dựng các ứng dụng.

Các thiết bị di động bắt đầu là điện thoại với những năng lực bổ sung hạn chế, nhưng khi Internet và các chức năng lan rộng đến các thiết bị di động, khả năng của các thiết bị này cũng đã được mở rộng. Từ điện thoại thông minh đến máy tính bảng, hệ thống di động ngày nay là một máy tính với hầu như tất cả các khả năng tính toán mà người ta có thể yêu cầu – với một điện thoại kèm theo. Hai hệ điều hành di động chính trên thị trường hiện nay là hệ điều hành iOS của Apple và hệ điều hành Android của Google.

Bất kể hệ điều hành nào, các bản cập nhật và bản vá lỗi phải được áp dụng bất cứ đâu và bất cứ khi nào có thể. Mọi dịch vụ và phần mềm không cần thiết phải được tắt và/hoặc loại bỏ. Các cổng mở không cần thiết nên bị chặn hoặc đóng lại. Tất cả người dùng nên cài đặt mật khẩu mạnh và thay đổi chúng một cách thường xuyên. Các chính sách và quyền truy cập phải được thực hiện dựa trên đặc quyền ít nhất, nếu thích hợp. Tài khoản người dùng đặc quyền chỉ nên được sử dụng khi cần thiết và không được có tài khoản quản trị cục bộ trên các hộp Windows. Ngoài ra, việc ghi nhật ký nên được thực hiện. Trong môi trường dựa trên miền, các chính sách nhóm nên được triển khai để duy trì các cài đặt bảo mật.

## Quản lý Bản vá

*Quản lý bản vá* là quá trình được sử dụng để duy trì hệ thống theo cách luôn được cập-nhật, bao gồm tất cả các bản vá bắt buộc. Mọi hệ điều hành, từ Linux đến Windows, đều yêu cầu cập nhật phần mềm và mỗi hệ điều hành có các phương pháp khác nhau để hỗ trợ người dùng trong việc giữ cho hệ thống của họ luôn cập nhật.

Kể từ Windows 10 trở đi, Microsoft đã áp dụng một phương pháp luận mới coi Hệ điều hành như một dịch vụ và đã cập nhật đáng kể mô hình cung cấp dịch vụ của mình. Windows 10 hiện có lịch phát hành bản cập nhật tính năng hai-lần-một-năm, vào tháng 3 và tháng 9, với thời gian bảo dưỡng 18 tháng cho mỗi bản phát hành. Việc áp dụng tất cả các bản vá lỗi của Microsoft rất được khuyến khích, vì sau khi các bản vá được phát hành, những kẻ tấn công sẽ biết được các lỗ hổng.

Cách bạn vá lỗi hệ thống Linux như thế nào phụ thuộc rất nhiều vào phiên bản cụ thể đang sử dụng và bản vá lỗi đang được áp dụng. Trong một số trường hợp, bản vá lỗi sẽ bao gồm một loạt các bước thủ công yêu cầu quản trị viên thay thế tập tin, thay đổi quyền và thay đổi thư mục. Trong các trường hợp khác, các bản vá lỗi là các tập lệnh thực thi hoặc các tiện ích thực hiện các hành động vá lỗi một cách tự động. Một số phiên bản Linux, chẳng hạn như Red Hat, có các tiện ích được tích-hợp để xử lý quá trình vá lỗi. Trong những trường hợp đó, quản trị viên tải xuống tập tin được định dạng cụ thể mà tiện ích vá lỗi sau đó sẽ xử lý để thực hiện bất kỳ sửa đổi hoặc cập nhật nào cần phải được thực hiện.

Bất kể phương pháp bạn sử dụng để cập nhật hệ điều hành là gì, điều tối quan trọng là phải giữ cho hệ thống luôn được cập nhật. Các cảnh báo bảo mật mới được đưa ra mỗi ngày, và mặc dù lỗi tràn bộ đệm có thể là một vấn đề “tiềm ẩn” ngày nay, nhưng nó gần như chắc chắn sẽ trở thành một vấn đề “chắc chắn” trong tương lai gần. Giống như các bước được

thực hiện để xác định đường cơ sở và bảo mật ban đầu cho một hệ điều hành, việc giữ cho mọi hệ thống luôn được vá lỗi và cập nhật là điều cực kỳ quan trọng để bảo vệ hệ thống và thông tin mà nó chứa bên trong.

Các nhà cung cấp thường tuân theo một hệ thống phân cấp cho các bản cập nhật phần mềm:

- **Vá lỗi khẩn cấp (Hotfix)** Thuật ngữ này (thông thường) đề cập đến một bản cập nhật phần mềm nhỏ được thiết kế để giải quyết một vấn đề cụ thể, chẳng hạn như tràn bộ nhớ đệm trong một ứng dụng khiến hệ thống bị tấn công. Các hotfix thường được phát triển để ứng phó với một vấn đề đã được phát hiện và được sản xuất và phát hành một cách khá nhanh chóng.
- **Bản vá lỗi (Patch)** Thuật ngữ này đề cập đến một bản cập nhật phần mềm lớn hơn, chính thức hơn có thể giải quyết một số hoặc nhiều sự cố phần mềm. Các bản vá lỗi thường chứa các tính năng nâng cao hoặc các tính năng bổ sung cũng như các bản vá lỗi cho các lỗi đã biết. Các bản vá lỗi thường được phát triển trong một khoảng thời gian dài hơn.
- **Gói Dịch vụ (Service pack)** Thuật ngữ này đề cập đến một bộ sưu tập lớn các bản vá lỗi và các hotfix được đóng gói lại thành một gói duy nhất khá lớn. Các gói dịch vụ được thiết kế để đưa hệ thống lên cấp độ tốt-đã-biết mới nhất cùng một lúc, thay vì yêu cầu người dùng hoặc quản trị viên hệ thống tải xuống hàng chục hoặc hàng trăm bản cập nhật riêng lẻ.

### Các Cập nhật Bên-thứ-ba

Việc duy trì phần mềm được cập-nhật là một vấn đề về quy mô kém. Khi ngày càng có nhiều ứng dụng được thêm vào, từ sự lựa chọn càng ngày càng nhiều các nhà cung cấp, quá trình theo dõi xem phần mềm nào được cập nhật và chương trình nào yêu cầu cập nhật thực sự là một thách thức.

Để giải quyết thách thức này, một loạt các nhà cung cấp đề xuất các dịch vụ có thể kiểm tra các bản cập nhật và thậm chí cập nhật các ứng dụng của bạn cho bạn. Chìa khóa để thực hiện công việc này là đảm bảo rằng (1) giải pháp được chọn bao gồm cả các ứng dụng bạn sử dụng và (2) bạn đăng ký ứng dụng đúng cách với chương trình để chương trình biết những gì cần được cập nhật.

### Tự động Cập nhật

Cập nhật phần mềm là một nhiệm vụ bảo trì năm ở gần cuối danh sách của mọi người. Nó tương đối đơn giản: bạn chỉ cần tra cứu và xem có bản cập nhật mới hay không, tải xuống nếu có và tiến hành cập nhật. Và sau đó lặp lại quá trình cho mọi phần mềm trên hệ thống của bạn. Tốn thời gian và nhàn chán, đây rõ ràng là một nhiệm vụ dành cho tự động hóa. Hơn nữa, nhiệm vụ này thực sự đủ quan trọng để tự động hóa quy trình vá lỗi, bản thân nó cũng là một biện pháp kiểm soát bảo mật trong loạt NIST 800-53. Việc sử dụng chức năng tự động cập nhật để cập nhật phần mềm sẽ giải quyết được nhiều vấn đề hơn những gì nó tạo ra. Nhiều nhà cung cấp phần mềm hiện nay trang bị cho phần mềm của họ chức năng *tự-động-cập-nhật* có chức năng gọi về nhà, nhận bản cập nhật và cài đặt nó một cách tự động. Dĩ nhiên, có rủi ro rằng bản cập nhật mới sẽ không hoạt động một cách đúng đắn, nhưng điều đó chỉ có thể được phát hiện khi thử nghiệm rộng rãi và ngoại trừ các hệ thống chuyên dụng trong các hoạt động tối quan trọng, thử nghiệm sẽ không bao giờ xảy ra.

### Ổ đĩa Tự Mã hóa (SED)/ Mã hóa Ổ đĩa Toàn bộ (FDE)

*Ổ đĩa tự mã hóa (self-encrypting drive - SED) và mã hóa toàn bộ đĩa (full disk encryption - FDE)* là những phương pháp triển khai bảo vệ bằng mật mã trên các ổ đĩa cứng và các phương tiện lưu trữ tương tự với mục đích rõ ràng là bảo vệ dữ liệu, thậm chí ngay cả khi ổ đĩa đã được lấy ra khỏi máy. Những máy móc di động, chẳng hạn như máy tính xách tay, có một

điểm yếu về bảo mật là chúng tương đối dễ bị đánh cắp và sau đó có thể bị tấn công ngoại tuyến khi kẻ tấn công rảnh rỗi. Việc sử dụng mật mã hiện đại, kết hợp với khả năng bảo vệ phần cứng của các khóa, khiến cho véc-tơ tấn công này trở nên khó khăn hơn nhiều. Về bản chất, cả hai phương pháp này đều cung cấp một cách thức mã hóa toàn bộ ổ cứng minh bạch và liền mạch bằng cách sử dụng các khóa chỉ dành cho người nào có thể đăng nhập vào máy đúng cách.

### Opal

FDE và SED đã khởi đầu như là các giải pháp độc quyền chỉ-là-phần-mềm, nhưng một tiêu chuẩn dựa-trên-phần-cứng được gọi là Opal đã được tạo ra. Được phát triển bởi Trusted Computing Group (TCG), Opal được sử dụng để áp dụng mã hóa dựa trên phần cứng cho các thiết bị lưu trữ thứ cấp, ổ cứng (phương tiện quay), ổ đĩa trạng thái rắn và ổ đĩa quang. Có được một tiêu chuẩn sẽ mang lại lợi thế về khả năng tương tác lẫn nhau giữa các nhà cung cấp và có thể độc lập với hệ điều hành. Có nó trong phần cứng sẽ cải thiện hiệu suất và gia tăng tính bảo mật. Các khóa mã hóa/giải mã được lưu trữ trong bộ điều khiển ổ cứng và không bao giờ được tải vào bộ nhớ hệ thống, giúp chúng trở nên an toàn trước sự tấn công.



**MÁCH NƯỚC CHO KỲ THI** SED, FDE và Opal là những phương pháp triển khai mã hóa trên các ổ đĩa cứng.

### Hardware Root of Trust

*Gốc tin cậy phần cứng (hardware root of trust)* là khái niệm về việc nếu ai đó tin tưởng vào các chức năng bảo mật cụ thể của một nguồn thì lớp này có thể được sử dụng để tăng cường bảo mật cho các lớp cao hơn của hệ thống. Bởi vì nguồn gốc của niềm tin vốn đã được tin cậy, nên chúng

phải được đảm bảo an toàn bởi thiết kế. Điều này thường được thực hiện bằng cách giữ cho chúng nhỏ và giới hạn tính năng của chúng chỉ trong một số tác vụ cụ thể. Rất nhiều nguồn gốc của sự tin tưởng được triển khai trong phần cứng được cài đặt khỏi hệ điều hành và phần còn lại của hệ thống để phần mềm độc hại không thể can thiệp vào các chức năng mà chúng cung cấp. Các ví dụ về nguồn gốc của sự tin tưởng bao gồm chip TPM trong máy tính và bộ đồng xử lý Secure Enclave của Apple trong iPhone và iPad. Apple cũng sử dụng cơ chế Boot ROM đã được ký cho tất cả quá trình tải phần mềm.

Liên quan đến UEFI và Khởi động An toàn, đã được truy cập trước đây để cập trong chương này, thuật ngữ Root of Trust để cập đến điều kiện mà phần cứng và BIOS làm việc cùng nhau để đảm bảo tính toàn vẹn của BIOS cũng như tất cả các lần tải phần mềm và phần firmware tiếp theo. Sau khi hoàn tất, điều này tạo thành một Root of Trust có thể được chứng thực thông qua chip TPM.

### **Trusted Platform Module (TPM)**

*Mô-đun Nền tảng Đáng tin cậy (TPM)* là một giải pháp phần cứng trên bo mạch chủ, một giải pháp hỗ trợ việc tạo ra và lưu trữ khóa cũng như tạo các số ngẫu nhiên. Khi các khóa mã hóa được lưu trữ trong TPM, chúng trở nên không thể truy cập được qua các kênh phần mềm thông thường và được tách biệt về vật lý khỏi ổ cứng hoặc các vị trí dữ liệu đã được mã hóa khác. Điều này làm cho TPM trở thành một giải pháp an toàn hơn so với việc lưu trữ các khóa trên bộ nhớ thông thường của máy.

Nền tảng TPM cũng hỗ trợ các chức năng bảo mật khác thông qua một loạt các vị trí lưu trữ được bảo vệ được gọi là các thanh ghi cấu hình nền tảng (platform configuration registers - PCR). Các vị trí này được bảo vệ bằng mật mã khỏi việc đọc và ghi trái phép và đóng vai trò là vị trí cho

những thông tin tối quan trọng, chẳng hạn như dữ liệu tạo cơ sở cho Gốc Tin cậy.

### **Sandboxing**

*Hộp cát (sandboxing)* đề cập đến sự cách ly hoặc cô lập của một hệ thống khỏi môi trường xung quanh nó. Nó đã trở thành thông lệ tiêu chuẩn cho một số chương trình có bề mặt rủi ro gia tăng để hoạt động trong hộp cát, hạn chế sự tương tác với CPU và các tiến trình khác, chẳng hạn như bộ nhớ. Việc này hoạt động như một phương tiện cách ly, ngăn chặn các vấn đề thoát ra khỏi hộp cát và vào Hệ điều hành và các ứng dụng khác trên hệ thống.

Ảo hóa có thể được sử dụng như một dạng hộp cát đối với toàn bộ hệ thống. Bạn có thể xây dựng một máy ảo, kiểm tra một cái gì đó bên trong máy ảo và dựa trên kết quả, đưa ra quyết định về độ ổn định hoặc bất kỳ mối quan tâm nào tồn tại.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các khía cạnh của việc triển khai các giải pháp bảo mật ứng dụng hoặc bảo mật máy vật chủ. Chương này bắt đầu bằng việc khám phá các giải pháp bảo vệ điểm đầu cuối. Các giải pháp này bao gồm chống vi-rút, chống-phần-mềm-độc-hại, phát hiện và ứng phó tại điểm đầu cuối, ngăn chặn mất dữ liệu, tường lửa thế-hệ-kết-tiếp, hệ thống phát hiện xâm nhập dựa-trên-máy-vật-chủ, hệ thống ngăn chặn xâm nhập dựa-trên-máy-vật-chủ và tường lửa dựa-trên-máy-vật-chủ. Chủ đề chính tiếp theo là tính toàn vẹn của khởi động trong đó bảo mật khởi động/UEFI, khởi động được đo lường và chứng thực khởi động được đề cập. Tiếp theo là chủ đề về bảo mật cơ sở dữ liệu và trong phần này, các yếu tố về mã hóa, trộn muối và băm đã được đề cập.

Chủ đề về bảo mật ứng dụng là một phần quan trọng của chương này. Phần này bao gồm các chủ đề về xác thực đầu vào, bảo mật cookie, tiêu đề Giao thức Truyền tải Siêu văn bản (HTTP) và ký mã. Chủ đề này tiếp tục với danh sách cho phép và danh sách chặn/danh sách từ chối. Sau đó, nó chuyển sang thực tiễn mã hóa an toàn, phân tích mã tĩnh (bao gồm cả xem xét mã thủ công), phân tích mã động và fuzzing.

Phần chính tiếp theo là về việc tăng cường bảo mật hệ thống. Ở đây, chúng tôi đã đề cập đến các cổng và dịch vụ mở, đăng ký, mã hóa đĩa, hệ điều hành, quản lý bản vá, cập nhật của bên-thứ-ba và cập-nhật-tự động. Chương này đã kết thúc với cuộc thảo luận về ổ đĩa tự-mã-hóa (SED) và mã hóa toàn bộ đĩa (FDE), bao gồm Opal, hardware root of trust, Mô-jun nền tảng đáng tin cậy (TPM) và hộp cát.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

- 1.** Kiểm nghiệm fuzz hoạt động tốt nhất trong những môi trường kiểm nghiệm nào dưới đây?
  - A.** Môi trường kiểm nghiệm đã biết
  - B.** Môi trường kiểm nghiệm đã biết một phần
  - C.** Môi trường kiểm nghiệm chưa biết
  - D.** Kiểm nghiệm fuzz hoạt động tốt trong mọi môi trường nói trên.
- 2.** Phương pháp phân tích mã nào được thực hiện trong khi phần mềm đang được thực thi, trên hệ thống được nhắm mục tiêu hay hệ thống giả lập?
  - A.** Phân tích tĩnh
  - B.** Phân tích theo thời gian chạy
  - C.** Phân tích hộp cát
  - D.** Phân tích động.
- 3.** Điều nào dưới đây được liên kết với bảo vệ điểm đầu cuối? (Chọn tất cả các đáp án đúng).
  - A.** EDR
  - B.** TPM
  - C.** DLP
  - D.** Tiêu đề HTTP.
- 4.** Bạn có một loạt máy chủ web mà bạn đang muốn tăng cường bảo mật. Giải pháp nào sau đây là tốt nhất cho trường hợp này?
  - A.** Danh sách chặn/danh sách từ chối
  - B.** Một danh sách cho phép
  - C.** Bảo mật Cookie

**D. Ký mã.**

5. Bạn đang kiểm tra cơ sở hạ tầng máy chủ và muốn tăng cường bảo mật các máy trong khu vực máy chủ của mình. Nhiệm vụ đầu tiên bạn nên thực hiện trên tất cả các máy chủ của mình là gì?
- A. Áp dụng danh sách chặn/danh sách từ chối.**
  - B. Áp dụng danh sách cho phép.**
  - C. Chặn các cổng đang mở và vô hiệu hóa các dịch vụ không sử dụng.**
  - D. Sử dụng mã hóa đĩa.**
6. Cơ sở dữ liệu có thể sử dụng cách nào sau đây để bảo mật? (Chọn tất cả các đáp án đúng)
- A. Tokenization**
  - B. Trộn muối**
  - C. Ký mã**
  - D. Bảo mật Cookie.**
7. Khi bạn đang tạo ra một trang web, điều nào sau đây sẽ bảo vệ để chống lại các cuộc tấn công của người dùng vào trang web của bạn? (Chọn tất cả các đáp án đúng)
- A. Tokenization**
  - B. Tiêu đề HTTP**
  - C. Ký mã**
  - D. Fuzzing.**
8. Công ty của bạn có 200 máy tính để bàn được đặt tại ba địa điểm, chia ra cho hàng chục bộ phận nghiệp vụ. Điều nào sau đây sẽ là điều đầu tiên bạn nên đảm bảo đang hoạt động một cách chính xác để giảm thiểu rủi ro?
- A. Bảo mật ứng dụng**
  - B. Khởi động an toàn**
  - C. Quản lý bản vá**

**D. Bảo mật Cookie.**

- 9.** Bạn có một cơ sở dữ liệu chứa đầy những dữ liệu rất nhạy cảm. Nhân viên bán hàng cần truy cập một số dữ liệu nhạy cảm này khi đang gặp gỡ khách hàng. Phương pháp tốt nhất để ngăn chặn rò rỉ dữ liệu quan trọng trong các phiên truy cập này là sử dụng phương pháp nào sau đây?
- A.** Trộn muối  
**B.** Băm  
**C.** Danh sách chặn  
**D.** Mã hóa.
- 10.** Yếu tố nào sau đây không phải là một phần của Gốc Tin cậy?
- A.** Registry  
**B.** UEFI  
**C.** TPM PCR  
**D.** Chữ ký điện tử.

## Đáp án

1. **D.** Kiểm tra fuzz hoạt động tốt trong việc kiểm tra môi trường đã biết, môi trường không xác định và môi trường đã biết một phần, vì nó có thể được thực hiện mà không cần biết về các chi tiết cụ thể của ứng dụng đang được kiểm tra.
2. **D.** Phân tích động được thực hiện trong khi phần mềm được thực thi, trên hệ thống được nhắm mục tiêu hoặc hệ thống giả lập. Phân tích tĩnh là khi mã được kiểm tra mà không cần phải thực thi. Hộp cát để cập đến việc thực thi mã máy tính trong môi trường được thiết kế để cô lập mã khỏi sự tiếp xúc trực tiếp với hệ thống mục tiêu. Phân tích theo thời gian chạy là mô tả của kiểu phân tích nhưng không phải là thuật ngữ được sử dụng trong ngành.
3. **A và C.** Phát hiện và ứng phó tại điểm đầu cuối (EDR) là sự kết hợp của một số cơ chế bảo vệ điểm đầu cuối riêng lẻ vào một khuôn khổ quản lý chung. Ngăn ngừa mất mát dữ liệu (DLP) là việc kiểm tra dữ liệu nhạy cảm trước khi lọc. Cả hai điều này đều được liên kết với bảo mật điểm đầu cuối. Mô-đun nền tảng đáng tin cậy (TPM), mặc dù liên quan đến nhiều công nghệ bảo mật nhưng không đóng vai trò trực tiếp trong việc bảo vệ điểm đầu cuối. Đáp án cũng không phải là tiêu đề HTTP, được liên kết với máy chủ cung cấp nội dung web.
4. **B.** Các danh sách cho phép là đáp án lý tưởng phù hợp cho các máy chủ đơn-mục-đích, vì các ứng dụng được phép thực thi đã được biết trước.
5. **C.** Bởi vì khu vực máy chủ có thể có nhiều loại hệ thống khác nhau, các yếu tố như danh sách cho phép trở nên phức tạp hơn, vì kết quả không mở rộng trên các loại máy chủ khác nhau. Tất cả các máy đều được hưởng lợi từ việc chặn các cổng không sử dụng và vô hiệu hóa các dịch vụ không sử dụng.

6. **A** và **B.** Cơ sở dữ liệu có thể sử dụng mã thông báo để đại diện cho dữ liệu nhạy cảm duy nhất, cho phép kết hợp giữa các bảng và bản ghi mà vẫn không làm lộ dữ liệu. Trộn muối có thể được sử dụng để đảm bảo rằng các giá trị băm của các trường đầu vào giống hệt nhau sẽ không tiết lộ thực tế là hai bản ghi chia sẻ cùng một dữ liệu.
7. **B** và **D.** Tiêu đề HTTP ngăn các trình duyệt thực hiện một số hoạt động được phép (theo giao thức) nhưng không được khuyến nghị bởi các quy tắc của trang web. Fuzzing sẽ cung cấp thông tin đầu vào về lỗi xác thực đầu vào.
8. **C.** Quản lý bản vá lỗi làm giảm bề mặt tấn công vào hệ điều hành và các thành phần ứng dụng. Việc tự động hóa quy trình này là một bước khởi đầu quan trọng trong hành trình bảo mật vì số lượng hạng mục mà nó xử lý.
9. **D.** Việc sử dụng mã thông báo để nối các bản ghi trong khi ẩn các trường nhạy cảm là thực tế phổ biến đối với các chế độ xem trên các bảng trong cơ sở dữ liệu.
10. **A.** Windows Registry là nơi lưu trữ các tham số cấu hình cho hệ điều hành và các ứng dụng. Nó không được liên kết với Root of Trust, vì nó thậm chí không thể truy cập được trong quá trình thiết lập chuỗi tin cậy này.

## Chương 19    Thiết kế Mạng Bảo mật

### Thiết kế Mạng Bảo mật

Trong chương này bạn sẽ

- Tìm hiểu các phần tử thiết yếu của thiết kế mạng bảo mật,
- Khám phá những thiết bị khác nhau được sử dụng để bảo mật một mạng.

Các hệ thống mạng kết nối các thành phần của hệ thống CNTT của một doanh nghiệp, mang các tín hiệu và dữ liệu và cho phép hệ thống CNTT hoạt động theo cách thức được mong muốn đối với doanh nghiệp. Việc có được rủi ro tối thiểu đến từ hệ thống mạng là điều rất quan trọng, và các phương pháp để đạt được điều này là thông qua bảo mật thiết kế hệ thống mạng. Chương này khám phá các yếu tố của Security+ về thiết kế mạng bảo mật.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 3.3 của kỳ thi CompTIA Security+: Với một kịch bản, hãy triển khai các thiết kế mạng bảo mật.



#### MÁCH NƯỚC CHO KỲ THI

Việc chuẩn bị cho các câu hỏi dựa-trên-kịch-bản đòi hỏi nhiều hơn chỉ đơn giản là tìm hiểu về các thuật ngữ tương ứng với các giải pháp bảo mật dựa-trên-mạng như bộ định tuyến, bộ chuyển mạch, các proxy, và các bộ cân bằng tải. Bạn nên làm quen với cách thức và thời điểm để thiết lập cấu hình cho từng thiết bị dựa trên một kịch bản nhất định.

## Cân bằng tải

Một số hệ thống nhất định, chẳng hạn như các máy chủ, quan trọng hơn đối với hoạt động kinh doanh và do đó phải là đối tượng của các biện pháp chịu-lỗi. Một kỹ thuật phổ biến được sử dụng trong khả năng chịu lỗi là cân bằng tải thông qua việc sử dụng một bộ cân bằng tải. Việc *Cân bằng tải* liên quan đến việc sử dụng các thiết bị di chuyển tải trên một tập hợp tài nguyên với nỗ lực không làm quá tải các máy chủ riêng lẻ. Kỹ thuật này được thiết kế để phân phối tải xử lý trên hai hoặc nhiều hệ thống. Nó được sử dụng để giúp cải thiện việc sử dụng tài nguyên và thông lượng nhưng cũng có thêm lợi thế là làm gia tăng khả năng chịu lỗi của hệ thống tổng thể vì một tiến trình quan trọng có thể được chia nhỏ trên nhiều hệ thống. Nếu bất kỳ một hệ thống nào bị lỗi, các hệ thống khác có thể tiếp nhận tiến trình mà nó hệ thống bị lỗi đang xử lý. Mặc dù có thể có tác động đến thông lượng tổng thể nhưng hoạt động không hoàn toàn giảm xuống. Cân bằng tải thường được sử dụng cho các hệ thống xử lý trang web, truyền tải tập tin băng-thông-cao và các mạng Internet Relay Chat (IRC) lớn. Cân bằng tải hoạt động bằng một loạt các kiểm tra sức khỏe để cho bộ cân bằng tải biết được rằng máy nào đang hoạt động và thông qua cơ chế lập lịch trình để phân phối công việc đồng đều. Cân bằng tải là tốt nhất cho các hệ thống không cần trạng thái, vì các yêu cầu tiếp theo có thể được xử lý bởi bất kỳ máy chủ nào, không chỉ là máy chủ đã xử lý yêu cầu trước đó.

### Hoạt động/Hoạt động (Active/Active)

Trong một lược đồ *hoạt động/hoạt động*, tất cả các bộ cân bằng tải đều đang hoạt động, chia sẻ các nhiệm vụ cân-bằng-tải. Cân bằng tải hoạt động/hoạt động có thể mang lại hiệu quả của hiệu suất, nhưng điều quan trọng là phải xem xét tải trọng tổng thể. Nếu tải trọng tổng thể không được bao phủ bởi  $N - 1$  bộ cân bằng tải (nghĩa là một bộ bị lỗi) thì sự cố của bộ cân bằng tải sẽ dẫn đến gián đoạn phiên và gây mất lưu lượng.

Nếu không có hệ thống thụ động dự phòng để khôi phục lại tải đã bị mất, hệ thống sẽ cắt tải dựa trên công suất, loại bỏ các yêu cầu mà hệ thống không đủ khả năng phục vụ.



**MÁCH NƯỚC CHO KỲ THI** Hai hay nhiều máy chủ hoạt động cùng nhau để phân phối tải trong một cấu hình cân-bằng-tải hoạt động/hoạt động. Nếu một máy chủ bị lỗi, sự gián đoạn dịch vụ hoặc mất lưu lượng có thể xảy ra.

### **Chủ động/Thụ động (Active/Passive)**

Đối với các giải pháp có tính-sẵn-sàng-cao, việc chỉ có một bộ cân bằng tải duy nhất tạo ra một điểm đơn lỗi (single point of failure – SPOF). Điều phổ biến là có nhiều bộ cân bằng tải cùng tham gia vào hoạt động cân bằng tải. Trong lược đồ *chủ động/thụ động*, bộ cân bằng tải chính đang thực hiện một cách chủ động công việc cân bằng tải trong khi bộ cân bằng tải thứ cấp quan sát một cách thụ động và sẵn sàng tham gia [công việc cân bằng tải] bất cứ thời điểm nào bộ cân bằng tải chính bị lỗi.



**MÁCH NƯỚC CHO KỲ THI** Tất cả lưu lượng được gửi đến cho máy chủ đang hoạt động trong cấu hình chủ động/thụ động. Nếu máy chủ đang hoạt động bị lỗi, máy chủ thụ động sẽ được thăng cấp thành chủ động.

### **Lập lịch trình**

Khi một bộ cân bằng tải chuyển các tải trọng qua một tập hợp các tài nguyên, nó quyết định máy nào sẽ nhận được một yêu cầu thông qua một thuật toán *lập lịch trình*. Có hai thuật toán lập lịch trình được sử dụng phổ biến: lập lịch trình dựa-trên-quan-hệ và lập lịch trình xoay-vòng.

## Quan hệ

*Lập lịch trình dựa-trên-quan-hệ* được thiết kế để giữ cho một máy vật chủ tiếp tục kết nối đến một máy chủ trong suốt một phiên. Một số ứng dụng, chẳng hạn như ứng dụng web, có thể được hưởng lợi từ việc lập lịch trình dựa-trên-quan-hệ. Phương pháp được sử dụng bởi lập lịch trình dựa-trên-quan-hệ là để bộ cân bằng tải theo dõi vị trí cuối cùng nó đã cân bằng một phiên cụ thể và hướng tất cả lưu lượng phiên tiếp tục đến cùng một máy chủ. Nếu đó là một kết nối mới, bộ cân bằng tải sẽ thiết lập một mục nhập mới quan hệ mới và chỉ định phiên cho máy chủ tiếp theo trong vòng quay đang sẵn sàng.

## Xoay-Vòng

*Lập lịch trình xoay-vòng* liên quan đến việc gửi từng yêu cầu mới đến máy chủ tiếp theo trong vòng quay. Mọi yêu cầu được gửi đến máy chủ với số lượng như nhau, bất kể tải của máy chủ. Các sơ đồ xoay-vòng thường xuyên được sửa đổi với một hệ số trọng số, còn được gọi là xoay-vòng có trọng số, để tính đến tải của máy chủ hoặc các tiêu chí khác khi chỉ định máy chủ tiếp theo.



## MÁCH NƯỚC CHO KỲ THI

Xoay-vòng và xoay-vòng có trọng số là các thuật toán lập lịch trình được sử dụng dành cho các chiến lược cân-bằng-tải.

## IP Ảo

Trong một môi trường đã được cân bằng tải, các địa chỉ IP dành cho các máy chủ mục tiêu của một bộ cân bằng tải sẽ không nhất thiết phải khớp với địa chỉ tương ứng với địa chỉ được liên kết với bộ định tuyến gửi lưu lượng truy cập. Bộ cân bằng tải xử lý việc này thông qua khái niệm địa

chỉ IP ảo hoặc *IP ảo*, cho phép nhiều hệ thống được phản ánh trở lại dưới dạng một địa chỉ IP duy nhất

### Tính bền bỉ

*Tính bền bỉ* là điều kiện mà một hệ thống kết nối đến cùng một mục tiêu trong một hệ thống cân bằng tải. Điều này có thể rất quan trọng để duy trì trạng thái và tính toàn vẹn của nhiều sự kiện khứ hồi. Tính bền bỉ đạt được thông qua việc lập lịch trình dựa-trên-quan-hệ của tài sản máy chủ trong cân bằng tải. Điều này đã được thảo luận trong phần “Mối quan hệ” trước đó trong chương này.

### Phân đoạn Mạng

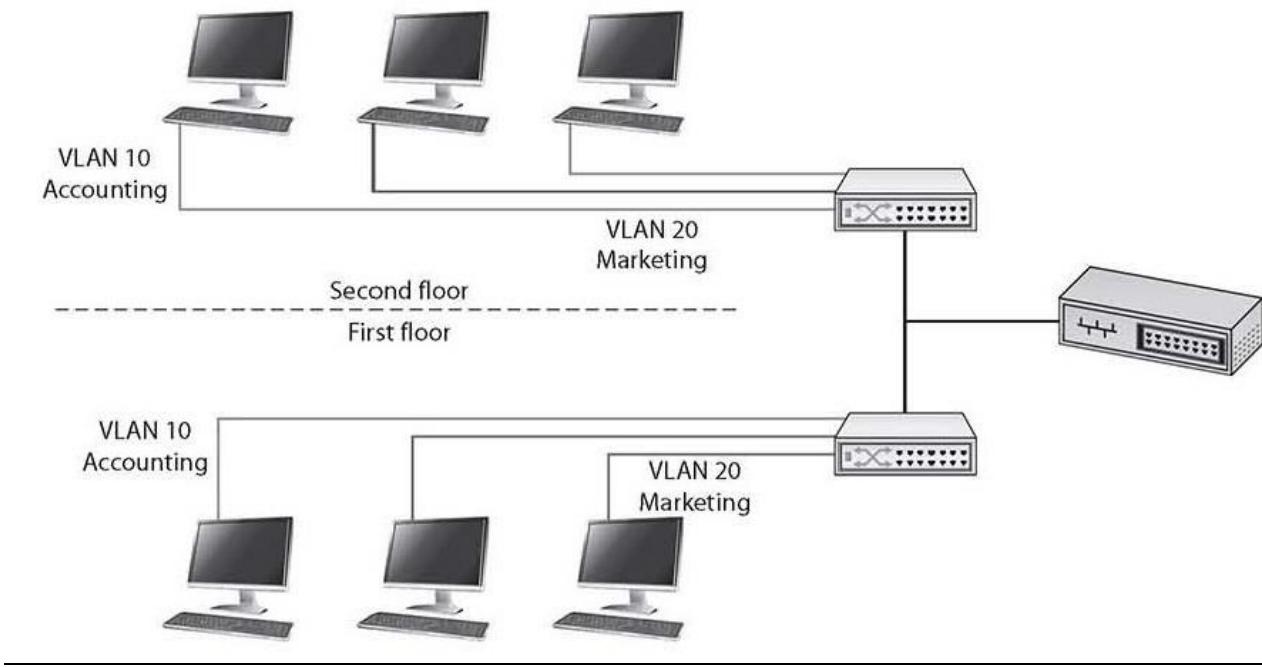
*Phân đoạn mạng* là nơi bạn đã thiết lập cấu hình các thiết bị mạng để giới hạn lưu lượng truy cập qua các phần khác nhau của mạng. Điều này có thể được thực hiện để ngăn chặn việc truy cập vào các máy nhạy cảm, nhưng vẫn hỗ trợ việc quản lý lưu lượng mạng. Một nhóm các máy chủ cơ sở dữ liệu không bao giờ cần kết nối trực tiếp với Internet có thể được đặt trên một phân đoạn mạng mà các quy tắc định tuyến sẽ không cho phép kết nối trực tiếp từ bên ngoài vùng được bảo vệ. Việc chia mạng thành các phân đoạn thường không tốn nhiều thiết bị hơn, mà thay vào đó, được thực hiện theo cách thiết bị mạng được cấu hình để giao tiếp qua các phân đoạn đã xác định. Một mạng con được sàng lọc (DMZ) là một ví dụ về một phân đoạn, một phân đoạn có thể truy cập được từ Internet và từ mạng nội bộ, nhưng không thể vượt qua trực tiếp.

### Mạng Khu vực Cục bộ Ảo (VLAN)

Mạng LAN là một tập hợp các thiết bị có chức năng tương tự nhau và nhu cầu giao tiếp tương tự nhau, thường được đặt-cùng-vị-trí và hoạt động trên một bộ chuyển mạch duy nhất. Đây là mức thấp nhất của hệ thống phân cấp mạng và xác định miền cho các giao thức nhất định ở lớp liên kết dữ liệu (lớp 2) để giao tiếp. Một mạng LAN ảo (VLAN) là sự triển khai

luận lý của một mạng LAN và cho phép các máy tính kết nối với các mạng vật lý khác nhau hoạt động và giao tiếp như thể chúng đang ở trên cùng một mạng vật lý. Một VLAN có nhiều thuộc tính đặc trưng giống như một mạng LAN và hoạt động giống như một mạng LAN vật lý nhưng được triển khai bằng cách sử dụng thiết bị chuyển mạch và phần mềm. Kỹ thuật cực kỳ mạnh mẽ này cho phép mạng có tính linh hoạt, khả năng mở rộng và hiệu suất đáng kể và cho phép quản trị viên thực hiện tái thiết lập cấu hình mạng mà không cần phải di dời hoặc đổi-lại hệ thống cáp.

Trunking (tạo đường trực) là quá trình mở rộng một VLAN đơn lẻ qua nhiều bộ thiết bị chuyển mạch. Kết nối dựa-trên-đường-trục giữa các bộ chuyển mạch cho phép các gói từ một VLAN di chuyển giữa các bộ chuyển mạch, như trong Hình 19-1. Hai trực được thể hiện trong hình: VLAN 10 được triển khai với một trực và VLAN 20 được triển khai với trực còn lại. Các máy chủ trên các VLAN khác nhau không thể giao tiếp bằng cách sử dụng các trực và do đó được chuyển qua mạng chuyển mạch. Các trực cho phép quản trị viên mạng thiết lập VLAN trên nhiều thiết bị chuyển mạch với nỗ lực tối thiểu. Với sự kết hợp của các trực và VLAN, quản trị viên mạng có thể chia nhỏ mạng theo chức năng của người dùng mà không cần quan tâm đến vị trí máy chủ trên mạng hoặc nhu cầu đi-lại cáp của các máy.



**Hình 19-1** Các VLAN và các trục

Các VLAN được sử dụng để chia một mạng thành nhiều mạng con dựa trên chức năng. Điều này cho phép các bộ phận kế toán và tiếp thị, chẳng hạn, cùng chia sẻ một bộ chuyển mạch vì ở gần nhau nhưng vẫn có các miền lưu lượng riêng biệt. Vị trí vật lý của thiết bị và cáp được phân tách một cách luận lý và theo chương trình để các cổng liền kề trên một bộ chuyển mạch có thể tham chiếu đến các mạng con riêng biệt. Điều này ngăn chặn việc sử dụng trái phép các thiết bị gần nhau về mặt vật lý thông qua các mạng con riêng biệt trên cùng một thiết bị. Các VLAN cũng cho phép quản trị viên mạng xác định một VLAN không có người dùng và ánh xạ tất cả các cổng không sử dụng đến VLAN này (một số thiết bị chuyển mạch được quản lý cho phép quản trị viên vô hiệu hóa các cổng không sử dụng). Sau đó, nếu người dùng trái phép có được quyền truy cập vào thiết bị, người dùng đó sẽ không thể sử dụng các cổng không được sử dụng, vì các cổng đó sẽ được xác định về mặt bảo mật là không

có gì. Mục đích và sức mạnh bảo mật của VLAN là rằng các hệ thống trên các VLAN riêng biệt không thể giao tiếp với nhau một cách trực tiếp.

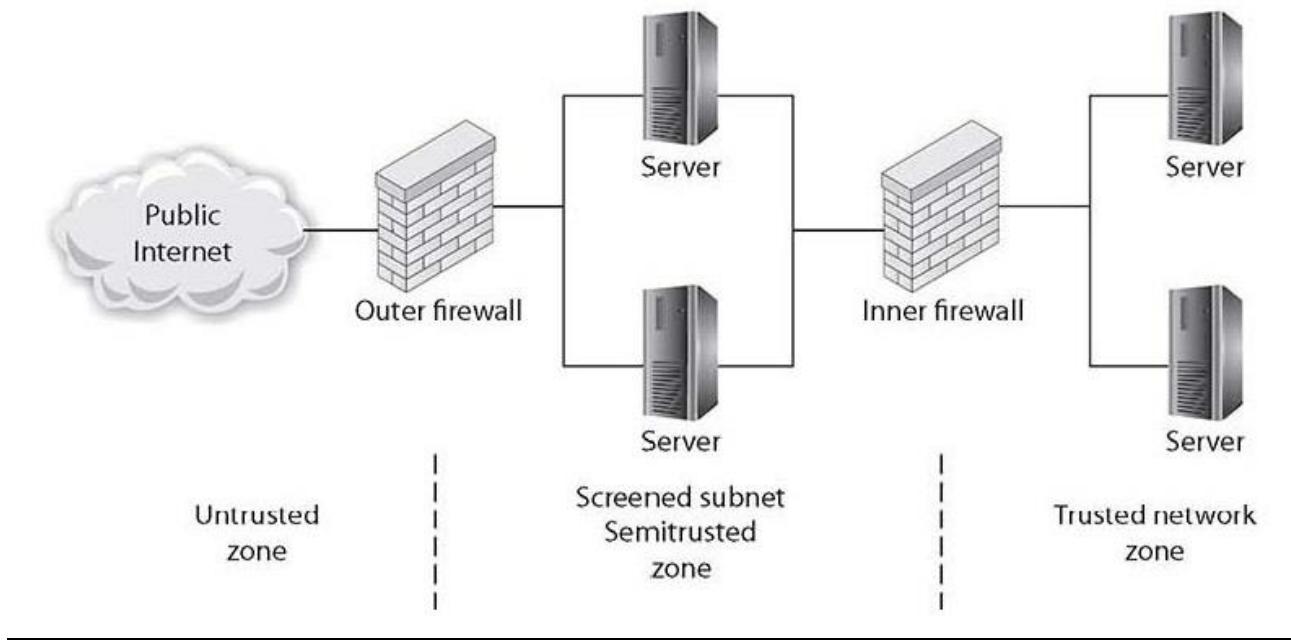


**MÁCH NƯỚC CHO KỲ THI** Sự phân tách về mặt vật lý đòi hỏi phải tạo ra hai hay nhiều mạng vật lý, mỗi mạng có các máy chủ, bộ chuyển mạch và bộ định tuyến của riêng nó. Sự phân tách về mặt luận lý sử dụng một mạng vật lý với các tường lửa và/hoặc bộ định tuyến phân tách và tạo điều kiện cho giao tiếp giữa các mạng luận lý.

### **Mạng con được Sàng lọc (Trước đây được gọi là Khu Phi quân sự - DMZ)**

Khu vực nằm giữa Internet không đáng tin cậy và mạng nội bộ đáng tin cậy được gọi là *mạng con được sàng lọc*. Điều này trước đây được biết đến với thuật ngữ *khu phi quân sự (DMZ)*, theo tên gọi của khu vực quân sự có cùng tên, nơi mà không bên nào có bất kỳ quyền kiểm soát cụ thể nào. Trong mạng nội bộ và bảo mật, các nhánh riêng biệt thường được tạo ra để cung cấp các khu vực chức năng cụ thể.

Một mạng con được sàng lọc trong mạng máy tính được sử dụng theo cách thức tương tự, nó hoạt động như một vùng đệm giữa Internet, nơi không tồn tại sự kiểm soát và mạng bên trong bảo mật, nơi một tổ chức có các chính sách bảo mật. Để phân định ranh giới các khu vực và thực thi sự phân tách, tường lửa được sử dụng ở mỗi bên của mạng con được sàng lọc. Khu vực giữa những tường lửa này có thể truy cập được từ mạng bên trong, mạng bảo mật hoặc Internet. Hình 19-2 minh họa các vùng này do vị trí của tường lửa tạo ra. Các tường lửa được thiết kế đặc biệt để ngăn chặn truy cập trực tiếp qua mạng con được sàng lọc từ Internet vào mạng nội bộ bảo mật.



**Hình 19-2** Mạng con được sàng lọc và khu vực đáng tin cậy

Sự chú ý đặc biệt là cần thiết đối với các cài đặt bảo mật của các thiết bị được đặt trong khu vực mạng con được sàng lọc, vì bạn nên coi chúng là luôn luôn bị xâm phạm bởi những người dùng trái phép. Các máy bị khóa chức năng để bảo lưu tính bảo mật thường được gọi là *hệ điều hành đã được tăng cường bảo mật* trong ngành. Phương pháp tiếp cận khóa này cần được áp dụng cho các máy nằm trong mạng con được sàng lọc và mặc dù điều đó có nghĩa là chức năng của chúng sẽ bị hạn chế, những biện pháp phòng ngừa như vậy đảm bảo rằng các máy sẽ hoạt động bình thường trong một môi trường kém-an-toàn.

Rất nhiều loại máy chủ thuộc về mạng con được sàng lọc, bao gồm máy chủ web đang cung cấp nội dung cho người dùng Internet, cũng như máy chủ truy cập từ xa và máy chủ email bên ngoài. Nói chung, bất kỳ máy chủ nào được truy cập trực tiếp từ bên ngoài – từ vùng Internet không đáng tin cậy – cần phải nằm trong mạng con được sàng lọc. Các máy chủ khác không nên được đặt trong mạng con đã được sàng lọc. Máy chủ tên

miễn cho mạng nội bộ đáng tin cậy của bạn và máy chủ cơ sở dữ liệu chứa cơ sở dữ liệu của công ty sẽ không nên truy cập được từ bên ngoài. Máy chủ ứng dụng, máy chủ tập tin, máy chủ in ấn - tất cả các máy chủ tiêu chuẩn được sử dụng trong mạng đáng tin cậy - phải nằm sau cả tường lửa bên trong lẫn bên ngoài, cùng với bộ định tuyến và thiết bị chuyển mạch được sử dụng để kết nối các máy này.

Ý tưởng đằng sau việc sử dụng cấu trúc liên kết mạng con được sàng lọc là buộc người dùng bên ngoài thực hiện ít nhất một bước trong mạng con được sàng lọc trước khi anh ta có thể truy cập thông tin bên trong mạng đáng tin cậy. Nếu người dùng bên ngoài đưa ra một yêu cầu về tài nguyên từ mạng đáng tin cậy, chẳng hạn như phần tử dữ liệu từ cơ sở dữ liệu thông qua trang web, thì yêu cầu này cần tuân theo tình huống sau:

- 1.** Người dùng từ mạng không đáng tin cậy (Internet) yêu cầu dữ liệu qua một trang web từ một máy chủ web trong mạng con được sàng lọc.
- 2.** Máy chủ web trong mạng con được sàng lọc yêu cầu dữ liệu từ máy chủ ứng dụng, có thể nằm trong mạng con được sàng lọc hoặc trong mạng nội bộ đáng tin cậy.
- 3.** Máy chủ ứng dụng yêu cầu dữ liệu từ máy chủ cơ sở dữ liệu trong mạng tin cậy.
- 4.** Máy chủ cơ sở dữ liệu trả lại dữ liệu cho máy chủ ứng dụng yêu cầu.
- 5.** Máy chủ ứng dụng trả lại dữ liệu cho máy chủ web đang yêu cầu.
- 6.** Máy chủ web trả lại dữ liệu cho người dùng đang yêu cầu từ mạng không đáng tin cậy.

Sự tách biệt này hoàn thành hai nhiệm vụ cụ thể và độc lập. Đầu tiên, người dùng được tách biệt khỏi yêu cầu dữ liệu trên một mạng bảo mật. Bằng cách nhờ người trung gian thực hiện yêu cầu, phương pháp tiếp cận

được phân lớp này cho phép các mức bảo mật đáng kể được thực thi. Người dùng không có quyền truy cập hoặc kiểm soát trực tiếp các yêu cầu của họ và quá trình lọc này có thể đưa ra các biện pháp kiểm soát. Thứ hai, khả năng mở rộng dễ dàng được hiện thực hóa hơn. Giải pháp đa-máy-chủ có thể được thực hiện để có khả năng mở rộng rất cao, theo đúng nghĩa đen đối với hàng triệu người dùng mà không làm chậm bất kỳ lớp cụ thể nào.

---



**MÁCH NƯỚC CHO KỲ THI** Các mạng con được sàng lọc đóng vai trò như một vùng đệm giữa những khu vực mạng không được bảo vệ (Internet) và những khu vực được bảo vệ (nơi đang lưu trữ dữ liệu nhạy cảm của công ty), cho phép giám sát và quy định lưu lượng giữa hai khu vực.

### Lưu lượng Đông-Tây

Các luồng dữ liệu trong doanh nghiệp có thể được mô tả theo các hình mẫu, chẳng hạn như bắc - nam và đông - tây. Dữ liệu ra vào trung tâm dữ liệu hoặc doanh nghiệp được gọi là lưu lượng bắc - nam. *Lưu lượng đông - tây* là mẫu luồng dữ liệu giữa các thiết bị trong một bộ phận của doanh nghiệp (nghĩa là giữa các hộp liên quan đến chức năng để hỗ trợ cho lưu lượng theo hướng bắc - nam). Mức độ lưu lượng truy cập đông - tây rất quan trọng đối với các kỹ sư mạng vì cơ sở hạ tầng mạng phải có khả năng duy trì tải hoạt động.

---



**MÁCH NƯỚC CHO KỲ THI** *Lưu lượng đông - tây* đề cập đến luồng dữ liệu mạng trong một mạng doanh nghiệp. *Lưu lượng bắc - nam* đề cập

đến dữ liệu theo luồng giữa mạng doanh nghiệp hoặc trung tâm dữ liệu và mạng bên ngoài.

### **Mạng ngoại vi (Extranet)**

*Mạng ngoại vi (extranet)* là phần mở rộng của một phần được chọn trong mạng nội bộ của công ty cho các đối tác bên ngoài. Điều này cho phép một doanh nghiệp chia sẻ thông tin với khách hàng, nhà cung cấp, đối tác và các nhóm đáng tin cậy khác trong khi sử dụng một bộ giao thức Internet chung để tạo điều kiện thuận lợi cho các hoạt động. Các mạng ngoại vi có thể sử dụng mạng công cộng để mở rộng phạm vi tiếp cận của chúng ra ngoài phạm vi mạng nội bộ của chính công ty và một số hình thức bảo mật, điển hình là mạng riêng ảo (virtual private network - VPN), được sử dụng để bảo mật kênh này. Việc sử dụng thuật ngữ *extranet* bao hàm cả quyền riêng tư và bảo mật. Quyền riêng tư là bắt buộc đối với nhiều giao tiếp và cần có bảo mật để ngăn chặn việc sử dụng và các sự kiện trái phép xảy ra. Cả hai chức năng này đều có thể đạt được thông qua việc sử dụng các công nghệ được mô tả trong chương này và các chương khác trong quyển sách này. Quản lý tường lửa thích hợp, truy cập từ xa, mã hóa, xác thực và đường hầm an toàn trên các mạng công cộng là tất cả những phương pháp được sử dụng để đảm bảo quyền riêng tư và bảo mật cho các mạng ngoại vi.



### **MÁCH NƯỚC CHO KỲ THI**

Một extranet là một mạng bán riêng tư sử dụng những công nghệ mạng phổ biến (HTTP, FTP, v.v...) để chia sẻ thông tin và cung cấp tài nguyên cho các đối tác kinh doanh. Các mạng ngoại vi có thể được truy cập bởi nhiều hơn một công ty vì chúng chia sẻ thông tin giữa các tổ chức.

## Intranet

Mạng Internet nội bộ (*intranet*) mô tả một mạng có chức năng giống như Internet cho người dùng nhưng nằm hoàn toàn bên trong vùng đáng tin cậy của mạng và chịu sự kiểm soát bảo mật của hệ thống và của quản trị viên mạng. Thường được gọi là mạng trường (campus) hoặc mạng công ty (corporate), mạng Internet nội bộ được sử dụng hàng ngày trong các công ty trên khắp thế giới. Mạng Internet nội bộ cho phép nhà phát triển và người dùng tập hợp đầy đủ các giao thức - HTTP, FTP, nhắn tin tức thời, v.v... - được cung cấp trên Internet, nhưng có thêm lợi thế về sự tin cậy từ bảo mật mạng. Nội dung trên các máy chủ web của mạng Internet nội bộ không được cung cấp qua Internet cho những người dùng không đáng tin cậy. Lớp bảo mật này cung cấp một lượng kiểm soát và quy định đáng kể, cho phép người dùng thực hiện chức năng nghiệp vụ trong khi vẫn đảm bảo được sự bảo mật.

Hai phương pháp có thể được sử dụng để cung cấp thông tin cho người dùng bên ngoài, bao gồm: nhân bản thông tin vào các máy trong mạng con được sàng lọc có thể khiến cho nó trở nên sẵn sàng đối với người dùng khác. Kiểm tra và kiểm soát bảo mật thích hợp nên được thực hiện trước khi nhân bản tài liệu để đảm bảo các chính sách bảo mật liên quan đến tính sẵn sàng của dữ liệu cụ thể vẫn đang được tuân thủ. Ngoài ra, các mạng ngoại vi (đã được thảo luận trong phần trước) có thể được sử dụng để xuất bản tài liệu cho các đối tác đáng tin cậy.



## MÁCH NƯỚC CHO KỲ THI

Một mạng Internet nội bộ là một mạng riêng tư, nội bộ sử dụng những công nghệ mạng phổ biến (HTTP, FTP, v.v...) để chia sẻ thông tin và cung cấp tài nguyên cho người dùng trong nội bộ tổ chức.

Nếu người dùng bên trong mạng nội bộ yêu cầu quyền truy cập thông tin từ Internet, máy chủ proxy có thể được sử dụng để ẩn vị trí của người yêu cầu. Điều này giúp bảo mật mạng Internet nội bộ khỏi việc ánh xạ bên ngoài của cấu trúc liên kết thực tế của nó. Tất cả các yêu cầu Internet sẽ được chuyển đến máy chủ proxy. Nếu một yêu cầu vượt qua các yêu cầu lọc, máy chủ proxy, giả sử nó cũng là một máy chủ bộ đệm cache, sẽ tìm kiếm trong bộ đệm cục bộ của các trang web đã được tải xuống trước đó. Nếu nó tìm thấy trang đó trong bộ nhớ đệm cache của nó, nó sẽ trả lại trang đó cho người yêu cầu mà không cần gửi yêu cầu đến Internet. Nếu trang đó không có trong bộ nhớ đệm cache, máy chủ proxy, hoạt động như một máy khách dưới danh nghĩa của người dùng, sử dụng một trong các địa chỉ IP của chính nó để yêu cầu trang đó từ Internet. Khi trang web được trả lại, máy chủ proxy sẽ lập tương quan nó với yêu cầu ban đầu và chuyển tiếp nó tới người dùng. Điều này che địa chỉ IP của người dùng khỏi Internet. Các máy chủ proxy có thể thực hiện một số chức năng cho một công ty, ví dụ, chúng có thể giám sát các yêu cầu về lưu lượng truy cập, loại bỏ các yêu cầu không phù hợp như nội dung không phù hợp với công việc. Chúng cũng có thể hoạt động như một máy chủ bộ nhớ đệm cache, cắt giảm các yêu cầu mạng bên ngoài cho cùng một đối tượng. Cuối cùng, máy chủ proxy bảo vệ danh tính của địa chỉ IP nội bộ bằng cách sử dụng Dịch Địa chỉ mạng (NAT), mặc dù chức năng này cũng có thể được thực hiện thông qua bộ định tuyến hoặc tường lửa bằng NAT. Máy chủ proxy và NAT sẽ được đề cập chi tiết ở phần sau của chương này.

## **Zero Trust**

Bảo mật mạng CNTT truyền thống được căn cứ vào mô hình lâu đài và hào chấn (castle and moat). Trong mô hình lâu đài và hào chấn, khó có thể truy cập từ bên ngoài mạng do có các bức tường và hào chấn, với quyền truy cập duy nhất là cổng, nơi ID được kiểm tra. Khi bạn đã vào

bên trong, niềm tin sẽ được lan truyền bằng việc bạn đã vượt qua kiểm tra tại cửa khẩu. Phương pháp tiếp cận này đã được sử dụng trong nhiều năm vì nó đơn giản để triển khai, nhưng vấn đề của cách tiếp cận này là một khi kẻ tấn công có được quyền truy cập vào mạng, chúng sẽ có quyền truy cập vào mọi thứ bên trong.

*Zero trust* là một mô hình bảo mật tập trung vào niềm tin rằng bạn không nên tin tưởng vào bất kỳ yêu cầu nào mà không xác minh xác thực và cấp phép. Việc triển khai Zero Trust yêu cầu xác minh danh tính nghiêm ngặt đối với tất cả những tài khoản đang cố gắng truy cập tài nguyên, bất kể vị trí của họ. Bảo mật Zero trust đòi hỏi một phương pháp tiếp cận toàn diện đối với bảo mật kết hợp một số lớp công nghệ và phòng thủ bổ sung.

## Mạng Riêng Ảo

Những công nghệ *mạng riêng ảo (VPN)* cho phép hai mạng kết nối một cách bảo mật trên một dải mạng không an toàn bằng cách tạo đường hầm qua các kết nối trung gian. Những công nghệ này đạt được với các giao thức đã được thảo luận trong nhiều chương trong quyển sách này, chẳng hạn như IPSec, L2TP, SSL/TLS và SSH. Ở cấp độ này, bạn nên hiểu rằng những công nghệ này cho phép hai địa điểm, chẳng hạn như mạng gia đình của nhân viên từ xa và mạng công ty, giao tiếp với nhau qua các mạng không bảo mật, bao gồm cả Internet, với hồ sơ rủi ro thấp hơn nhiều. Hai cách sử dụng chính cho công nghệ đường hầm/VPN là giao tiếp điểm-tới-điểm và truy cập từ xa vào một mạng.

VPN hoạt động vì chỉ các điểm đầu cuối mới có những thông tin để giải mã các gói tin đang được gửi qua mạng. Tại tất cả các bước nhảy trung gian, nếu một gói tin bị chặn lại, nó sẽ không thể được đọc. Điều này cho phép giao tiếp mạng bảo mật giữa hai điểm đầu cuối của mạch.

## **Luôn Bật (Always On)**

Một trong những thách thức liên quan đến VPN là việc thiết lập kết nối bảo mật. Trong rất nhiều trường hợp, điều này đòi hỏi sự tham gia bổ sung của người-dùng-đầu-cuối, dưới hình thức khởi chạy chương trình, nhập thông tin đăng nhập hoặc cả hai. Điều này đóng vai trò như một trở ngại khi sử dụng, vì người dùng tránh các bước bổ sung. *VPN luôn-bật (VPNs always-on)* là một phương tiện để tránh vấn đề này thông qua việc sử dụng các thông số kết nối và tự động hóa đã-được-thiết-lập-trước. VPN luôn-bật có thể tự định cấu hình và kết nối khi kết nối Internet được phát hiện và cung cấp chức năng VPN mà không cần sự can thiệp của người dùng.



## **MÁCH NƯỚC CHO KỲ THI**

Khi một kết nối Internet được thực hiện, một máy khách VPN luôn-bật sẽ thiết lập một kết nối VPN một cách tự động.

## **Đường hầm Phân tách so với Đường hầm Toàn bộ**

*Đường hầm phân tách* là một dạng VPN trong đó không phải tất cả lưu lượng đều được định tuyến đi qua VPN. Phân tách đường hầm cho phép nhiều đường kết nối, một số thông qua một tuyến đường được bảo vệ như VPN, trong khi lưu lượng truy cập khác từ các nguồn Internet công cộng được định tuyến qua các đường dẫn không-phải-là-VPN. Ưu điểm của việc phân tách đường hầm là khả năng tránh sự tắc nghẽn do tất cả lưu lượng phải được mã hóa qua VPN. Một đường hầm phân tách sẽ cho phép người dùng truy cập riêng tư vào thông tin từ các địa điểm qua VPN và quyền truy cập kém bảo mật hơn vào thông tin từ các địa điểm khác. Điểm bất lợi là các cuộc tấn công từ phía không-phải-VPN của kênh giao tiếp có thể ảnh hưởng đến các yêu cầu lưu lượng từ phía VPN. Một giải

pháp *đường hầm toàn bộ* định tuyển tất cả lưu lượng qua VPN, cung cấp khả năng bảo vệ cho tất cả lưu lượng mạng.

---



**MÁCH NƯỚC CHO KỲ THI** Đối với những câu hỏi dựa-trên-hiệu-suất, việc chỉ đơn giản tìm hiểu về những thuật ngữ liên quan đến VPN và IPSec nói riêng là không đủ. Bạn nên làm quen với thiết lập cấu hình và sử dụng các thành phần IPSec, bao gồm các kiểu cấu hình và việc sử dụng chúng để hỗ trợ cho bảo mật của tổ chức.

### **Truy cập Từ xa và Điểm-nối-Điểm**

Các kết nối giao tiếp *điểm-nối-điểm* là các kết nối mạng đến hai hay nhiều mạng qua một lớp mạng trung gian. Trong hầu hết các trường hợp, mạng trung gian này là Internet hoặc một số mạng công cộng khác. Để bảo mật lưu lượng đi từ điểm này sang điểm khác, mã hóa dưới dạng VPN hoặc đường hầm có thể được sử dụng. Về bản chất, điều này khiến cho tất cả các gói tin giữa các điểm cuối trong hai mạng trở nên không thể đọc được đối với các nút giữa hai địa điểm.

*Truy cập từ xa* là khi một người dùng yêu cầu quyền truy cập vào mạng và tài nguyên của mạng đó nhưng không có khả năng thực hiện một kết nối vật lý. Truy cập từ xa qua đường hầm hoặc VPN có tác dụng tương tự như kết nối hệ thống từ xa với mạng một cách trực tiếp - giống như thế người dùng từ xa chỉ cắm cáp mạng trực tiếp vào máy của họ. Vì vậy, nếu bạn không tin tưởng một máy được kết nối trực tiếp với mạng của mình, bạn không nên sử dụng VPN hoặc đường hầm, vì nếu làm vậy, đó là điều bạn đang thực hiện về mặt logic [*hàm ý là nếu làm vậy thì có nghĩa là đang cung cấp kết nối từ xa cho các máy không được tin cậy*].

---



**MÁCH NƯỚC CHO KỲ THI** Công nghệ tạo đường hầm/VPN là một phương tiện mở rộng một mạng để bao gồm những người dùng từ xa hoặc để kết nối hai địa điểm. Khi kết nối được thực hiện, điều này sẽ giống như các máy được kết nối đang ở trên mạng cục bộ.

### **IPSec**

*IPSec* là một tập hợp các giao thức do IETF phát triển để trao đổi các gói tin một cách an toàn ở lớp mạng (lớp 3) của mô hình tham chiếu OSI (các RFC 2401 - 2412). Mặc dù các giao thức này chỉ hoạt động kết hợp với mạng IP, một khi kết nối *IPSec* đã được thiết lập, có thể tạo đường hầm qua các mạng khác ở các cấp thấp hơn của mô hình OSI. Tập hợp các dịch vụ bảo mật được cung cấp bởi *IPSec* diễn ra ở lớp mạng của mô hình OSI, vì vậy các giao thức lớp cao hơn, chẳng hạn như TCP, UDP, Giao thức Kiểm soát Thông điệp Internet (ICMP), Giao thức Cửa khẩu (BGP), và các giao thức tương tự, không bị thay đổi về mặt chức năng bởi việc triển khai các dịch vụ *IPSec*.

Loạt giao thức *IPSec* có một loạt các dịch vụ mà nó được thiết kế để cung cấp, bao gồm nhưng không giới hạn ở kiểm soát truy cập, tính toàn vẹn không kết nối, tính bảo mật của luồng-lưu-lượng, từ chối các gói được phát lại, bảo mật dữ liệu (mã hóa) và xác thực nguồn gốc dữ liệu. *IPSec* có hai chế độ đã được xác định – truyền tải và đường hầm - cung cấp các mức độ bảo mật khác nhau. *IPSec* cũng có ba chế độ kết nối: host-to-server, server-to-server và host-to-host.

Chế độ truyền tải chỉ mã hóa phần dữ liệu của gói tin, do đó cho phép một người bên ngoài nhìn thấy cả địa chỉ IP nguồn và đích. Chế độ truyền tải bảo vệ các giao thức cấp-cao-hơn được liên kết với một gói tin và bảo vệ dữ liệu đang được truyền nhưng cho phép biết được chính bản thân

quá trình truyền tải. Bảo vệ phần dữ liệu của gói tin được gọi là bảo vệ nội dung.

Chế độ đường hầm cung cấp mã hóa địa chỉ IP nguồn và đích, cũng như dữ liệu của chính nó. Điều này cung cấp khả năng bảo mật cao nhất, nhưng nó chỉ có thể được thực hiện giữa các máy chủ (hoặc bộ định tuyến) IPSec vì đích cuối cùng cần phải được biết để phân phôi. Bảo vệ thông tin tiêu đề được gọi là bảo vệ ngữ cảnh.



**MÁCH NƯỚC CHO KỲ THI** Trong *chế độ truyền tải* (từ-đầu-đến-cuối), việc bảo mật của lưu lượng gói tin được cung cấp bởi máy tính điểm đầu cuối. Trong *chế độ đường hầm* (cổng-đến-cổng), việc bảo mật lưu lượng gói tin được cung cấp giữa các máy nút điểm đầu cuối trong từng mạng và không phải tại máy vật chủ trạm đầu cuối.

Có thể sử dụng cả hai phương pháp tại cùng một thời điểm, chẳng hạn như sử dụng chế độ truyền tải trong mạng của chính mình để đi đến máy chủ IPSec, sau đó là chế độ đường hầm đến mạng của máy chủ đích, kết nối với máy chủ IPSec ở đó, rồi sử dụng phương thức truyền tải từ máy chủ IPSec của mạng mục tiêu đến máy chủ đích. IPSec sử dụng thuật ngữ *liên kết bảo mật (SA)* để mô tả sự kết hợp một chiều giữa thuật toán cụ thể và sự lựa chọn khóa để cung cấp một kênh được bảo vệ. Nếu lưu lượng truy cập là hai chiều, hai SA được cần đến và trên thực tế có thể khác nhau.

## **SSL/TLS**

*Bảo mật Lớp Cổng (SSL)/Bảo mật Lớp Truyền tải (TLS)* là một ứng dụng của công nghệ mã hóa được phát triển cho các giao thức lớp-truyền-tải trên Web. Giao thức này sử dụng các phương pháp mã hóa khóa công

khai để trao đổi một khóa đối xứng để sử dụng trong bảo vệ tính bảo mật và toàn vẹn cũng như tính xác thực. Mọi phiên bản SSL đã không còn được sử dụng nữa do các vấn đề về bảo mật và trong phần lớn các máy chủ thương mại sử dụng SSL/TLS, SSL đã ngừng hoạt động. Vì tính phổ biến của nó, thuật ngữ SSL sẽ tồn tại trong một thời gian khá dài, nhưng về mặt chức năng, nó hiện được thực hiện thông qua TLS. TLS có thể được sử dụng để ảnh hưởng đến VPN giữa một trình duyệt máy khách và máy chủ web và là một trong những phương pháp phổ biến nhất để bảo vệ lưu lượng truy cập web.

Cổng tiêu chuẩn cho SSL và TLS không được xác định vì nó phụ thuộc vào giao thức đang được bảo vệ sử dụng, ví dụ: cổng 80 cho HTTP trở thành cổng 443 khi nó là cho HTTPS. Nếu kết nối dành cho FTP thì FTPS sử dụng cổng TCP 989 và 990.

## **HTML5**

HTML5 là phiên bản hiện tại của tiêu chuẩn giao thức HTML, và phiên bản này đã được phát triển để xử lý nội dung web hiện đại về âm thanh và phim ảnh cũng như để tăng cường khả năng của một trình duyệt để hoạt động mà không cần những tiện ích bổ sung (add-in) như Flash, Java, và các đối tượng trợ giúp trình duyệt cho những chức năng phổ biến. Một trong những lĩnh vực mà việc này đã tăng cường là khả năng kết nối với VPN bằng cách triển khai giải pháp truy cập từ xa dựa-trên-HTML5 bảo mật. Điều này không đòi hỏi Java hoặc các plugin khác, do đó loại bỏ các vấn đề về khả năng tương thích và cập nhật phụ kiện. Vì HTML5 được thiết kế để hoạt động trên một loạt các thiết bị, bao gồm cả nền tảng di động, nên chức năng này có thể nâng cao tính bảo mật trên nhiều nền tảng.



## MÁCH NƯỚC CHO KỲ THI

HTML5 không đòi hỏi các plugin của trình duyệt và được coi là một giải pháp thay thế truy cập từ xa an toàn để sử dụng các kết nối VPN SSL/TLS.

### Giao thức Đường hầm Lớp 2 (L2TP)

*Giao thức Đường hầm Lớp 2 (L2TP)* là một tiêu chuẩn Internet và xuất phát từ giao thức Chuyển tiếp Lớp 2 (Layer 2 Forwarding - L2F), một sáng kiến của Cisco được thiết kế để giải quyết các vấn đề với Giao thức đường hầm Điểm-nối-Điểm (Point-to-Point Tunneling Protocol - PPTP). Trong khi PPTP được thiết kế xoay quanh Giao thức Điểm-nối-Điểm (Point-to-Point Protocol - PPP) và mạng IP, thì L2F (và do đó là L2TP) được thiết kế để sử dụng trên tất cả các loại mạng, bao gồm cả ATM và Frame Relay. Ngoài ra, trong khi PPTP được thiết kế để triển khai trong phần mềm tại thiết bị máy khách, L2TP được hình thành như một triển khai phần cứng bằng cách sử dụng bộ định tuyến hoặc một thiết bị có mục đích đặc biệt. L2TP có thể được thiết lập cấu hình trong phần mềm và nằm trong Dịch vụ Định tuyến và Truy cập Từ xa (Microsoft Routing and Remote Access Service - RRAS) của Microsoft, sử dụng L2TP để tạo ra một VPN.

L2TP hoạt động giống như PPTP, nhưng nó mở ra một số hạng mục để mở rộng. Ví dụ, trong L2TP, các bộ định tuyến có thể được kích hoạt để tập trung lưu lượng VPN qua các đường kết nối có băng thông cao hơn, tạo ra các mạng phân cấp lưu lượng VPN có thể được quản lý một cách hiệu quả hơn trong một doanh nghiệp. L2TP cũng có khả năng sử dụng IPSec và các giao thức mã hóa, mang lại mức độ bảo mật dữ liệu cao hơn. L2TP cũng được thiết kế để hoạt động với các dịch vụ AAA đã được thiết lập như RADIUS và TACACS + để hỗ trợ xác thực, cấp phép và tính toán người

dùng. L2TP được thiết lập thông qua cổng UDP 1701, vì vậy đây là một cổng cần thiết phải mở trên tường lửa hỗ trợ lưu lượng L2TP.

## DNS

*Hệ thống Tên Miền (DNS)* là một giao thức để diễn dịch tên miền thành địa chỉ IP. Khi người dùng nhập một tên miền chẳng hạn như [www.example.com](http://www.example.com), hệ thống DNS sẽ chuyển đổi tên này thành địa chỉ IP là những con số thực [dạng xxx.xxx.xxx.xxx – xxx: từ 0 đến tối đa là 255, ngoại trừ một số địa chỉ đặc biệt]. Các bản ghi DNS cũng được sử dụng để gửi e-mail. Giao thức DNS sử dụng giao thức UDP qua cổng 53 cho các truy vấn tiêu chuẩn, mặc dù các giao thức TCP có thể được sử dụng cho các chuyển giao lớn như chuyển vùng. DNS là một hệ thống phân cấp bao gồm các máy chủ, từ các bản sao cục bộ của các bản ghi, thông qua các nhà cung cấp Internet đến các máy chủ cấp-root. DNS là một trong những giao thức nền tảng chính được sử dụng trên Internet và có liên quan đến hầu hết mọi tra cứu địa chỉ. Vấn đề với DNS là các yêu cầu và phản hồi được gửi ở dạng văn bản rõ ràng và có thể bị giả mạo.

*DNSSEC (Phần mở rộng Bảo mật Hệ thống Tên Miền)* là một tập hợp các phần mở rộng dành cho giao thức DNS, thông qua việc sử dụng mật mã, cho phép xác thực nguồn gốc của dữ liệu DNS, xác thực từ chối sự tồn tại và tính toàn vẹn của dữ liệu nhưng không mở rộng đến tính sẵn sàng hoặc tính bảo mật. Các bản ghi DNSSEC được ký để tất cả các phản hồi DNSSEC được xác thực nhưng không được mã hóa. Điều này ngăn chặn việc các phản hồi DNS trái phép được hiểu là chính xác. Sự từ chối được xác thực về sự tồn tại cũng cho phép trình phân giải xác thực rằng một tên miền nhất định không tồn tại.

Dữ liệu truyền qua cổng UDP 53 có kích thước giới hạn ở 512-byte và các gói tin DNSSEC có thể có kích thước lớn hơn. Vì lý do này, DNSSEC thường sử dụng cổng TCP 53 cho hoạt động của nó. Có khả năng mở rộng kích

thuộc gói UDP lên thành 4096-byte để ứng phó với DNSSEC và điều này đã được đề cập trong RFC 6891.

### Kiểm soát Truy cập Mạng (NAC)

Các mạng bao gồm các máy trạm và máy chủ được kết nối lại. Việc quản lý bảo mật trên mạng bao gồm việc quản lý một loạt các vấn đề không chỉ liên quan đến các phần cứng đã được kết nối khác nhau mà còn liên quan đến phần mềm vận hành các thiết bị đó. Giả sử rằng mạng đã được bảo mật nhưng mỗi kết nối bổ sung đều có rủi ro. Việc quản lý các điểm đầu cuối theo từng-trường-hợp khi chúng kết nối là một phương pháp bảo mật được gọi là *kiểm soát truy cập mạng* (*Network Access Control - NAC*). Có hai phương pháp cạnh tranh chính cùng tồn tại, bao gồm: Bảo vệ Truy cập Mạng (*Network Access Protection - NAP*) là công nghệ của Microsoft để kiểm soát quyền truy cập mạng vào máy chủ máy tính và Kiểm soát Truy cập Mạng (*Network Admission Control - NAC*) là công nghệ của Cisco để kiểm soát truy cập mạng.

Hệ thống NAP của Microsoft dựa trên việc đo lường tình trạng sức khỏe hệ thống của máy đang kết nối, bao gồm các mức độ vá lỗi của hệ điều hành, bảo vệ chống vi-rút và các chính sách hệ thống. NAP lần đầu tiên được sử dụng trong Windows XP Service Pack 3, Windows Vista và Windows Server 2008, và nó đòi hỏi các máy chủ cơ sở hạ tầng bổ sung để triển khai các kiểm tra tình trạng sức khỏe. Hệ thống bao gồm các tác nhân thực thi thẩm tra các máy khách và xác minh các tiêu chí truy cập. Phía máy khách được khởi tạo bắt cứ khi nào kết nối mạng đã được thực hiện. Các tùy chọn phản hồi bao gồm từ chối yêu cầu kết nối và hạn chế quyền truy cập vào một mạng con.

Hệ thống NAC của Cisco được xây dựng dựa trên một thiết bị thực thi các chính sách được chọn bởi quản trị viên hệ thống mạng. Một loạt các giải pháp của bên-thứ-ba có thể giao tiếp với thiết bị, cho phép xác minh toàn

bộ các tùy chọn, bao gồm cài đặt chính sách ứng dụng máy khách, cập nhật phần mềm và tư hình bảo mật của ứng dụng máy khách. Việc sử dụng các thiết bị và phần mềm của bên-thứ-ba khiến cho hệ thống này trở thành một hệ thống có thể mở rộng được trên nhiều loại thiết bị.

Cả Cisco NAC và Microsoft NAP đều không được áp dụng rộng rãi trong các doanh nghiệp. Các phần mềm máy khách đã sẵn sàng nhưng các doanh nghiệp còn chậm chạp trong việc triển khai đầy đủ tại phía máy chủ của công nghệ này. Khái niệm kiểm tra truy cập tự động dựa trên các đặc điểm của thiết bị máy khách vẫn tồn tại ở đây vì nó cung cấp khả năng kiểm soát kịp thời trong thế giới mạng luôn thay đổi của các doanh nghiệp ngày nay. Với sự gia tăng của chính sách “mang theo thiết bị của riêng bạn” (Bring Your Own Device - BYOD) trong các tổ chức, ngày càng có nhiều quan tâm đến việc sử dụng kiểm soát truy cập mạng để hỗ trợ bảo vệ mạng khỏi các thiết bị không an toàn.



## MÁCH NƯỚC CHO KỲ THI

Đối với kỳ thi Security+, NAC đề cập đến *kiểm soát truy cập mạng*. Các giải pháp của Microsoft và Cisco được tham chiếu trong phần này là những ví dụ về các kiểu kiểm soát này – tên gọi và viết tắt của chúng không liên quan đến kỳ thi Security+. Khái niệm về kiểm soát truy cập mạng (NAC) và những gì mà nó thực hiện mới có liên quan và có thể được kiểm tra.

## Có Tác nhân và Không có Tác nhân

Khi nhận ra rằng việc triển khai các tác nhân cho các máy có thể gặp phải vấn đề trong một số trường hợp, các nhà cung cấp cũng đã phát triển các giải pháp không cần tác nhân cho NAC. Thay vì để tác nhân chờ đợi trên máy chủ để kích hoạt và sử dụng, tác nhân có thể hoạt động từ trong chính bản thân mạng đó, kết xuất máy chủ một cách không cần tác

nhân. Trong các giải pháp *dựa-trên-tác-nhân*, mã được lưu trữ trên máy chủ để kích hoạt và sử dụng tại thời điểm kết nối. Trong các giải pháp *không có tác nhân*, mã được lưu trữ trên mạng và được triển khai vào bộ nhớ để sử dụng trong máy yêu cầu kết nối, nhưng bởi vì nó không bao giờ tồn tại trên máy chủ nên nó được gọi là không có tác nhân. Trong hầu hết các trường hợp, không có sự khác biệt thực sự về hiệu suất của các giải pháp tác nhân so với các giải pháp không có tác nhân khi được triển khai một cách đúng đắn. Sự khác biệt thực sự nằm ở vấn đề có các tác nhân nằm trên hộp [máy tính] so với các kết nối mạng liên tục cho không có tác nhân.

NAC không có tác nhân thường được triển khai trong miền Microsoft thông qua bộ điều khiển Active Directory (Active Directory controller). Ví dụ: mã NAC xác minh các thiết bị tuân thủ chính sách truy cập khi miền được người dùng tham gia hoặc khi họ đăng nhập hoặc đăng xuất. NAC không có tác nhân cũng thường được triển khai thông qua việc sử dụng các hệ thống ngăn chặn xâm nhập.



**MÁCH NƯỚC CHO KỲ THI** Các tác nhân NAC được cài đặt trên các thiết bị để kết nối đến các mạng nhằm tạo ra những môi trường mạng an toàn. Với NAC không có tác nhân, mã NAC không lưu trú trên các thiết bị đang kết nối mà là trên hệ thống mạng, và nó được triển khai vào bộ nhớ để sử dụng trong các máy yêu cầu kết nối vào mạng.

### **Quản lý Ngoài-dải-băng-tần (Out-of-band)**

Quản lý một hệ thống trên toàn mạng có thể là trong-dải-tần (in-band) hoặc ngoài-dải-tần (out-of-band). Trong hệ thống quản lý trong-dải-tần, kênh quản lý là kênh giống như kênh dữ liệu. Điều này có ưu điểm trong việc đơn giản hóa kết nối vật lý và nhược điểm là nếu sự cố xảy ra do

các luồng dữ liệu, các lệnh quản lý có thể không truy cập được vào thiết bị. Đối với các thiết bị và dịch vụ mạng quan trọng, kênh quản lý ngoài-dải-tần nên được sử dụng. Các kênh *quản lý ngoài-dải-tần* là các kết nối riêng biệt về mặt vật lý, thông qua các giao diện riêng biệt cho phép quản lý thiết bị một cách chủ động ngay cả khi kênh dữ liệu bị chặn vì lý do nào đó.

### Bảo mật Cổng

Bộ chuyển mạch có thể thực hiện một loạt các chức năng bảo mật khác nhau. Bộ chuyển mạch hoạt động bằng cách di chuyển các gói tin từ kết nối đi vào (inbound) sang kết nối đi ra (outbound). Trong khi di chuyển các gói tin, bộ chuyển mạch có khả năng kiểm tra tiêu đề gói tin và thực thi các chính sách bảo mật. *Bảo mật cổng* là một khả năng được cung cấp bởi bộ chuyển mạch cho phép bạn kiểm soát thiết bị nào và bao nhiêu thiết bị được phép kết nối qua mỗi cổng trên bộ chuyển mạch. Bảo mật cổng hoạt động thông qua việc sử dụng địa chỉ MAC. Mặc dù không hoàn hảo - địa chỉ MAC có thể bị giả mạo – nhưng bảo mật cổng có thể cung cấp chức năng bảo mật mạng hữu ích.

Bảo mật địa chỉ cổng dựa trên các địa chỉ Kiểm soát Truy cập Phương tiện (Media Access Control - MAC) có thể xác định xem một gói được cho phép hay bị chặn khỏi kết nối. Đây là chính chức năng mà tường lửa sử dụng cho chức năng xác định của nó và chính chức năng này là những gì cho phép thiết bị 802.1X hoạt động như một “thiết bị biên”.

Bảo mật cổng có ba biến thể:

- **Học tĩnh (Static learning)** Một địa chỉ MAC cụ thể được gán cho một cổng. Điều này rất hữu ích cho các kết nối phần cứng cố định và chuyên dụng. Điểm bất lợi là địa chỉ MAC cần phải được biết và

lập trình trước, điều này tốt cho các kết nối đã được xác định nhưng không tốt cho các kết nối đang truy cập.

- **Học động (Dynamic learning)** Cho phép bộ chuyển mạch xác định địa chỉ MAC khi chúng kết nối. Học động rất hữu ích khi bạn dự kiến một số lượng máy nhỏ và giới hạn kết nối với một cổng.
- **Học liên tục (Sticky learning)** Cho phép nhiều thiết bị truy cập vào một cổng nhưng cũng lưu trữ thông tin trong bộ nhớ vẫn tiếp tục tồn tại qua các lần khởi động lại. Điều này ngăn chặn việc kẻ tấn công thay đổi các cài đặt thông qua việc chuyển đổi nguồn của bộ chuyển mạch.

### Ngăn chặn Bảo Quảng bá

Một trong số các hình thức tấn công là gây ngập lụt. Có rất nhiều kiểu tấn công lũ lụt: lũ ping, lũ SYN, lũ ICMP (các cuộc tấn công của Xì Trum) và lũ lụt do lưu lượng. Các cuộc tấn công ngập lụt được sử dụng như một hình thức từ chối dịch vụ (DoS) đối với mạng hoặc hệ thống. Việc phát hiện ra các cuộc tấn công ngập lụt là tương đối dễ dàng, nhưng sẽ có sự khác biệt giữa việc phát hiện cuộc tấn công và giảm nhẹ cuộc tấn công. Ngập lụt có thể được quản lý một cách chủ động thông qua việc giảm kết nối hoặc quản lý lưu lượng. *Bảo vệ [chống] lũ lụt* hành động bằng cách quản lý các luồng lưu lượng. Bằng cách theo dõi tốc độ lưu lượng và tỷ lệ phần trăm băng thông bị chiếm dụng bởi lưu lượng quảng bá, lưu lượng đa hướng và đơn hướng, bộ phận bảo vệ chống ngập có thể phát hiện được khi nào cần chặn lưu lượng để quản lý lũ lụt.



### MÁCH NƯỚC CHO KỲ THI

Bảo vệ [chống] lũ lụt thường được triển khai trên các tường lửa và các giải pháp IDS/IPS để ngăn chặn các cuộc tấn công DoS và DDoS.

## Bảo vệ Đơn vị Dữ liệu Giao thức Cầu nối (BPDU)

Để quản lý Giao thức Spanning Tree (STP), các thiết bị và các bộ chuyển mạch có thể sử dụng các gói tin Đơn vị Dữ liệu Giao thức Cầu nối (Bridge Protocol Data Units – BPDU). Đây là những thông báo được tạo ra thủ công một cách đặc biệt với các khung có chứa thông tin về Giao thức Spanning Tree. Vấn đề với các gói BPDU là, trong một số trường hợp cần thiết, việc sử dụng chúng dẫn đến việc tính toán lại STP và điều này làm tiêu tốn tài nguyên. Một kẻ tấn công có thể phát hành nhiều gói BPDU cho một hệ thống để buộc hệ thống phải thực hiện nhiều phép tính lại và đóng vai trò như một cuộc tấn công từ chối dịch vụ mạng. Để ngăn chặn hình thức tấn công này, các thiết bị biên có thể được thiết lập cấu hình với các bộ phận bảo vệ *Đơn vị Dữ liệu Giao thức Cầu nối (BPDU)* để phát hiện và ngăn chặn các gói này. Mặc dù điều này giúp loại bỏ việc sử dụng chức năng này ở một số vị trí, nhưng việc bảo vệ kết quả là đáng giá với sự tổn thất nhỏ của chức năng.

## Ngăn chặn Lặp

Các thiết bị chuyển mạch hoạt động ở Lớp 2 của mô hình tham chiếu OSI và ở cấp độ này, không có cơ chế đếm ngược để tiêu diệt các gói bị kẹt trong các vòng lặp hoặc trên các đường dẫn sẽ không bao giờ phân giải. Điều này có nghĩa là cần có một cơ chế để *ngăn chặn vòng lặp*. Trên lớp 3 [của mô hình OSI], một bộ đếm thời-gian-tồn-tại (time-to-live - TTL) được sử dụng, nhưng không có một bộ đếm tương tự trên lớp 2. Không gian lớp 2 hoạt động như một lưới, nơi có khả năng là việc bổ sung thêm một thiết bị mới có thể tạo ra các vòng lặp trong các kết nối thiết bị hiện có. Open Shortest Path First (OSPF) là một giao thức định tuyến trạng-thái-liên-kết thường được sử dụng giữa các cửa ngõ trong một hệ thống tự trị duy nhất. Để ngăn chặn các vòng lặp, một công nghệ được gọi là spanning tree được sử dụng bởi hầu như tất cả các thiết bị chuyển mạch. STP cho phép nhiều đường dẫn dự phòng và đồng thời để ngắt các vòng

lặp nhằm đảm bảo một hình mẫu quảng bá thích hợp. STP là một giao thức lớp liên kết dữ liệu và được chấp thuận trong các tiêu chuẩn IEEE 802.1D, 802.1w, 802.1s và 802.1Q. Nó hoạt động bằng cách cắt bớt các kết nối không phải là một phần của cây (tree) bao trùm kết nối tất cả các nút. Các thông điệp STP được mang trong các khung BPDU được mô tả trong phần trước.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng bảo vệ BPDU, lọc MAC và phát hiện lặp là tất cả những cơ chế được sử dụng để mang lại sự bảo mật cho cổng. Hãy tìm hiểu sự khác biệt giữa những hoạt động của chúng. Lọc MAC xác minh địa chỉ MAC trước khi cho phép một kết nối, bảo vệ BPDU ngăn chặn việc giả mạo các gói tin BPDU, và phát hiện lặp phát hiện ra các vòng lặp trong các mạng cục bộ.

### **Snooping Giao thức Cấu hình Máy chủ Động (DHCP)**

Khi quản trị viên thiết lập mạng, họ thường gán địa chỉ IP cho các hệ thống bằng một trong hai cách: tĩnh hoặc động thông qua DHCP. Việc gán địa chỉ IP tĩnh khá đơn giản: quản trị viên quyết định địa chỉ IP nào sẽ được gán cho máy chủ hoặc PC nào và địa chỉ IP đó vẫn được gán cho hệ thống đó cho đến khi quản trị viên quyết định thay đổi địa chỉ IP đó. Phương pháp phổ biến khác là thông qua Giao thức Cấu hình Máy chủ Động (DHCP). Trong DHCP, khi hệ thống khởi động hoặc được kết nối với hệ thống mạng, nó sẽ gửi một truy vấn quảng bá tìm kiếm máy chủ DHCP. Tất cả các máy chủ DHCP đang có sẵn đều sẽ trả lời yêu cầu này. Nếu có nhiều hơn một máy chủ DHCP đang hoạt động trong mạng, máy khách sử dụng máy chủ có phản hồi đến với họ trước. Từ máy chủ DHCP này, máy khách sau đó nhận được chỉ định địa chỉ. DHCP rất phổ biến trong môi

trường người dùng lớn, nơi chi phí cho việc gán và theo dõi địa chỉ IP giữa hàng trăm hoặc hàng nghìn hệ thống của người dùng là cực kỳ cao.

Điểm yếu của việc sử dụng phản hồi đầu tiên nhận được cho phép một máy chủ DNS giả mạo cấu hình lại mạng. Một máy chủ DHCP giả mạo có thể định tuyến máy khách đi đến một cửa ngõ khác, một cuộc tấn công được gọi là giả mạo DHCP. Những kẻ tấn công có thể sử dụng một cửa ngõ giả để ghi lại quá trình truyền dữ liệu, lấy được thông tin nhạy cảm, trước khi gửi dữ liệu đến đích dự định của nó, được gọi là một cuộc tấn công người-trung-gian. Địa chỉ không chính xác có thể dẫn đến một cuộc tấn công DoS chặn các dịch vụ mạng chính lại. *Theo dõi giao thức Cấu hình Máy chủ Động (DHCP)* là một biện pháp phòng thủ chống lại kẻ tấn công đang cố gắng sử dụng thiết bị DHCP giả mạo. DHCP snooping ngăn các máy chủ DHCP độc hại thiết lập giao tiếp bằng cách kiểm tra các phản hồi DHCP ở cấp độ chuyển mạch và không gửi các phản hồi từ các máy chủ DHCP trái phép. Phương pháp này được trình bày chi tiết trong RFC 7513, do Cisco là đồng tác giả và được áp dụng bởi nhiều nhà cung cấp thiết bị chuyển mạch.

### **Lọc Kiểm soát Truy cập Phương tiện (MAC)**

*Lọc MAC* là việc tiếp nhận có chọn lọc các gói tin dựa trên một danh sách các địa chỉ Kiểm soát Truy cập Phương tiện (MAC) đã được phê duyệt. Được sử dụng trên các thiết bị chuyển mạch, phương pháp này được sử dụng để cung cấp một phương tiện xác thực máy. Trong các mạng có dây, điều này được hưởng sự bảo vệ của các dây dẫn, khiến cho việc đánh chặn các tín hiệu để xác định địa chỉ MAC của chúng trở nên khó khăn. Trong mạng không dây, cơ chế tương tự này gặp phải thực tế là kẻ tấn công có thể nhìn thấy địa chỉ MAC của tất cả lưu lượng truy cập đến và đi từ điểm truy cập, sau đó có thể giả mạo địa chỉ MAC được phép giao tiếp qua điểm truy cập.



**MÁCH NƯỚC CHO KỲ THI** Lọc MAC có thể được sử dụng trên các điểm truy cập không dây nhưng có thể bị vượt qua bởi những kẻ tấn công đang quan sát các địa chỉ MAC đã được chấp thuận và giả mạo các địa chỉ MAC được chấp thuận đối với các card không dây.

### **Thiết bị Mạng (Network Appliances)**

*Thiết bị mạng* là các máy móc cung cấp các dịch vụ trên một mạng. Rất nhiều chức năng dựa trên mạng có thể được quản lý một cách hiệu quả thông qua các thiết bị mạng. Các chức năng bảo mật như máy chủ jump, hệ thống phát hiện xâm nhập dựa-trên-mạng, điểm cuối VPN, bộ thu thập và bộ tổng hợp là một số ví dụ phổ biến. Các phần tiếp theo chứa thông tin về những gì đã được xác định một cách cụ thể trong mục tiêu của Security+.

### **Máy chủ Jump**

*Máy chủ jump* là một hệ thống được tăng cường bảo mật trên mạng được sử dụng một cách đặc biệt để truy cập vào các thiết bị trong một vùng bảo mật riêng biệt. Để ai đó bên ngoài mạng truy cập vào những tài nguyên được bảo vệ bên trong mạng, trước tiên họ kết nối với máy chủ jump và các hoạt động của họ với các dịch vụ nội bộ được thực hiện thông qua kết nối đó. Do việc giám sát và tăng cường cụ thể, một máy chủ jump có thể hoạt động như một giải pháp thay thế an toàn hơn việc cho phép truy cập trực tiếp từ bên ngoài. Mức độ chức năng thông qua máy chủ jump có thể được kiểm soát và hoạt động có thể được theo dõi một cách cụ thể để phát hiện và ngăn chặn các cuộc tấn công.



**MÁCH NƯỚC CHO KỲ THI** Các máy chủ jump là những hệ thống đã được tăng cường bảo mật thường được sử dụng để bảo vệ và cung cấp một phương tiện để truy cập vào những nguồn tài nguyên, ví dụ như trong một mạng con đã được sàng lọc.

### **Máy chủ Proxy**

Mặc dù không phải hoàn toàn là một công cụ bảo mật nhưng một *máy chủ giám quản (proxy)* có thể được sử dụng để lọc ra lưu lượng truy cập không mong muốn và ngăn nhân viên truy cập các trang web độc hại tiềm ẩn. Một máy chủ proxy nhận các yêu cầu từ một hệ thống máy khách và chuyển tiếp chúng đến máy chủ đích dưới danh nghĩa của máy khách. Các loại máy chủ proxy khác nhau được mô tả trong các phần dưới đây.

Việc triển khai một giải pháp proxy trong môi trường mạng thường được thực hiện bằng cách thiết lập proxy và yêu cầu tất cả các hệ thống máy khách định cấu hình trình duyệt của họ sử dụng proxy hoặc bằng cách triển khai một proxy ngăn chặn chủ động để chặn tất cả các yêu cầu mà không đòi hỏi cấu hình phía-máy-khách.

Xét từ góc độ bảo mật, proxy hữu ích nhất ở khả năng kiểm soát và lọc các yêu cầu gửi đi. Bằng cách hạn chế các loại nội dung và trang web mà nhân viên có thể truy cập từ các hệ thống của công ty, nhiều quản trị viên hy vọng sẽ tránh được việc thất thoát dữ liệu của công ty, hệ thống bị xâm nhập và lây nhiễm từ các trang web độc hại. Quản trị viên cũng sử dụng proxy để thực thi các chính sách sử dụng được chấp nhận của công ty và theo dõi việc sử dụng tài nguyên của công ty.

## Chuyển tiếp

Các [máy chủ] proxy có thể hoạt động theo hai hướng. Một *proxy chuyển tiếp* hoạt động để chuyển tiếp các yêu cầu cho các máy chủ dựa trên một loạt các tham số khác nhau, như đã được mô tả trong những phần khác của quyển sách này. Các máy chủ proxy chuyển tiếp có thể được sử dụng để vượt qua những giới hạn của tường lửa, đóng vai trò như một máy chủ bộ đệm, và thay đổi địa chỉ IP của bạn (hữu ích hơn trước khi NAT được sử dụng một cách rộng rãi). Các máy chủ proxy chuyển tiếp có thể được triển khai bởi những kẻ tấn công để khiến người dùng sử dụng chúng “cho mục đích lưu bộ nhớ đệm” dưới chiêu bài tăng tốc các kết nối, khi, và trong thực tế, chúng thực sự làm chậm kết nối và tạo ra một kịch bản tấn công người-trung-gian.

## Đảo ngược

Một *proxy đảo ngược* thường được cài đặt trên phía máy chủ của kết nối mạng, thường đặt trước một nhóm các máy chủ web, và can thiệp vào mọi yêu cầu web được gửi đến. Nó có thể thực hiện một số các chức năng, bao gồm lọc lưu lượng, giải mã Bảo mật Lớp Cổng (SSL)/Bảo mật Lớp Truyền tải (TLS), phân phõi những nội dung tĩnh phổ biến như đồ họa, và thực hiện cân bằng tải.



## MÁCH NƯỚC CHO KỲ THI

Một proxy chuyển tiếp sẽ đổi-diện-với-Internet và hoạt động dưới danh nghĩa của máy khách. Nó bảo vệ máy khách. Một proxy đảo ngược đổi mặt với nội bộ và hoạt động dưới danh nghĩa của máy chủ mà nó đang bảo vệ.

## Hệ thống Phát hiện Xâm nhập dựa-trên-Mạng (NIDS)/Hệ thống Ngăn chặn Xâm nhập dựa-trên-Mạng (NIPS)

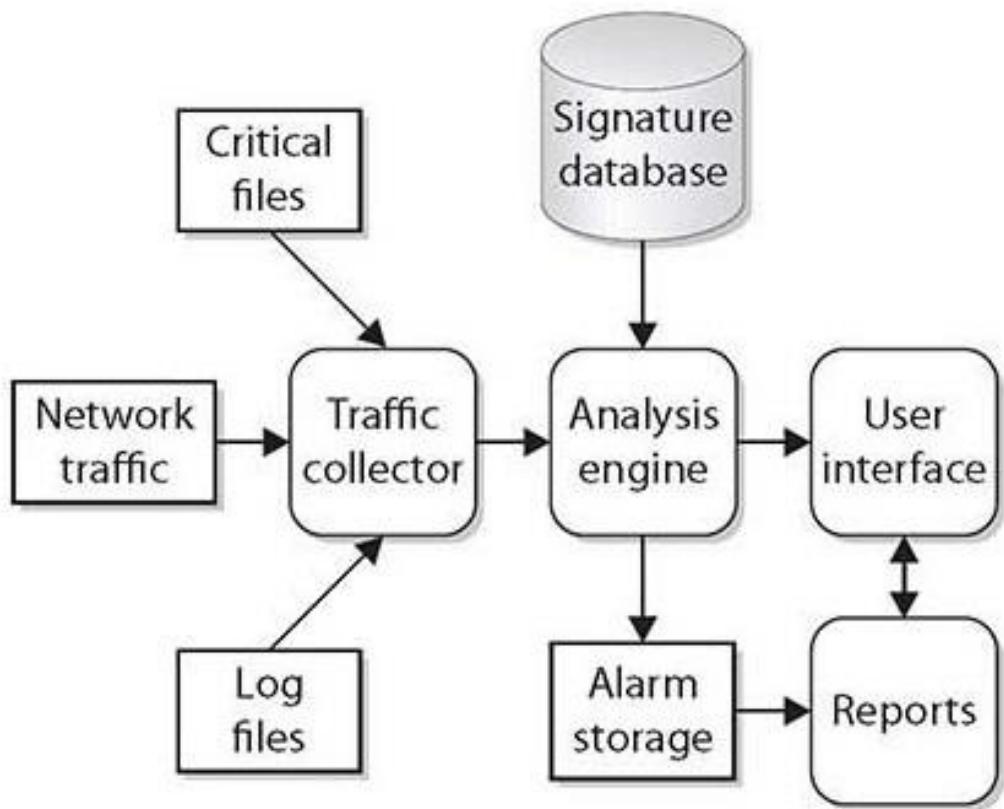
*Hệ thống phát hiện xâm nhập dựa-trên-mạng (NIDS)* được thiết kế để phát hiện, ghi lại nhật ký và ứng phó với việc sử dụng máy chủ hoặc mạng trái phép, cả trong thời gian thực và sau khi xảy ra trong thực tế. NIDS sẵn có từ rất nhiều nhà cung cấp và là một phần thiết yếu của bảo mật mạng. Các hệ thống này được triển khai trong phần mềm, nhưng trong các hệ thống lớn cũng cần phải có phần cứng chuyên dụng.

*Hệ thống ngăn chặn xâm nhập dựa-trên-mạng (NIPS)* có cốt lõi là hệ thống phát hiện xâm nhập. Tuy nhiên, trong khi NIDS chỉ có thể cảnh báo khi lưu lượng mạng khớp với một bộ quy tắc xác định thì NIPS còn có thể thực hiện các hành động khác. NIPS có thể thực hiện những hành động trực tiếp để ngăn chặn một cuộc tấn công, với các hành động của nó được chi phối bởi các quy tắc. Bằng cách tự động hóa việc ứng phó, NIPS rút ngắn đáng kể thời gian phản ứng từ khi phát hiện đến khi hành động.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhận thức rằng NIPS có tất cả các đặc điểm giống như NIDS nhưng, không giống như NIDS, NIPS có thể tự động ứng phó với các sự kiện nhất định (ví dụ, bằng cách thiết lập lại kết nối TCP) mà không cần sự can thiệp của người vận hành.

Dù là dựa-trên-mạng hay dựa-trên-máy-vật-chủ, một IDS sẽ thường được cấu thành từ một số các thành phần chuyên biệt hoạt động cùng nhau, như được minh họa trong Hình 19-3. Những thành phần này thường là luận lý và dựa-trên-phần mềm thay vì là những thiết bị vật lý và sẽ khác nhau một chút giữa các nhà cung cấp, và giữa các sản phẩm. Thông thường một IDS sẽ có những thành phần logic dưới đây:



**Hình 19-3** Mô tả logic các thành phần của IDS

- **Bộ thu thập lưu lượng (hoặc cảm biến)** Thành phần này thu thập các hoạt động/sự kiện để IDS kiểm tra. Trên một IDS dựa-trên-máy-chủ, đây có thể là các tập tin nhật ký, các nhật ký kiểm toán, hoặc lưu lượng đi đến/từ hoặc rời khỏi một hệ thống cụ thể. Trên một IDS dựa-trên-mạng, đây thường là một cơ chế sao chép lưu lượng của liên kết mạng – về cơ bản hoạt động giống như một trình bắt gói tin. Thành phần này thường được gọi là một cảm biến.
- **Động cơ phân tích (bộ phân tích)** Thành phần này kiểm tra lưu lượng mạng đã được thu thập và so sánh nó với những hình mẫu của các hoạt động độc hại hoặc đáng ngờ đã biết được lưu trữ trong cơ sở dữ liệu chữ ký. Động cơ phân tích này là “bộ não” của IDS.

- **Cơ sở dữ liệu chữ ký** Cơ sở dữ liệu chữ ký là một bộ sưu tập các hình mẫu và định nghĩa các hoạt động độc hại hoặc đáng ngờ đã biết.
- **Giao diện người dùng và báo cáo** Thành phần này tương tác với các yếu tố con người, đưa ra các cảnh báo khi thích hợp và cung cấp cho người dùng một phương tiện để tương tác với và vận hành IDS.

Hầu hết các IDS có thể được tinh chỉnh để phù hợp với một môi trường cụ thể. Các chữ ký nhất định có thể được tắt đi để nói cho IDS biết rằng không cần tìm kiếm những kiểu lưu lượng nhất định. Ví dụ, nếu bạn đang vận hành một môi trường thuần túy Linux, bạn có thể sẽ không muốn thấy những cảnh báo dựa-trên-Windows, vì chúng sẽ không ảnh hưởng đến các hệ thống của bạn. Ngoài ra, tính nghiêm trọng của các mức độ cảnh báo có thể được điều chỉnh tùy thuộc vào việc bạn quan tâm đến những kiểu lưu lượng nhất định như thế nào. Một số IDS cũng sẽ cho phép người dùng loại bỏ những hình mẫu hoạt động nhất định từ những máy chủ cụ thể. Nói cách khác, bạn có thể yêu cầu IDS bỏ qua thực tế rằng một số các hệ thống tạo ra những lưu lượng trông giống như hoạt động độc hại, nhưng thực tế những hệ thống đó không phải là độc hại.

Các NIDS/NIPS có thể được chia thành 3 thể loại, dựa trên những phương pháp phát hiện chính được sử dụng: dựa trên chữ ký, dựa trên khám phá/hành vi, và dựa trên sự bất thường. Chúng sẽ được mô tả trong các phần tiếp theo dưới đây.

### Dựa trên chữ ký

Mô hình này dựa trên một bộ các hình mẫu đã được xác định trước (được gọi là các *chữ ký*). IDS phải nhận biết được hành vi nào được coi là “xấu” trước khi nó có thể xác định và hành động tùy theo lưu lượng độc hại

hoặc đáng ngờ. Các hệ thống *dựa-trên-chữ-ký* hoạt động bằng cách đối chiếu các chữ ký trong luồng lưu lượng mạng với các hình mẫu đã được xác định được lưu trữ trong hệ thống. Các hệ thống *dựa-trên-chữ-ký* có thể rất nhanh và chính xác với tỷ lệ dương-tính-giả thấp. Điểm yếu của các hệ thống *dựa-trên-chữ-ký* là rằng chúng phụ thuộc vào việc có được các định nghĩa chữ ký chính xác từ trước, và khi số lượng các chữ ký gia tăng, điều này tạo ra một vấn đề về khả năng mở rộng.



**MÁCH NƯỚC CHO KỲ THI** Âm tính giả thường xảy ra khi các cảnh báo nêu được tạo ra đã không xảy ra. Dương tính giả diễn ra khi những hành vi được kỳ vọng được xác định là độc hại.

### Dựa trên khám phá/hành vi

Mô hình *hành vi* dựa trên một bộ “hành vi bình thường” đã được thu thập – những gì nên diễn ra trên mạng và được xem là lưu lượng “bình thường” hoặc “có thể chấp nhận được”. Hành vi không phù hợp với các thể loại hoặc hình mẫu hoạt động “bình thường” được xem là độc hại hoặc đáng ngờ. Mô hình này có thể có khả năng phát hiện ra những cuộc tấn công zero-day hoặc chưa được công bố nhưng tạo ra một lượng tỷ lệ dương-tính-giả cao do bất kỳ hình mẫu lưu lượng nào nào đều có thể bị gán nhãn là “đáng ngờ”.

Mô hình *khám phá* sử dụng trí tuệ nhân tạo (AI) để phát hiện các lưu lượng xâm nhập và lưu lượng độc hại. Mô hình này thường được triển khai thông qua các thuật toán để giúp cho một IDS quyết định xem liệu một hình mẫu lưu lượng có phải là độc hại hay không. Ví dụ, một URL có chứa một ký tự được lặp lại 10 lần có thể được xem là “lưu lượng” xấu với một chữ ký duy nhất. Với mô hình khám phá, IDS sẽ tìm hiểu xem nếu 10 ký tự lặp lại là xấu, 11 vẫn là xấu và thậm chí 20 sẽ còn tệ hơn. Việc

triển khai logic mờ (fuzzy) này cho phép mô hình này rơi vào đâu đó giữa các mô hình dựa-trên-chữ-ký và dựa-trên-hành-vi.

## Sự bất thường

Mô hình nhận diện này tương tự như phương pháp dựa-trên-hành-vi. Đầu tiên, IDS được dạy rằng lưu lượng “bình thường” trông sẽ như thế nào và sau đó, tìm kiếm những sai lệch từ những hình mẫu “bình thường” đó. Một *bất thường* là một sai lệch so với một hình mẫu hoặc hành vi được kỳ vọng. Những bất thường cụ thể cũng có thể được xác định, chẳng hạn như các câu lệnh Linux được gửi đến các hệ thống dựa-trên-Windows và được triển khai thông qua một công cụ dựa-trên-AI để mở rộng tính tiện ích của các định nghĩa cụ thể.



**MÁCH NƯỚC CHO KỲ THI** Phát hiện bất thường xác định những sai lệch so với hành vi bình thường.

## Nội tuyển so với Thụ động

Sự phân biệt giữa NIDS/NIPS trong-dải-tần và ngoài-dải-tần tương tự như sự phân biệt giữa cảm biến nội tuyển và cảm biến thụ động. Một NIDS/NIPS *trong-dải-tần* là một cảm biến nội tuyển được kết hợp với NIDS/NIPS để đưa ra quyết định “trong dải tần” của nó và ban hành những thay đổi thông qua cảm biến. Điều này có ưu điểm là tính bảo mật cao, nhưng nó cũng có những tác động liên quan đến mức độ lưu lượng và độ phức tạp của lưu lượng. Các giải pháp trong-dải-tần hoạt động khá hiệu quả để bảo vệ các phân đoạn mạng có các hệ thống giá-trị-cao và một số loại lưu lượng hạn chế, chẳng hạn như trước một tập hợp các máy chủ cơ sở dữ liệu với dữ liệu công ty cực kỳ quan trọng, nơi các kiểu truy cập duy nhất sẽ là thông qua các kết nối cơ sở dữ liệu .

Một hệ thống ngoài-dài-tần dựa vào một cảm biến *thụ động*, hoặc tập hợp các cảm biến thụ động và có ưu điểm là khả năng phát hiện linh hoạt hơn đối với nhiều loại lưu lượng hơn. Điểm bất lợi là sự chậm trễ trong việc phản ứng với các phát hiện dương tính, vì lưu lượng đã được chuyển đến máy chủ đầu cuối.

## HSM

Một *mô-đun bảo mật phần cứng* (*hardware security module – HSM*) là một thiết bị được sử dụng để quản lý hoặc lưu trữ các khóa mã hóa. Nó cũng có thể hỗ trợ cho các hoạt động mật mã chặng hạn như mã hóa, băm, hoặc áp dụng các chữ ký kỹ thuật số. Các HSM thường là các thiết bị ngoại vi, được kết nối qua cổng USB hoặc một kết nối mạng. HSM có các cơ chế bảo-vệ-chống-giả-mạo để ngăn ngừa việc truy cập vật lý vào những bí mật mà chúng đang bảo vệ. Do thiết kế chuyên biệt của chúng, chúng có thể mang lại những lợi thế hiệu suất đáng kể hơn các máy tính có mục-đích-chung khi thực hiện các hoạt động mật mã. Khi một doanh nghiệp có những hoạt động mật mã đáng kể, các HSM có thể mang lại tính hiệu quả.



**MÁCH NƯỚC CHO KỲ THI** Việc lưu trữ khóa riêng tư ở bất kỳ nơi đâu trên một hệ thống được nối mạng là một nguyên nhân dẫn đến tổn thất. Các HSM được thiết kế để cho phép sử dụng khóa mà không làm lộ khóa trước hàng loạt các mối đe dọa dựa-trên-máy-chủ.

## Các Cảm biến

Các *cảm biến* là những thiết bị thu thập dữ liệu và hành động dựa trên những dữ liệu này. Có rất nhiều loại cảm biến và nhiều kịch bản lắp đặt khác nhau. Mỗi loại cảm biến là khác nhau, và không có loại cảm biến duy nhất nào có thể cảm nhận được mọi thứ. Các cảm biến có thể được

chia thành hai loại dựa trên vị trí mà chúng được lắp đặt: trên mạng và trên máy vật chủ. Các cảm biến dựa-trên-mạng có thể tạo ra phạm vi bao phủ trên nhiều máy nhưng bị giới hạn bởi kỹ thuật lưu lượng đối với các hệ thống mà các gói tin truyền qua chúng. Chúng có thể gặp vấn đề với lưu lượng được mã hóa vì nếu gói tin đã được mã hóa và chúng không thể đọc được, các cảm biến sẽ không thể hành động dựa trên các gói tin đó. Mặt khác, các cảm biến dựa-trên-mạng có kiến thức hạn chế về những gì đang được thực hiện trên các máy chủ mà chúng đang quan sát, do đó, phân tích cảm biến bị hạn chế trong khả năng của chúng trong việc đưa ra quyết định chính xác về nội dung. Cảm biến dựa-trên-máy-vật-chủ cung cấp thông tin cụ thể và chính xác hơn liên quan đến những gì máy vật chủ đang nhìn thấy và đang thực hiện, nhưng chúng chỉ giới hạn ở phạm vi máy vật chủ đó. Một ví dụ điển hình về sự khác biệt trong vị trí và khả năng của cảm biến nhận thấy trong hệ thống phát hiện xâm nhập dựa-trên-máy-vật-chủ và hệ thống phát hiện xâm nhập dựa-trên-mạng.

Các cảm biến có một số hành động khác nhau mà chúng có thể thực hiện: chúng có thể báo cáo về những gì chúng quan sát được, chúng có thể sử dụng nhiều lần đọc để đối chiếu với một hình mẫu và tạo ra sự kiện và chúng có thể hoạt động dựa trên các quy tắc bị bài trừ. Không phải tất cả các cảm biến đều có thể thực hiện tất cả các hành động và việc áp dụng các cảm biến cụ thể là một phần của chiến lược triển khai giám sát và kiểm soát. Chiến lược triển khai này phải xem xét kỹ thuật lưu lượng mạng, phạm vi hoạt động và những hạn chế khác.

### **Các Bộ thu thập**

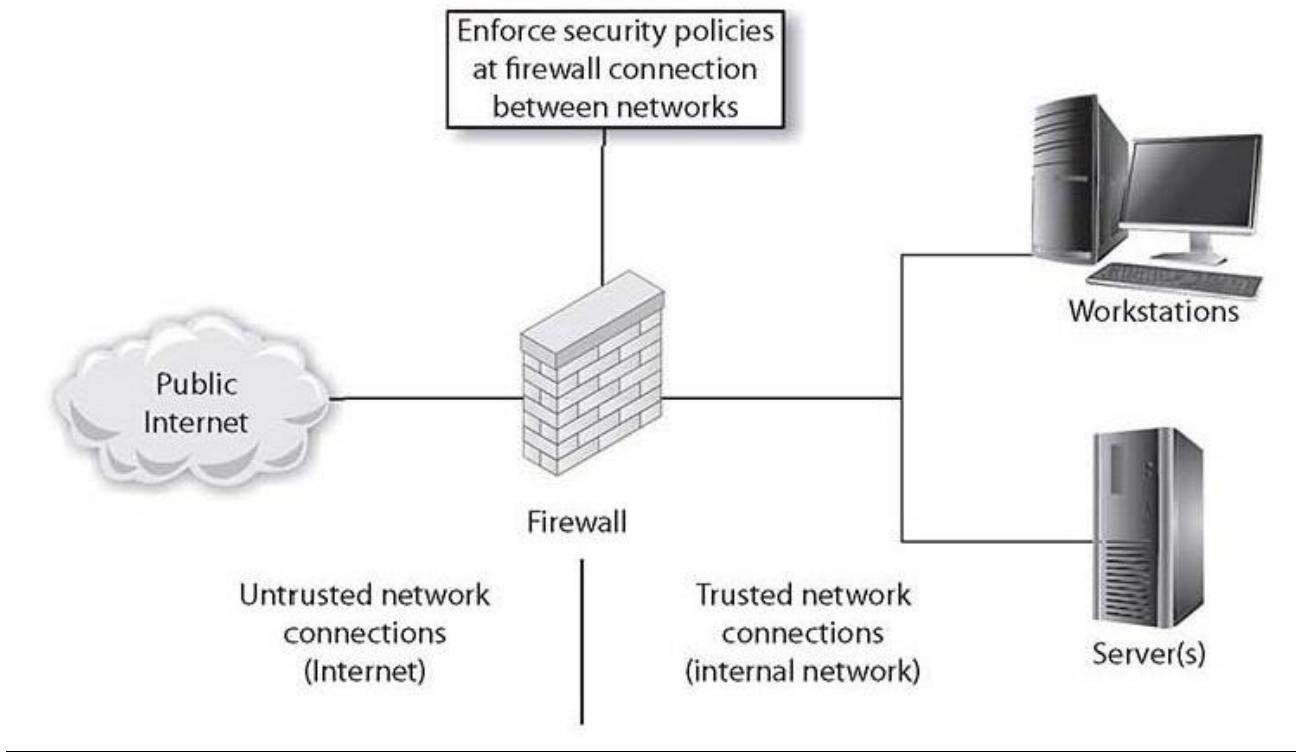
Các *bộ thu thập* là các cảm biến, hoặc các bộ tập trung kết hợp nhiều cảm biến để thu thập dữ liệu để xử lý bởi các hệ thống khác. Các bộ thu thập cũng phải tuân theo các quy tắc và giới hạn về vị trí giống như các cảm biến.

## Các Bộ tổng hợp

Một *bộ tổng hợp* là một thiết bị nhận được nhiều đầu vào và kết hợp chúng thành một đầu ra duy nhất. Hãy coi nó như một loại thiết bị nhiều-một (many-to-one). Nó được đặt ở thượng nguồn của vô số thiết bị và có thể thay thế cho một bộ định tuyến hoặc một bộ chuyển mạch lớn hơn nhiều. Hãy giả sử rằng bạn có mười người dùng trên mỗi tầng trong sô ba tầng. Bạn có thể đặt một bộ chuyển mạch 16-cổng trên từng tầng, sau đó sử dụng ba cổng bộ định tuyến. Nay giờ, hãy tạo ra mười tầng gồm mười người dùng và bạn đang sử dụng mười cổng trên bộ định tuyến của mình cho mười tầng. Một bộ chuyển mạch tổng hợp sẽ giảm điều này xuống một kết nối, đồng thời mang lại sự chuyển đổi giữa những người dùng nhanh hơn so với bộ định tuyến. Các thiết bị quản lý lưu lượng này được định vị dựa trên cấu trúc liên kết bố trí mạng để hạn chế việc sử dụng bộ định tuyến không cần thiết.

## Tường lửa

Một *tường lửa* có thể là phần cứng, phần mềm hoặc một kết hợp của những gì có mục đích là thực thi một bộ các chính sách bảo mật mạng trên các kết nối mạng. Nó giống như một bức tường có cửa sổ: bức tường dùng để ngăn mọi thứ ra ngoài, ngoại trừ những thứ được phép thông qua cửa sổ (xem Hình 19-4). Các chính sách bảo mật mạng hoạt động giống như tấm kính trong cửa sổ: chúng cho phép một số thứ đi qua, chẳng hạn như ánh sáng, trong khi chặn lại những thứ khác, chẳng hạn như không khí. Trung tâm của tường lửa là tập hợp các chính sách bảo mật mà nó thực thi. Cấp quản lý xác định những gì được phép dưới dạng lưu lượng mạng giữa các thiết bị và các chính sách này được sử dụng để xây dựng bộ quy tắc cho các thiết bị tường lửa được sử dụng để lọc lưu lượng mạng trên toàn bộ mạng.



**Hình 19-4** Một tường lửa hoạt động như thế nào

Các chính sách bảo mật là các quy tắc xác định lưu lượng nào được phép và lưu lượng nào bị chặn hoặc bị từ chối. Những quy tắc không phải là các quy tắc chung và có nhiều bộ quy tắc khác nhau được tạo ra cho một tổ chức với nhiều kết nối. Ví dụ, một máy chủ web được kết nối với Internet có thể được định cấu hình để chỉ cho phép lưu lượng truy cập trên cổng 80 cho HTTP và có tất cả các cổng khác bị chặn. Máy chủ email có thể chỉ có các cổng cần thiết để mở email, còn các cổng khác sẽ bị chặn. Tường lửa mạng có thể được lập trình để chặn tất cả lưu lượng truy cập vào máy chủ web ngoại trừ lưu lượng truy cập cổng 80 và chặn tất cả lưu lượng liên kết đến máy chủ email ngoại trừ cổng 25. Theo cách này, tường lửa hoạt động như một bộ lọc bảo mật, cho phép kiểm soát lưu lượng mạng, theo máy, theo cổng và trong một số trường hợp dựa trên chi tiết cấp-ứng-dụng. Chìa khóa để thiết lập các chính sách bảo mật

cho tường lửa cũng giống như đối với các chính sách bảo mật khác - nguyên tắc quyền truy cập ít nhất: chỉ cho phép truy cập cần thiết cho một chức năng, chặn hoặc từ chối tất cả chức năng không cần thiết. Cách thức một tổ chức triển khai tường lửa của mình xác định những gì cần thiết cho các chính sách bảo mật cho mỗi tường lửa.

Như sẽ được thảo luận sau này, cấu trúc bảo mật sẽ xác định những thiết bị mạng nào được sử dụng tại những điểm nào trong một hệ thống mạng. Tối thiểu, các kết nối của tổ chức của bạn đến Internet nên đi qua một tường lửa. Tường lửa này nên chặn mọi lưu lượng mạng ngoại trừ những lưu lượng đã được cấp phép một cách cụ thể bởi tổ chức. Việc chặn các giao tiếp trên một cổng là khá đơn giản – chỉ cần cho tường lửa biết rằng nó cần phải đóng cổng lại. Vấn đề nằm ở việc đưa ra quyết định về những dịch vụ nào là cần thiết và bởi ai, và do đó, những cổng nào nên được mở và cổng nào nên được đóng. Đây là những gì khiến cho một chính sách bảo mật trở nên hữu ích. Bộ chính sách bảo mật mạng hoàn hảo đối với một tường lửa là bộ chính sách mà người dùng đầu cuối không bao giờ trông thấy và không bao giờ cho phép thậm chí chỉ một gói tin trái phép đi vào mạng. Cũng giống như với bất kỳ hạng mục hoàn hảo nào khác, sẽ hiếm khi tìm thấy bộ chính sách bảo mật hoàn hảo trong một doanh nghiệp. Khi phát triển các quy tắc dành cho một tường lửa, nguyên tắc quyền truy cập ít nhất là tốt nhất để sử dụng, bạn muốn tường lửa chặn càng nhiều lưu lượng càng tốt, trong khi cho phép chỉ những lưu lượng đã được cấp phép đi qua.

Để phát triển một chính sách bảo mật toàn diện và hoàn chỉnh, đầu tiên bạn cần có một hiểu biết toàn diện và hoàn chỉnh về những tài nguyên mạng của bạn và những cách sử dụng của chúng. Khi bạn đã biết cách mà hệ thống mạng sẽ được sử dụng như thế nào, bạn sẽ có một ý tưởng về những gì cần được chặn. Các tường lửa được thiết kế để ngăn chặn

các cuộc tấn công trước khi chúng tìm đến được máy được nhắm mục tiêu. Những mục tiêu phổ biến là các máy chủ web, máy chủ email, máy chủ DNS, các dịch vụ FTP, và các cơ sở dữ liệu. Mỗi một trong số chúng có các chức năng riêng biệt, và đều có những lỗ hổng riêng biệt. Khi bạn quyết định được rằng ai nên nhận được kiểu lưu lượng nào và kiểu lưu lượng nào nên bị chặn, bạn có thể quản lý việc này thông qua tường lửa.



**MÁCH NƯỚC CHO KỲ THI** Các mục tiêu kỳ thi Security+ liệt kê rất nhiều kiểu tường lửa – từ tường lửa ứng dụng web đến các thiết bị (appliance), các tường lửa dựa-trên-máy-vật-chủ và các tường lửa ảo. Hãy có khả năng phân biệt chúng với nhau và biết được cách thức chúng có thể được triển khai như thế nào theo một kịch bản nhất định.

### Tường lửa Ứng dụng Web (WAF)

Một *tường lửa ứng dụng web (WAF)* là một thiết bị thực hiện những hạn chế dựa trên các quy tắc liên quan đến lưu lượng HTTP/HTTPS. Theo định nghĩa, tường lửa ứng dụng web là một dạng bộ lọc nội dung và các cấu hình khác nhau của chúng cho phép chúng cung cấp những khả năng và biện pháp bảo vệ đáng kể. Mức độ cụ thể của những gì có thể được cho phép hoặc bị chặn có thể chính xác như “cho phép Facebook nhưng chặn các trò chơi trên Facebook”. WAF có thể phát hiện và ngăn chặn việc tiết lộ dữ liệu quan trọng, chẳng hạn như số tài khoản, số thẻ tín dụng, v.v... Các WAF cũng có thể được sử dụng để bảo vệ các trang web khỏi các véc-tơ tấn công phổ biến như các cuộc tấn công tạo tập lệnh kịch bản chéo-trang, làm mờ (fuzzing) và tràn bộ đệm.

Bạn có thể thiết lập cấu hình tường lửa ứng dụng web để kiểm tra bên trong một phiên TLS. Đây là điều rất quan trọng nếu như kẻ tấn công đang cố gắng sử dụng một kênh được mã hóa như TLS để che giấu hoạt

động của chúng. Vì các kênh TLS hợp pháp được khởi tạo bởi hệ thống nên bạn có thể chuyển các thông tin xác thực phù hợp trong nội bộ cho WAF để kích hoạt việc kiểm tra TLS.

## **NGFW**

Những tường lửa tiên tiến sử dụng lọc gói tín toàn trạng thái để ngăn chặn một số kiểu giao tiếp không mong muốn. Để phân biệt những tường lửa này với những tường lửa chỉ đóng hoạt động dựa trên thông tin về địa chỉ và cổng, chúng được gọi là *tường lửa thế-hệ-kế-tiếp (NGFW)*. Các tường lửa thế-hệ-kế-tiếp có thể theo dõi trạng thái tương ứng với một giao tiếp, và chúng có thể lọc dựa trên những hành vi không được quan sát một cách đúng đắn với trạng thái của giao tiếp. Ví dụ, nếu một gói tin đến từ bên ngoài mạng đang cố gắng giả vờ rằng nó là hồi đáp cho một thông điệp từ bên trong mạng, tường lửa thế-hệ-kế-tiếp sẽ không có bất kỳ bản ghi nào về việc nó đang được yêu cầu và có thể loại bỏ gói tin đó, chặn những nỗ lực truy cập từ bên ngoài không được mong muốn.

## **Toàn trạng thái (Stateful)**

Một tường lửa kiểm tra *toàn trạng thái* có thể hoạt động dựa trên tình trạng trạng thái của một cuộc hội thoại - đây là cuộc hội thoại mới hay là phần tiếp theo của cuộc hội thoại và nó bắt nguồn từ bên trong hay phía bên ngoài tường lửa? Điều này cung cấp năng lực lớn hơn, nhưng với một chi phí xử lý có ý nghĩa về khả năng mở rộng. Để xem xét tất cả các gói tin và xác định nhu cầu của từng gói và dữ liệu của nó đòi hỏi việc lọc gói tin toàn trạng thái. Toàn trạng thái có nghĩa là tường lửa duy trì, hoặc biết được, ngữ cảnh của một cuộc hội thoại. Trong rất nhiều trường hợp, các quy tắc phụ thuộc vào ngữ cảnh của một kết nối giao tiếp cụ thể. Ví dụ, lưu lượng truy cập từ máy chủ bên ngoài đến máy chủ bên trong có thể được phép nếu nó là cần thiết nhưng sẽ bị chặn nếu không cần thiết. Một ví dụ phổ biến là một yêu cầu cho một trang web.

Yêu cầu này thực sự là một chuỗi các yêu cầu đến nhiều máy chủ, mỗi máy chủ có thể được cho phép hoặc bị chặn. Vì rất nhiều giao tiếp sẽ được chuyển đến các cổng cao (trên 1023), việc giám sát toàn trạng thái sẽ cho phép hệ thống xác định bộ giao tiếp cổng cao nào được cho phép và bộ nào nên bị chặn lại. Một nhược điểm của giám sát toàn trạng thái là yêu cầu nguồn lực và năng lực xử lý đáng kể để thực hiện loại giám sát này, và điều này làm giảm hiệu quả và đòi hỏi phần cứng mạnh mẽ hơn và đắt tiền hơn.

### **Không trạng thái (Stateless)**

Những tường lửa mang điển hình hoạt động trên các địa chỉ IP và các cổng, về bản chất là một tương tác *không trạng thái* với lưu lượng. Hầu hết các tường lửa cơ bản chỉ đơn giản là ngắt các cổng hoặc địa chỉ IP, chặn những gói tin đó khi chúng đến. Mặc dù khá hữu ích nhưng chúng bị hạn chế trong khả năng của chúng khi rất nhiều dịch vụ có thể có những địa chỉ IP khác nhau, và việc duy trì một danh sách các địa chỉ IP được cho phép rất tốn thời gian và, trong rất nhiều trường hợp, sẽ là không thực tế. Tuy nhiên, đối với các hệ thống nội bộ (nghĩa là, một máy chủ cơ sở dữ liệu) không cần phải kết nối đến một lượng lớn các máy chủ khác, việc có một tường lửa dựa-trên-IP đơn giản đứng trước có thể giới hạn sự truy cập đến tập hợp các máy mong muốn đó.

### **Quản lý Mối đe dọa Hợp nhất (UTM)**

*Quản lý mối đe dọa hợp nhất (UTM)* là một thuật ngữ hiện đại được sử dụng để mô tả những thiết bị tất-cả-trong-một được sử dụng trong bảo mật mạng. Các thiết bị UTM thường cung cấp một loạt các dịch vụ, bao gồm chuyển mạch, tường lửa, IDS/IPS, chống-phần-mềm-độc-hại, chống-thư-rác, lọc nội dung, và định hình lưu lượng. Những thiết bị này được thiết kế đơn giản hóa công việc quản lý bảo mật và được nhắm mục tiêu cho các mạng có quy mô nhỏ và trung bình. Do một loạt các dịch vụ mà

các UTM cung cấp, chúng thường được định vị tại đường biên của mạng, quản lý lưu lượng đi vào và đi ra khỏi mạng. Khi một UTM gửi một cảnh báo, tốt nhất là xử lý cảnh báo giống như bất kỳ hành động nào khác để kích hoạt ứng phó sự cố và điều tra nguyên nhân. Những công ty khác nhau có thể xếp chồng các thiết bị bảo mật cùng nhau như một phần của giải pháp UTM của họ, và thông lượng và chức năng có thể khác nhau giữa các nhà cung cấp dựa trên tải trọng công việc của ngăn xếp tạo ra khi xử lý các gói tin đến.

---



**MÁCH NƯỚC CHO KỲ THI** Các thiết bị UTM cung cấp một loạt các dịch vụ, bao gồm chuyển mạch, tường lửa, chống-phần-mềm-độc-hại, chống-thư-rác, lọc nội dung, và định hình lưu lượng. Điều này có thể đơn giản hóa công việc quản trị [bảo mật mạng]. Tuy nhiên, một thiết bị UTM cũng có thể là một điểm đơn lỗi (SPOF).

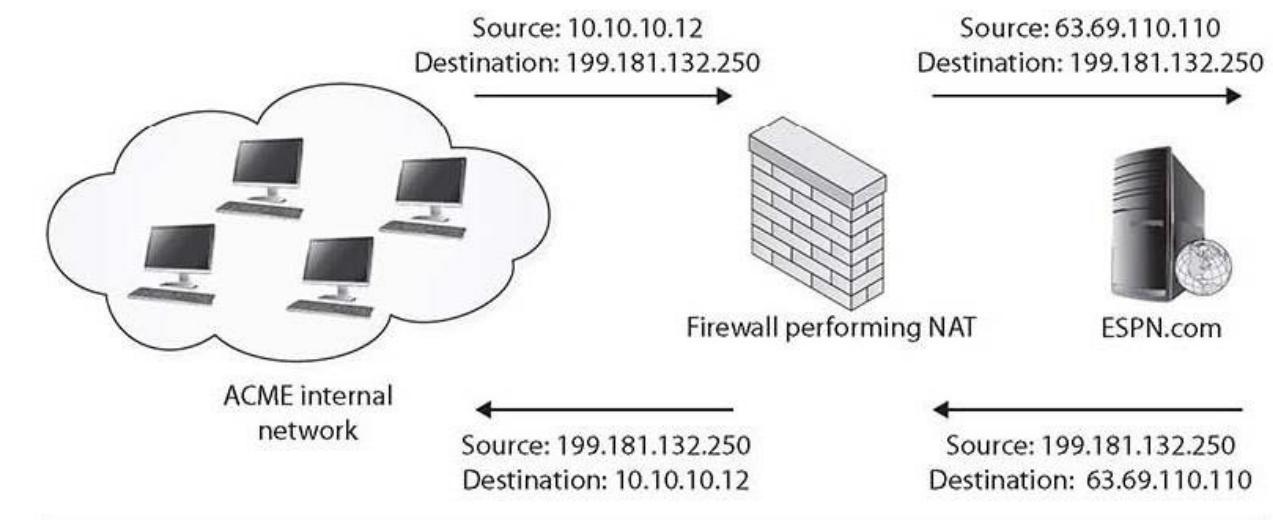
### **Cửa ngõ Diễn dịch Địa chỉ Mạng (NAT Gateway)**

Nếu bạn đang nghĩ rằng không gian địa chỉ 32-bit được cắt nhỏ và chia thành mạng con là không đủ để xử lý tất cả các hệ thống trên thế giới thì bạn đã đúng. Mặc dù các khối địa chỉ IPv4 đã được chỉ định cho các tổ chức như công ty và trường đại học, nhưng thường không có đủ địa chỉ IP-tường-minh trên Internet để gán cho mọi hệ thống trên hành tinh một địa chỉ IP duy nhất và có thể định-tuyến-được-trên-Internet. Để bù đắp cho việc thiếu không gian địa chỉ IP có sẵn này, các tổ chức sử dụng *Diễn dịch Địa chỉ Mạng (Network Address Translation - NAT)*, vốn diễn dịch các địa chỉ IP riêng tư (không thể định tuyến [trên Internet]) thành địa chỉ IP công cộng (có thể định tuyến).

Các khối địa chỉ IP nhất định được dành riêng cho “mục đích sử dụng cá nhân”, và không phải mọi hệ thống trong tổ chức đều cần một địa chỉ IP

trực tiếp và có thể định-tuyến-trên-Internet. Trên thực tế, vì lý do bảo mật, sẽ tốt hơn nhiều nếu hầu hết các hệ thống của tổ chức được ẩn khỏi việc truy cập Internet trực tiếp. Hầu hết các tổ chức xây dựng mạng nội bộ của họ bằng cách sử dụng các dải địa chỉ IP riêng (chẳng hạn như 10.1.1.X) để ngăn việc người ngoài truy cập trực tiếp vào các mạng nội bộ đó. Tuy nhiên, trong nhiều trường hợp, các hệ thống đó vẫn cần có khả năng kết nối đến Internet. Điều này được thực hiện bằng cách sử dụng một thiết bị NAT (thường là tường lửa hoặc bộ định tuyến) dịch nhiều địa chỉ IP nội bộ thành một trong số ít các địa chỉ IP công cộng.

Ví dụ: hãy xem xét một công ty hư cấu, ACME.com. ACME có hàng nghìn hệ thống nội bộ sử dụng địa chỉ IP riêng tư trong dải 10.X.X.X. Để cho phép các địa chỉ IP đó giao tiếp với thế giới bên ngoài, ACME thuê một kết nối Internet và một số địa chỉ IP công cộng, đồng thời triển khai thiết bị có khả năng NAT. Quản trị viên ACME định cấu hình tất cả các máy chủ nội bộ của họ để sử dụng thiết bị NAT làm cửa ngõ mặc định (default gateway) của họ. Khi các máy chủ nội bộ cần gửi các gói tin ra bên ngoài công ty, chúng sẽ gửi các gói tin đến thiết bị NAT. Thiết bị NAT xóa địa chỉ IP nguồn trong nội bộ ra khỏi các gói gửi đi và thay thế nó bằng địa chỉ công khai và có thể định tuyến của thiết bị NAT và gửi các gói theo đường đi của chúng. Khi các gói phản hồi được nhận từ các nguồn bên ngoài, thiết bị sẽ thực hiện NAT theo chiều ngược lại, loại bỏ địa chỉ IP bên ngoài và công khai ra khỏi trường địa chỉ đích và thay thế nó bằng địa chỉ IP nội bộ, riêng tư chính xác trước khi gửi các gói vào mạng ACME.com riêng tư. Hình 19-5 minh họa quá trình NAT này.



**Hình 19-5** Miêu tả logic về NAT

Trong Hình 19-5, chúng ta thấy một ví dụ về việc NAT đang được thực hiện. Một máy trạm nội bộ (10.10.10.12) muốn truy cập một trang web tại địa chỉ 199.181.132.250. Khi gói tin đi đến thiết bị NAT, thiết bị dịch địa chỉ nguồn 10.10.10.12 thành địa chỉ 63.69.110.110 có thể định tuyến trên toàn cầu, là địa chỉ tương tác tường minh với bên ngoài của thiết bị. Khi trang web phản hồi, nó phản hồi lại cho địa chỉ của thiết bị giống như thế thiết bị NAT đã yêu cầu thông tin ban đầu. Thiết bị NAT sau đó phải nhớ lại máy trạm nội bộ nào đã yêu cầu thông tin và định tuyến các gói tin đi đến đích đúng phù hợp.

Mặc dù khái niệm nền tảng của NAT là như nhau nhưng trên thực tế có một số các phương pháp tiếp cận để triển khai NAT, bao gồm:

- **NAT Tĩnh (Static NAT)** Ánh xạ một địa chỉ riêng tư nội bộ thành một địa chỉ công khai bên ngoài. Cùng một địa chỉ công khai thường được sử dụng cho địa chỉ riêng tư đó. Kỹ thuật này thường được sử dụng khi lưu trữ một thứ gì đó mà bạn muốn công chúng có khả năng truy cập được, chẳng hạn như một máy chủ web, đằng sau một tường lửa.

- **NAT Động (Dynamic NAT)** Ánh xạ một địa chỉ riêng tư nội bộ thành một địa chỉ IP công khai được chọn từ một dải các địa chỉ IP (công khai) đã được đăng ký. Kỹ thuật này thường được sử dụng khi diễn dịch các địa chỉ cho các máy trạm người-dùng-đầu-cuối và thiết bị NAT phải theo dõi các bản đồ địa chỉ nội bộ/bên ngoài.
- **Dịch Địa chỉ Cổng (Port Address Translation – PAT)** Cho phép nhiều địa chỉ nội bộ và riêng tư khác nhau cùng chia sẻ một địa chỉ IP bên ngoài. Các thiết bị thực hiện PAT thay thế địa chỉ IP nguồn bằng địa chỉ IP NAT và thay thế trường cổng của nguồn bằng một cổng từ một nhóm kết nối có sẵn. Các thiết bị PAT giữ một bảng dịch để theo dõi các máy chủ nội bộ đang sử dụng cổng nào để các gói tiếp theo có thể được đóng dấu với cùng một số cổng. Khi nhận được các gói phản hồi, thiết bị PAT sẽ đảo ngược quá trình và chuyển tiếp gói đến đúng máy chủ nội bộ. PAT là một kỹ thuật NAT rất phổ biến và được sử dụng tại nhiều tổ chức.

## Bộ lọc Nội dung/URL

Các *bộ lọc nội dung/URL* được sử dụng để hạn chế những kiểu nội dung cụ thể trên Web đối với người dùng. Một cách sử dụng phổ biến là chặn các trang web không liên quan đến công việc như Facebook và trò chơi trực tuyến. Các bộ lọc nội dung cũng có thể kiểm tra những nội dung thực tế đang được trả về cho một trình duyệt, tìm kiếm một danh sách các hạng mục hoặc các hạng mục bị hạn chế và chặn không chỉ URL mà còn nội dung đã được trả về. Cũng giống như mọi thiết bị thực thi chính sách khác, các bộ lọc nội dung dựa trên một bộ các quy tắc, và duy trì quy tắc là một vấn đề. Một trong số những vấn đề phổ biến nhất với các bộ lọc nội dung là phạm vi quá rộng để chặn. Trong một môi trường y tế, việc chặn từ "breast" sẽ không hoạt động, cũng tương tự như ở trong một nhà máy chế biến thịt gà. Cần phải có một cơ chế để nâng các khối một

cách dễ dàng và nhanh chóng nếu người dùng phản đối và dễ dàng xác định rằng họ nên có quyền truy cập.

### **Nguồn Mở so với Độc quyền**

Tường lửa có nhiều dạng và nhiều loại, và một trong số các phương pháp để phân biệt chúng là tách chúng thành các giải pháp *nguồn mở* và *độc quyền* (thương mại). Tường lửa mã nguồn mở được minh họa bởi iptables, một chức năng được tích-hợp sẵn trong hệ thống Linux. Iptables và các giải pháp mã nguồn mở khác có lợi thế về chi phí khi chúng là miễn phí, nhưng chi phí ban đầu của giải pháp tường lửa không phải là yếu tố duy nhất. Dễ dàng bảo trì và quản lý quy tắc là động lực chính để sử dụng lâu-dài và rất nhiều giải pháp độc quyền đã làm việc để gia tăng tiện ích của các dịch vụ của họ thông qua việc cải thiện các tương tác này.

Một trong những tường lửa phổ biến nhất được sử dụng là tường lửa Microsoft Windows Defender, một tường lửa độc quyền được tích hợp trong Hệ điều hành Windows.

### **Phần cứng so với Phần mềm**

Tường lửa có thể là các thiết bị vật lý, phần cứng hoặc một tập hợp các dịch vụ phần mềm hoạt động trên một hệ thống. Để sử dụng trên máy chủ, một giải pháp phần mềm như Microsoft Windows Defender hoặc iptables trên máy chủ Linux có thể phù hợp với chi phí. Để sử dụng trong môi trường doanh nghiệp ở cấp độ mạng, với nhu cầu phân tách các vùng bảo mật khác nhau, thiết bị phần cứng chuyên dụng sẽ có hiệu quả và tiết kiệm chi phí hơn.

### **Thiết bị so với Dựa trên Máy chủ so với Ảo**

Tường lửa có thể được đặt trên một máy chủ, dưới dạng một ứng dụng riêng biệt hoặc một phần của chính bản thân hệ điều hành. Trong các kết nối mạng do-phần-mềm-định-nghĩa (SDN), tường lửa có thể được khởi tạo

như các chức năng mạng ảo, cung cấp mọi tính năng của một giải pháp phần mềm ảo. Tường lửa cũng có thể được khởi tạo thông qua một thiết bị, hoạt động giống như một thiết bị phân tách mạng, phân tách các phần của mạng dựa trên các quy tắc tường lửa.

### **Danh sách Kiểm soát Truy cập (ACL)**

*Danh sách kiểm soát truy cập* cung cấp thông tin hệ thống về những đối tượng nào được phép thực hiện những hành động nào. Trong trường hợp hệ thống mạng, ACL có thể kiểm soát ai có thể thay đổi các thông số mạng thông qua các cấu hình, ai có thể vượt qua tường lửa cụ thể và một loạt các quyết định khác. Khái niệm có được một danh sách người dùng được chấp thuận, hoặc ACL, được các mạng sử dụng rộng rãi để quản lý các khía cạnh của bảo mật mạng.

### **Bảo mật Định tuyến**

Định tuyến là cơ sở của việc kết nối các mạng với nhau để bao gồm Internet. Các gói thông qua các mạng để di chuyển thông tin từ nguồn đến đích. Tùy thuộc vào việc đâu là nguồn và đâu là đích, lộ trình mà một gói tin đi qua có thể rất đa dạng, từ đơn giản và ngắn đến phức tạp và dài. Các giao thức được sử dụng để kết nối các mạng khác nhau từ đơn giản, như Giao thức Internet (IP) đến phức tạp hơn, chẳng hạn như BGP, IS-IS, OSPF, EIGRP và RIPv2. Việc duy trì bảo mật định tuyến là một phần chức năng của mỗi giao thức này, và mỗi giao thức đều phục vụ để thực hiện một chức năng cần thiết cụ thể trong việc kết nối mạng. Xét từ quan điểm Security+, chi tiết đằng sau mỗi giao thức này nằm ngoài phạm vi, nhưng việc hiểu rằng chúng hoạt động cùng nhau để hỗ trợ chức năng mạng và truyền gói tin bảo mật là điều quan trọng.

### **Chất lượng Dịch vụ (QoS)**

*Chất lượng Dịch vụ (QoS)* là việc sử dụng các công nghệ cụ thể trên một mạng để đảm bảo khả năng của nó [mạng] trong việc quản lý lưu lượng

truy cập dựa trên nhiều chỉ số khác nhau. Băng-thông-cao, lưu lượng theo thời-gian-thực, chẳng hạn như Âm thanh thoại qua IP (VoIP), hội nghị truyền hình và video-theo-nhu-cầu, có độ nhạy cao đối với các vấn đề mạng như độ trễ và chập chờn. Những công nghệ QoS được sử dụng để quản lý các điều kiện mạng như băng thông (thông lượng), độ trễ (delay), jitter (phương sai về độ trễ) và tỷ lệ lỗi. Chúng thực hiện điều này bằng cách cung cấp khả năng xử lý khác biệt và phân bổ công suất cho các luồng cụ thể dựa trên kiểu và nguồn gốc của gói tin. QoS cho phép quản trị viên mạng chỉ định mức độ ưu tiên mà theo đó, các gói được xử lý cũng như lượng băng thông dành cho ứng dụng hoặc luồng lưu lượng đó.

### Tác động của IPv6

Sự thay đổi được chú ý phổ biến nhất với IPv6 so với IPv4 là phạm vi đánh địa chỉ được gia tăng, từ địa chỉ 32-bit lên địa chỉ 128-bit, cung cấp không gian địa chỉ hầu như không giới hạn, nhưng đây không phải là bước tiến duy nhất. IPv6 có rất nhiều tác động đối với các thiết kế mạng bảo mật - một số tốt và một số khác lại có vấn đề. IPv6 cho phép mã hóa từ đầu đến cuối, điều này rất tốt cho bảo mật giao tiếp nhưng không tốt cho việc giám sát mạng. IPv6 sử dụng giao thức Khám phá Hàng xóm An toàn (Secure Neighbor Discovery – SEND)), giúp giảm bớt các cuộc tấn công nhiễm độc ARP. IPv6 sử dụng không gian địa chỉ rộng của nó theo cách thức khác với IPv4 - không có NAT trong IPv6, do đó, mạng sẽ cần được thiết kế lại để tận dụng lợi thế của không gian rộng hơn và những lợi ích vốn có của các phiên bản mới của các giao thức hỗ trợ như ICMPv6, DHCPv6, v.v... Tóm lại, IPv6 là một sự tái tạo lại hoàn toàn của lĩnh vực mạng với nhiều ưu điểm mới - và ít vấn đề hơn. Thách thức ở đây nằm trong việc tìm hiểu các giao thức mới và tác động cụ thể của chúng. Như một trong những kiến trúc sư IPv6 đã giải thích tại một sự kiện công khai, IPv6 không chỉ là thủ thuật làm đẹp trên một giao thức cũ [hàm ý]

chỉ sự tân trang giao thức IPv4], nó là một giao thức hoàn toàn mới - tương thích ngược ở một số khía cạnh, nhưng là một giao thức mở ra một thế giới mạng hoàn toàn mới.

### **Mở rộng Cổng/Phản chiếu Cổng (Port Spanning/Port Mirroring)**

Hầu hết các thiết bị chuyển mạch doanh nghiệp đều có khả năng sao chép hoạt động của một hoặc nhiều cổng thông qua cổng Bộ phân tích Cổng Chuyển mạch (Switch Port Analyzer - SPAN), còn được gọi là *phản chiếu cổng*. Lưu lượng này sau đó có thể được gửi đến một thiết bị để phân tích. Phản chiếu cổng có thể gấp ván đề khi mức lưu lượng truy cập trở nên dày đặc, vì lưu lượng SPAN tổng hợp có thể vượt quá thông lượng của thiết bị. Ví dụ, một bộ chuyển mạch có 16 cổng, với mỗi cổng chạy ở tốc độ 100 Mbps, có thể có mức lưu lượng là 1,6 GB nếu tất cả các mạch đều được tăng tối đa, điều này cho bạn biết lý do tại sao công nghệ này có thể gặp sự cố trong môi trường có lưu-lượng-truy-cập cao.

### **Port Taps**

Một *điểm truy cập thử nghiệm* (*test access point – TAP*) là một cơ chế sao-chép-tín-hiệu thụ động được thiết lập giữa hai điểm trên mạng. TAP có thể sao chép tất cả các gói tin mà nó nhận được, xây dựng tại một bản sao của tất cả các gói tin. Các TAP mang lại một ưu điểm khác biệt là không bị áp đảo bởi các mức lưu lượng truy cập, ít nhất là không trong quá trình thu thập dữ liệu. Nhược điểm chính là TAP là một phần cứng riêng biệt, và làm gia tăng thêm chi phí của mạng. Các TAP trái phép có thể gây ra mối đe dọa về bảo mật, vì chúng tạo ra một kết nối sẵn sàng để giám sát và thay đổi lưu lượng truy cập như một cuộc tấn công người-trung-gian.



**MÁCH NƯỚC CHO KỲ THI** Port tap, khi được đặt giữa các thiết bị gửi và nhận, có thể được sử dụng để thực hiện các cuộc tấn công người-trung-gian. Vì vậy, khi được lắp đặt bởi một bên trái phép, chúng có thể trở thành một rủi ro bảo mật.

### **Giám sát các Dịch vụ**

*Giám sát bảo mật mạng (NSM)* là quá trình thu thập và phân tích dữ liệu mạng để phát hiện ra hoạt động trái phép. NSM không phải là một cách thức ngăn chặn sự xâm nhập, nhưng khi được triển khai bên trong một mạng, nó có thể phát hiện ra nơi mà các biện pháp phòng thủ khác đã thất bại. Nó giống như việc có một nhân viên bảo vệ địa phương tuần tra bên trong một tòa nhà đóng cửa. NSM có thể được triển khai như một dịch vụ và nhiều công ty có đề nghị hỗ trợ các dịch vụ giám sát để cung cấp cho doanh nghiệp một phương tiện phát hiện hoạt động trái phép. Việc có hệ thống phòng thủ là điều quan trọng, nhưng theo dõi để biết khi nào các hệ thống phòng thủ đó thất bại là mục đích của NMS và các dịch vụ giám sát.

### **Giám sát Tính toàn vẹn của Tập tin**

*Trình theo dõi tính toàn vẹn của tập tin* là một loạt các quy trình nội bộ có thể xác nhận tính toàn vẹn của tập tin của Hệ điều hành và ứng dụng. Có các tiện ích của Hệ điều hành có thể được tự động hóa để thực hiện việc này cũng như các ứng dụng để quản lý tác vụ tối quan trọng này. Một số dạng giải pháp danh sách trắng thực hiện tác vụ tương tự, thực hiện việc kiểm tra hàm băm đối với giá trị tốt-đã-biết trước khi cho phép khởi chạy chương trình.

Bất cứ khi nào bạn tải xuống tập tin từ một nguồn trực tuyến, ngay cả khi tải về từ nhà cung cấp tập tin, bạn nên thực hiện kiểm tra tính toàn

vẹn của tập tin để đảm bảo rằng tập tin đã không bị giả mạo theo bất kỳ hình thức nào. Điều này sẽ cảnh báo bạn về một đã thay đổi nhị phân, thậm chí ngay cả khi tác nhân lưu trữ của tập tin không hề hay biết về vấn đề cụ thể. Kiểm tra tính toàn vẹn của tập tin hoạt động bằng cách lấy một hàm băm của tập tin và so sánh giá trị này với một kho lưu trữ ngoại tuyến các giá trị chính xác. Nếu các hàm băm khớp nhau nghĩa là tập tin đã không bị thay đổi.

Trên các máy Microsoft Windows, có thể thực hiện kiểm tra tính toàn vẹn của tập tin hệ thống bằng lệnh dòng-lệnh **sfc /scannow**. Trên hệ thống Debian Linux, lệnh **debsums** được sử dụng để xác minh giá trị băm của các thành phần gói đã cài đặt.



**MÁCH NƯỚC CHO KỲ THI** Để hoạt động một cách đúng đắn, mỗi thiết bị bảo mật được đề cập trong phần này đều phải được lắp đặt một cách phù hợp với luồng lưu lượng mà nó dự định tương tác. Nếu có các đường dẫn mạng xung quanh thiết bị, nó sẽ không hoạt động như thiết kế. Việc hiểu được kiến trúc mạng là điều quan trọng khi lắp đặt thiết bị.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các nguyên tắc đứng sau thiết kế mạng bảo mật. Chương được mở đầu bằng việc tìm hiểu về cân bằng tải, bao gồm chủ động/chủ động, chủ động/thụ động, phương pháp lập lịch trình, IP ảo và tính bền bỉ. Phần tiếp theo đề cập đến phân đoạn mạng, bao gồm các cuộc thảo luận về các mạng cục bộ ảo (VLAN), mạng con được sàng lọc, luồng lưu lượng đông-tây, mạng ngoại vi, mạng nội bộ và khái niệm zero trust.

Phần tiếp theo xem xét các mạng riêng ảo (VPN). Các khái niệm về luân bật, phân tách đường hầm so với toàn bộ đường hầm, truy cập từ xa so với điểm-đến-điểm, IPSec, thuyết minh SSL/TLS, tác động của HTML5 và Giao thức Đường hầm Lớp 2 (L2TP) đã được trình bày. Phần tiếp theo là về DNS, tiếp theo là kiểm soát truy cập mạng (NAC), bao gồm cả dạng có tác nhân và không có tác nhân. Quản lý ngoài-dải-tần đã được đề cập, tiếp theo là một phần về bảo mật cổng. Trong lĩnh vực bảo mật cổng, các chủ đề về phòng chống bão quảng bá, bảo vệ Đơn vị Dữ liệu Giao thức Cầu nối (BPDU), ngăn chặn lặp, theo dõi Giao thức Cấu hình Máy chủ Động (DHCP) và lọc kiểm soát truy cập phương tiện (MAC) đã được đề cập.

Phần chính tiếp theo bao gồm các thiết bị mạng. Trong phần này, các máy chủ jump và máy chủ proxy, cả chuyển tiếp và đảo ngược, đều được đề cập. Tiếp theo là xem xét các hệ thống phát hiện xâm nhập dựa-trên-mạng (NIDS) và hệ thống ngăn chặn xâm nhập dựa-trên-mạng (NIPS), bao gồm các phần về hệ thống dựa-trên-chữ-ký, hệ thống khám phá/hành vi, hệ thống dựa-trên-sự-bất-thường và các tùy chọn lắp đặt nội tuyến so với thụ động. Các thiết bị mạng bổ sung được đề cập bao gồm thiết bị HSM, các cảm biến, bộ thu thập và bộ tổng hợp. Phần chính tiếp theo về các thiết bị mạng đề cập đến các tường lửa. Trong lĩnh vực này, các chủ

đề về tường lửa ứng dụng web (WAF), tường lửa thế-hệ-kế-tiếp (NGFW), lưu lượng toàn trạng thái so với không trạng thái, hệ thống quản lý mối đe dọa hợp nhất (UTM), cửa ngõ Diễn dịch Địa chỉ Mạng (NAT), bộ lọc nội dung/URL, triển khai tường lửa nguồn mở so với độc quyền, triển khai phần cứng so với phần mềm và thiết bị so với hệ thống ảo dựa-trên-máy-vật-chủ đã được đề cập.

Tiếp theo là các chủ đề về danh sách kiểm soát truy cập (ACL), bảo mật định tuyến, Chất lượng Dịch vụ (QoS) và tác động của IPv6. Chương này đã kết thúc với các phần về mở rộng cổng/phản chiếu cổng, bao gồm TAP của cổng, dịch vụ giám sát và trình theo dõi tính toàn vẹn của tập tin.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

- 1.** Một hệ thống ngăn chặn xâm nhập dựa-trên-mạng (NIPS) dựa trên công nghệ nào khác ở cốt lõi của nó?
  - A.** VPN
  - B.** IDS
  - C.** NAT
  - D.** ACL.
- 2.** Bạn đã được yêu cầu chuẩn bị một báo cáo về hệ thống phát hiện xâm nhập dựa-trên-mạng so sánh các giải pháp NIDS từ hai nhà cung cấp tiềm năng mà công ty của bạn đang xem xét. Một giải pháp là dựa trên chữ ký và một là dựa trên hành vi. Điều nào sau đây liệt kê những gì mà báo cáo của bạn sẽ xác định là ưu điểm chính của từng loại?
  - A.** Hành vi: tỷ lệ âm tính giả thấp; Chữ ký: khả năng phát hiện các cuộc tấn công zero-day
  - B.** Hành vi: khả năng phát hiện các cuộc tấn công zero-day; Chữ ký: tỷ lệ dương tính giả thấp
  - C.** Hành vi: tỷ lệ dương tính giả cao; Chữ ký: tốc độ phát hiện cao
  - D.** Hành vi: tỷ lệ dương tính giả thấp; Chữ ký: tỷ lệ dương tính giả cao
- 3.** Các máy chủ proxy có thể cải thiện bảo mật như thế nào?
  - A.** Chúng sử dụng mã hóa dựa trên TLS để truy cập tất cả các trang web.
  - B.** Chúng có thể kiểm soát các trang web và nội dung mà nhân viên truy cập, làm giảm cơ hội tiếp xúc với phần mềm độc hại.

- C.** Chúng thực thi việc sử dụng thích hợp các nguồn lực của công ty.
- D.** Chúng ngăn chặn việc truy cập vào các trang web lừa đảo.
- 4.** Công nghệ nào có thể kiểm tra tình trạng của máy khách trước khi cho phép truy cập vào mạng?
- A.** DLP
- B.** Proxy đảo ngược
- C.** NIDS/NIPS
- D.** NAC.
- 5.** Loại thiết bị nào cung cấp khả năng bảo vệ chống giả mạo cho các khóa mã hóa?
- A.** HSM
- B.** IPSec
- C.** Máy chủ jump
- D.** HTML5.
- 6.** Mục đích của giao thức DNS là gì?
- A.** Nó cung cấp chức năng định phí SaaS trên cơ sở mỗi lần sử dụng.
- B.** Nó hỗ trợ cho cơ sở hạ tầng mạng.
- C.** Nó diễn dịch tên thành địa chỉ IP.
- D.** Nó xác định khách thuê trong một đám mây công cộng.
- 7.** Một người dùng báo cáo với bộ phận trợ giúp rằng anh ta đang nhận được thông báo lỗi “không thể phân giải địa chỉ” từ trình duyệt của mình. Cổng nào có thể là sự cố trên tường lửa của anh ấy?
- A.** 22
- B.** 553
- C.** 440
- D.** 53.

- 8.** Mục đích chính của mạng con được sàng lọc là gì?
  - A.** Để ngăn truy cập trực tiếp vào các máy chủ bảo mật từ Internet
  - B.** Cung cấp một nơi lưu trú cho các máy chủ của công ty để chúng có thể truy cập Internet
  - C.** Để tạo ra một môi trường máy tính bảo mật bên cạnh Internet
  - D.** Để giảm tốc độ lưu lượng truy cập đến và đi vào mạng.
- 9.** Công cụ tốt nhất để đảm bảo các ưu tiên lưu lượng mạng cho hội nghị truyền hình được duy trì là gì?
  - A.** QoS
  - B.** VLAN
  - C.** Phân đoạn mạng
  - D.** Tường lửa thế-hệ-kế-tiếp.
- 10.** Nếu bạn muốn giám sát 100% việc truyền tải từ đại diện dịch vụ khách hàng của mình tới Internet và các dịch vụ nội bộ khác thì công cụ nào tốt nhất để sử dụng?
  - A.** Cổng SPAN
  - B.** TAP
  - C.** Phản chiếu cổng
  - D.** Bộ chuyển mạch tổng hợp.

## Đáp án

1. **B.** Một NIPS dựa vào công nghệ của một hệ thống phát hiện xâm nhập (IDS) ở cốt lõi của nó để phát hiện ra các cuộc tấn công tiềm năng.
2. **B.** Ưu điểm chính của NIDS dựa trên hành vi là khả năng phát hiện các cuộc tấn công zero-day, trong khi ưu điểm chính của NIDS dựa trên chữ ký là tỷ lệ dương tính giả thấp.
3. **B.** Máy chủ proxy có thể cải thiện bảo mật bằng cách giới hạn các trang web và nội dung được truy cập bởi nhân viên, do đó hạn chế khả năng truy cập vào phần mềm độc hại.
4. **D.** NAC, hay kiểm soát truy cập mạng, là một công nghệ có thể bắt buộc tình trạng bảo mật của máy khách trước khi cho phép nó truy cập vào mạng.
5. **A.** Mô-đun bảo mật phần cứng (HSM) có các biện pháp bảo vệ chống giả mạo để ngăn chặn việc các khóa mã hóa mà nó quản lý bị thay đổi.
6. **C.** Hệ thống tên miền (DNS) diễn dịch các tên thành các địa chỉ IP.
7. **D.** Hệ thống tên miền (DNS) sử dụng TCP và UDP cổng 53 cho các truy vấn và phản hồi tiêu chuẩn.
8. **A.** Mục đích chính của mạng con được sàng lọc là cung cấp sự tách biệt giữa vùng không đáng tin cậy của Internet và vùng đáng tin cậy của các hệ thống doanh nghiệp. Nó làm như vậy bằng cách ngăn việc truy cập trực tiếp vào các máy chủ bảo mật từ Internet.
9. **A.** Các giải pháp Chất lượng Dịch vụ (QoS) có thể quản lý các luồng lưu lượng theo loại để cung cấp quyền truy cập được đảm bảo và ưu tiên cho các luồng lưu lượng cụ thể.

**10. B.** Cần có điểm truy cập kiểm nghiệm (TAP) để giám sát 100% việc truyền tải từ đại diện dịch vụ khách hàng của bạn tới Internet và các dịch vụ nội bộ khác.

## Chương 20    Bảo mật Không dây

---

### Bảo mật Không dây

Trong chương này bạn sẽ

- Tìm hiểu về các giao thức mật mã và xác thực không dây,
  - Tìm hiểu về các phương pháp và những cẩn nhắc cài đặt.
- 

Không dây ngày càng trở thành cách thức mà mọi người sử dụng để truy cập Internet. Bởi vì truy cập không dây được coi là một tiện ích của người tiêu dùng, nhiều doanh nghiệp đã bổ sung thêm các điểm truy cập không dây để thu hút khách hàng đến với cửa hàng của họ. Cùng với việc ra mắt mạng di động thế hệ thứ năm (5G), mọi người cũng ngày càng truy cập Internet từ điện thoại di động của họ. Sự phát triển mạnh mẽ về mức độ phổ biến của các máy tính phi truyền thống chẳng hạn như netbook, máy đọc-sách-điện-tử (e-reader) và máy tính bảng cũng đã thúc đẩy sự phổ biến của truy cập không dây.

Khi việc sử dụng mạng không dây gia tăng, tính bảo mật của các giao thức không dây đã trở thành một yếu tố quan trọng hơn trong bảo mật của toàn bộ mạng. Là một chuyên gia bảo mật, bạn cần tìm hiểu các ứng dụng mạng không dây vì những rủi ro cố hữu trong việc quảng bá tín hiệu mạng mà bất kỳ ai cũng có thể chặn được. Việc gửi thông tin không bảo mật qua các làn sóng công cộng cũng tương tự như đăng nhập khống của công ty bạn ở cửa trước của tòa nhà. Chương này xem xét một số giao thức không dây hiện tại và các tính năng bảo mật của chúng.



ADMINISTRATION & SECURITY  
VIETNAM

## Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 3,4 của kỳ thi CompTIA Security+: Đưa ra một tình huống, cài đặt và thiết lập cấu hình cài đặt bảo mật không dây.

## Các Giao thức Mật mã

Về bản chất, các mạng không dây khiến cho việc bảo vệ an ninh về mặt vật lý để chống lại các kết nối giả mạo trở nên khó khăn hơn rất nhiều. Việc thiếu hàng rào vật lý này làm cho việc bảo vệ chống lại những người khác đang nghe trộm trên một kết nối cũng là một thách thức. *Giao thức mật mã* là các tiêu chuẩn được sử dụng để mô tả các phương pháp và triển khai mật mã nhằm đảm bảo khả năng tương tác lẫn nhau giữa các thiết bị của các nhà cung cấp khác nhau.

Lịch sử của các giao thức mật mã trong mạng không dây bắt đầu với Quyền riêng tư Tương đương Có dây (Wired Equivalent Privacy - WEP) và sau đó chuyển sang Truy cập Wi-Fi được Bảo vệ (Wi-Fi Protected Access - WPA), tuy nhiên, cả hai đều có thiết kế kém. Các nhà thiết kế của giao thức 802.11 đã cố gắng để duy trì tính bảo mật trong các hệ thống không dây bằng cách đưa ra giao thức WEP, sử dụng mật mã để mã hóa dữ liệu khi nó được truyền qua không khí. WEP ban đầu đã là một thành công, nhưng theo thời gian, một số điểm yếu đã được phát hiện trong giao thức này. WEP mã hóa dữ liệu truyền qua mạng bằng mật mã dòng RC4, cố gắng đảm bảo tính bảo mật. Lỗ hổng trong WEP là véc-tơ khởi tạo không đủ độ dài để bảo vệ kênh.

Tiêu chuẩn đầu tiên được sử dụng trên thị trường để thay thế WEP là WPA. Tiêu chuẩn này sử dụng thuật toán WEP bị thiếu sót với Giao thức Toàn vẹn Khóa Tạm thời (Temporal Key Integrity Protocol - TKIP). TKIP hoạt động bằng cách sử dụng bí mật được chia sẻ kết hợp với địa chỉ MAC của thẻ để tạo ra khóa mới, khóa này được trộn với véc-tơ khởi tạo (IV) để tạo khóa cho mỗi gói mã hóa một gói bằng cách sử dụng cùng một mật mã RC4 được sử dụng bởi WEP truyền thống. Việc này đã khắc phục được điểm yếu của khóa WEP, vì khóa chỉ được sử dụng trên một gói.

Mặc dù cả WEP và WPA đều có những thiết sót nhưng chúng đã dẫn đến WPA2 và cuối cùng là WPA3, cả hai đều đang được sử dụng ngày nay. Nếu bạn thấy các giao thức cũ vẫn đang được sử dụng, hãy hiểu rằng chúng không cung cấp bất kỳ mức độ bảo mật đáng kể nào và nên được nâng cấp.

---



**MÁCH NƯỚC CHO KỲ THI** WEP và WPA không còn được liệt kê trong các mục tiêu của kỳ thi Security+, nhưng những dữ kiện và thông tin nền tảng là có liên quan đến WPA2 và minh họa cho cách thức mà chúng ta đến được vị trí của mình.

### Wi-Fi Protected Access 2 (WPA2)

IEEE 802.11i là tiêu chuẩn dành cho bảo mật trong mạng không dây và còn được gọi là *Truy cập Không dây được Bảo vệ 2 (Wi-Fi Protected Access 2 (WPA2))*. Nó sử dụng 802.1X để cung cấp xác thực và sử dụng Tiêu chuẩn Mã hóa Nâng cao (AES) làm giao thức mã hóa. WPA2 sử dụng mật mã khối AES, một cải tiến đáng kể so với việc sử dụng mã hóa dòng RC4 của WEP và WPA. WPA2 chỉ định việc sử dụng Chế độ Bộ đếm với Giao thức CBC-MAC (đầy đủ là Chế độ Bộ đếm với Chuỗi Khối Mã hóa - Giao thức Mã Xác thực Thông điệp hoặc đơn giản là CCMP). CCMP sẽ được mô tả sau trong chương này.

Mặc dù WPA2 đã giải quyết những sai sót trong WPA và đã là tiêu chuẩn thực tế trong rất nhiều năm trên các mạng không dây nghiêm túc về bảo mật, nhưng nó cũng có một loạt vấn đề, và dẫn đến sự phát triển của WPA3. WPA2 đi kèm với nhiều phương pháp khác nhau để thiết lập các phần tử khóa chia sẻ và những phương pháp đó sẽ được mô tả ở phần sau của chương. Mật khẩu WPA2-Personal có thể bị bẻ khóa bằng cách sử dụng các cuộc tấn công brute force. tệ hơn nữa, một khi tin tức đã chiếm

được dữ liệu từ sóng không dây, việc bẻ khóa mật khẩu thực sự có thể xảy ra một cách ngoại tuyến trên một máy chuyên dụng mạnh mẽ hơn. Sau đó, bất kỳ tin nhắn đã được mã hóa nào mà chúng ghi lại đều có thể được giải mã, do đó cung cấp thêm mật khẩu và dữ liệu nhạy cảm khác.

WPA2 có hai phiên bản: WPA2-Personal và WPA2-Enterprise. WPA2-Personal còn được gọi là WPA2-PSK vì nó sử dụng xác thực dựa trên khóa chia-sẻ-trước (pre-shared key - PSK), cho phép người dùng gia đình không cần máy chủ xác thực cấp doanh nghiệp để quản lý khóa. Để sử dụng WPA2-PSK trên mạng, bộ định tuyến được cung cấp khóa chia-sẻ-trước, thường là một cụm mật khẩu bằng tiếng Anh thuần túy có độ dài từ 8 đến 63 ký tự. Sau đó, WPA2-Personal sử dụng TKIP để kết hợp cụm mật khẩu đó với Mã định danh Nhóm Dịch vụ (Service Set Identifier - SSID) của mạng để tạo ra các khóa mã hóa duy nhất cho từng máy khách không dây. WPA2-Enterprise thay thế khóa chia-sẻ-trước bằng IEEE 802.1X, sẽ được thảo luận trong phần riêng của nó tại phần sau của chương này. Bằng cách loại bỏ phần tử PSK, WPA2-Enterprise có thể tạo ra các khóa mạnh hơn và thông tin sẽ không bị thu thập.

Trong WPA2, một kẻ tấn công có thể ghi lại quá trình bắt tay 4-chiều giữa máy khách và điểm truy cập và sử dụng dữ liệu này để bẻ khóa mật khẩu. Điều này sau đó sẽ bẻ khóa tất cả các khóa đã được sử dụng hoặc sẽ được sử dụng trong tương lai. Vì khả năng phá vỡ các thông điệp trong tương lai dựa trên các tin nhắn trong quá khứ nên tính năng bảo mật chuyển tiếp không được cung cấp bởi WPA2.

### **Wi-Fi Protected Access 3 (WPA3)**

*Truy cập Không dây được Bảo vệ 3 (Wi-Fi Protected Access - WPA3)* là sự kế thừa của WPA2. Được phát triển vào năm 2018, nó đang cố gắng để giải quyết những điểm yếu được tìm thấy trong WPA2. WPA3 cải thiện tính bảo mật của mã hóa bằng cách sử dụng Xác thực Đồng thời Bằng

nhau (Simultaneous Authentication of Equals - SAE) thay cho phương pháp xác thực PSK được sử dụng trong các phiên bản WPA trước đây. SAE sẽ được mô tả chi tiết ở phần sau của chương này. Sự thay đổi này cho phép WPA3-Personal sử dụng các cụm mật khẩu đơn giản nhưng tiêu tốn nhiều thời gian hơn để phá vỡ so với trường hợp của WPA/WPA2.

WPA3-Enterprise giới thiệu một loạt các nâng cấp, bao gồm các giao thức bảo mật độ-mạnh-tối-thiểu 192-bit và các công cụ mật mã như sau:

- **Mã hóa được Xác thực** Giao thức Chẽ độ Bộ đếm (Counter Mode Protocol/Galois 256-bit) (GCMP-256)
- **Lấy ra và xác nhận khóa** Mã Xác thực Thông điệp được Băm (Hashed Message Authentication Code) 384-bit (HMAC) với Thuật toán Băm An toàn (Secure Hash Algorithm - HMACSHA-384)
- **Thiết lập và xác thực khóa** trao đổi Đường cong Elliptic Diffie-Hellman (ECDH) và Thuật toán Ký Số Đường con Elliptic (ECDSA) bằng cách sử dụng một đường cong elliptic 384-bit
- **Bảo vệ khung quản lý mạnh mẽ** Mã Xác thực Thông điệp Galois Giao thức Toàn vẹn Quảng bá/Đa hướng (Broadcast/Multicast Integrity Protocol Galois Message Authentication Code - BIPGMAC-256)

WPA3 tích hợp với cơ sở hạ tầng xác thực doanh nghiệp ở phía sau, chẳng hạn như một máy chủ RADIUS. Nó có thể sử dụng đường cong elliptic trao đổi Diffie-Hellman và các giao thức Thuật toán Chữ ký số (DSA) đường cong elliptic để cung cấp một phương pháp xác thực mạnh mẽ. Giao thức WPA3 sử dụng mã Phản hồi Nhanh (Quick Response - QR) để người dùng kết nối thiết bị của họ với mạng "Wi-Fi CERTIFIED Easy Connect", cho phép họ quét mã QR trên thiết bị bằng điện thoại thông minh của họ. WPA3 cung cấp bí mật chuyển tiếp dựa trên phương pháp

mã hóa của nó, các thông điệp trước đó không cho phép giải mã trong tương lai.



**MÁCH NƯỚC CHO KỲ THI** WPA-2 sử dụng khóa được chia-sẻ-trước còn WPA-3 thì không. Nếu SAE được sử dụng thì đó là xác thực cấp-độ-3. Chuyển tiếp bảo mật chỉ được cung cấp bởi WPA-3.

### **Chế độ Bộ đếm/Giao thức CBC-MAC (CCMP)**

CCMP là viết tắt của *Chế độ Bộ đếm với Chuỗi Khối Mật mã – Giao thức Mã Xác thực Thông điệp* (*Counter Mode with Cipher Block Chaining – Message Authentication Code Protocol*) (hoặc *Counter Mode with CBC-MAC Protocol*). CCMP là một cơ chế mã hóa đóng gói dữ liệu được thiết kế để sử dụng không dây. CCMP trong thực tế là chế độ mà trong đó mã AES được sử dụng để mang lại tính toàn vẹn cho thông điệp. Không giống như WPA/TKIP, WPA2/CCMP đòi hỏi những phần cứng mới để thực hiện mã hóa AES.

### **Xác thực Đồng thời Bằng nhau (SAE)**

*Xác thực Đồng thời Bằng nhau* (*Simultaneous Authentication of Equals - SAE*) là một phương pháp trao đổi khóa dựa-trên-mật-khẩu được phát triển cho các mạng lưới. Được định nghĩa trong RFC 7664, nó sử dụng giao thức Dragonfly để thực hiện trao đổi khóa và an toàn trước sự giám sát thụ động. SAE không phải là một giao thức mới, nó đã tồn tại hơn một thập kỷ, nhưng việc kết hợp nó như một phần của các giao thức không dây ở cấp doanh nghiệp là tương đối mới. Nó rất phù hợp cho việc này bởi vì nó tạo ra một bí mật được chia sẻ mạnh mẽ về mặt mật mã để bảo mật dữ liệu khác. Do phương pháp tạo khóa không-kiến-thức (*zero-knowledge*) của nó, nó có khả năng chống lại các cuộc tấn công chủ động, bị động và từ điển. Là một giao thức ngang hàng, nó không dựa vào các

bên khác, vì vậy nó là một giải pháp thay thế cho việc sử dụng chứng nhận hoặc cơ quan quản lý tập trung để xác thực. Để thiết lập cấu hình SAE, bạn phải đặt tham số bảo mật "k" thành giá trị ít nhất là 40, theo khuyến nghị trong RFC 7664, "Dragonfly Key Exchange," cho tất cả các nhóm để ngăn rò rỉ thời gian.

### Các Giao thức Xác thực

Các mạng không dây cần các giao thức xác thực bảo mật. Những giao thức xác thực dưới đây nên được tìm hiểu cho kỳ thi Security+: EAP, PEAP, EAP-FAST, EAP-TLS, EAP-TTLS, IEEE 802.1X và Liên bang RADIUS.

### Giao thức Xác thực Có thể mở rộng (EAP)

*Giao thức Xác thực Có thể mở rộng (Extensible Authentication Protocol – EAP)* là một giao thức dành cho các mạng không dây để mở rộng các phương pháp xác thực đã được sử dụng bởi Giao thức Điểm-đến-Điểm (Point-to-Point Protocol – PPP). PPP là một giao thức đã được sử dụng một cách phổ biến để kết nối các thiết bị với nhau một cách trực tiếp. EAP được định nghĩa trong RFC 2284 (đã được thay thế bằng 3748). EAP có thể hỗ trợ cho nhiều cơ chế xác thực, bao gồm các token, thẻ thông minh, mật khẩu một-lần, và xác thực mã hóa khóa công khai. EAP đã được mở rộng thành rất nhiều phiên bản, một vài trong số đó được đề cập trong những phần sau đây.

### Giao thức Xác thực Có thể mở rộng được Bảo vệ (PEAP)

PEAP, hay *EAP được Bảo vệ*, đã được phát triển để bảo vệ giao tiếp EAP bằng cách đóng gói nó với Bảo mật Lớp Truyền tải (TLS). Đây là một tiêu chuẩn mở được Cisco, Microsoft và RSA cùng cộng tác phát triển. EAP đã được thiết kế với giả định là một kênh giao tiếp an toàn. PEAP cung cấp sự bảo vệ đó như một phần của giao thức thông qua một đường hầm TLS. PEAP được hỗ trợ rộng rãi bởi các nhà cung cấp để sử dụng trong các

mạng không dây. Wi-Fi Alliance đã bổ sung PEAP vào danh sách các giao thức được hỗ trợ của mình dành cho WPA/WPA2/WPA3.

### EAP-FAST

*EAP-FAST (Xác thực Mềm dẻo EAP thông qua Đường hầm Bảo mật – EAP Flexible Authentication via Secure Tunneling)* được mô tả trong RFC 4851 và được đề xuất bởi Cisco để thay thế cho LEAP, một phiên bản trước đó của EAP của Cisco. Nó cung cấp một giao thức đường hầm hạng nhẹ để hỗ trợ xác thực. Đặc điểm phân biệt là việc chuyển Thông tin đăng nhập Truy cập được Bảo vệ (Protected Access Credential – PAC) được sử dụng để thiết lập một đường hầm TLS thông qua đó thông tin đăng nhập của máy khách được xác minh. Wi-Fi Alliance đã bổ sung EAP-FAST vào danh sách các giao thức được hỗ trợ của mình dành cho WPA/WPA2/WPA3.

### EAP-TLS

*EAP-TLS* là một tiêu chuẩn mở của Lực lượng Đặc nhiệm Kỹ thuật Internet (Internet Engineering Task Force - IETF) (RFC 5216) sử dụng giao thức TLS để bảo mật quá trình xác thực. EAP-TLS dựa trên TLS, một nỗ lực để chuẩn hóa cấu trúc Lớp Cổng Bảo mật (SSL) để chuyển thông tin đăng nhập. Đây vẫn được coi là một trong những triển khai bảo mật nhất, chủ yếu vì các triển khai phổ biến sử dụng chứng chỉ phía-máy-khách. Điều này có nghĩa là kẻ tấn công cũng phải sở hữu khóa cho chứng chỉ phía-máy-khách để phá vỡ kênh TLS. Wi-Fi Alliance đã bổ sung EAP-TLS vào danh sách các giao thức được hỗ trợ của mình dành cho WPA/WPA2/WPA3.



**MÁCH NƯỚC CHO KỲ THI** KỲ THI Security+ sử dụng những câu hỏi liên quan đến các chứng chỉ và giao thức xác thực trong quá khứ. EAP-TLS để xác thực lẫn nhau yêu cầu các chứng chỉ của cả máy khách lẫn

máy chủ. PEAP và EAP-TTLS loại bỏ yêu cầu triển khai hoặc sử dụng các chứng chỉ máy khác. EAP-FAST không yêu cầu chứng chỉ máy khách.

### EAP-TTLS

*EAP-TTLS* (viết tắt của *EAP – Tunneled TLS*) là một biến thể của giao thức EAP-TLS. EAP-TTLS hoạt động giống như EAP-TLS, với máy chủ xác thực với máy khách bằng một chứng chỉ, nhưng giao thức này tạo ra đường hầm cho phía máy khách của xác thực, cho phép sử dụng các giao thức xác thực kế thừa như Giao thức Xác thực Mật khẩu (PAP) , Giao thức Xác thực Bắt tay Thủ thách (CHAP), Giao thức Xác thực Bắt tay Thủ thách của Microsoft (MS-CHAP) và MSCHAP-V2. Trong EAP-TTLS, quá trình xác thực được bảo vệ bởi đường hầm khỏi các cuộc tấn công người-trung-gian và mặc dù các chứng chỉ phía máy khách có thể được sử dụng nhưng chúng không bắt buộc phải có, điều này khiến cho việc thiết lập EAP-TLS trở nên dễ dàng hơn cho những máy khách không có chứng chỉ . Wi-Fi Alliance đã bổ sung EAP-TLS vào danh sách các giao thức được hỗ trợ của mình dành cho WPA/WPA2/WPA3.



### LƯU Ý

WPA3 được thiết kế để hoạt động cùng với một loạt các phương pháp EAP khác nhau trong một doanh nghiệp. Một trạm WPA3 thực hiện xác thực chứng chỉ máy chủ khi sử dụng các phương pháp EAP-TTLS, EAP-TLS, EAP và PEAP.



### MÁCH NƯỚC CHO KỲ THI

Có hai phần tử then chốt liên quan đến EAP. Đầu tiên, nó chỉ là một khuôn khổ để bảo mật quá trình xác thực, không phải là một phương pháp xác thực thực tế. Thứ hai, có rất nhiều biến thể đang tồn tại, và việc hiểu được những khác biệt và cách thức

nhận ra chúng trong thực tế, giữa EAP, PEAP, EAP-FAST, EAP-TLS, và EAP-TTLS là điều quan trọng đối với kỳ thi.

### **IEEE 802.1X**

*IEEE 802.1X* là một tiêu chuẩn xác thực hỗ trợ cho các dịch vụ xác thực dựa-trên-cổng giữa một người dùng và một thiết bị cấp phép, chẳng hạn như một bộ định tuyến biên. IEEE 802.1X thường được sử dụng trên các điểm truy cập không dây như một dịch vụ xác thực dựa-trên-cổng trước khi truy cập vào mạng không dây. WPA2-Enterprise sử dụng IEEE 802.1X để thiết lập một kết nối giữa các thiết bị. IEEE 802.1X trên mạng không dây sử dụng cả IEEE 802.1i hoặc giao thức dựa-trên-EAP như EAP-TLS hoặc PEAP-TLS.

### **Liên bang Dịch vụ Xác thực Từ xa Người dùng Quay số (RADIUS)**

Việc sử dụng một loạt các máy chủ RADIUS trong kết nối liên bang đã được sử dụng trong một số mạng *liên kết RADIUS* trên toàn thế giới. Một ví dụ là dự án eduroam (viết tắt của *chuyển vùng giáo dục*), kết nối người dùng của các tổ chức giáo dục trên toàn thế giới. Quá trình này tương đối đơn giản về mặt khái niệm, mặc dù các chi tiết kỹ thuật để duy trì hệ thống phân cấp của máy chủ RADIUS và bảng định tuyến là điều khó khăn trên quy mô toàn thế giới. Một người dùng đóng gói thông tin xác thực của họ tại một điểm truy cập cục bộ bằng một phương pháp giao thức đường hầm dựa-trên-chứng-chỉ. Máy chủ RADIUS đầu tiên xác định máy chủ RADIUS nào để gửi yêu cầu đến và từ đó người dùng được xác thực thông qua máy chủ RADIUS cục bộ của họ và kết quả được chuyển trở lại, cho phép tham gia vào mạng.

Bởi vì thông tin xác thực phải vượt qua nhiều mạng khác nhau nên các phương pháp EAP được giới hạn ở những mạng có chứng chỉ và thông tin đăng nhập để tránh mất thông tin xác thực trong quá trình truyền tải.

Loại nhận dạng liên hợp này ở quy mô toàn cầu thể hiện sức mạnh của các phương pháp RADIUS và EAP.



**MÁCH NƯỚC CHO KỲ THI** Liên kết RADIUS cho phép người dùng sử dụng những thông tin đăng nhập bình thường trên các mạng được tin cậy. Điều này cho phép người dùng trong một tổ chức được xác thực và truy cập đến nguồn tài nguyên trên mạng của tổ chức được tin cậy khác bằng cách sử dụng một bộ các thông tin đăng nhập.

### Các Phương pháp

Các phương pháp xác thực được sử dụng để cung cấp các dịch vụ xác thực (trong trường hợp các mạng không dây, từ xa) thông qua cấu hình của các giao thức được sử dụng để bảo vệ kênh giao tiếp. Phần này đề cập đến thiết lập cấu hình của các hệ thống để từ đó, các giao thức có thể được sử dụng để theo cách an toàn.

### Pre-shared Key so với Enterprise so với Open

Khi xây dựng một mạng không dây, bạn phải quyết định cách thức bạn dự định sử dụng bảo mật trên mạng như thế nào. Đặc biệt, bạn cần phải xác định xem ai sẽ được phép kết nối, và mức độ bảo vệ nào sẽ được cung cấp trong quá trình truyền tải dữ liệu giữa các thiết bị và điểm truy cập.

Cả WPA và WPA2, đã được thảo luận trước đây cũng trong chương này, đều có hai phương pháp để thiết lập một kết nối: PSK và Enterprise. PSK là viết tắt của khóa được-chia-sẻ-trước, vốn là một bí mật đã được chia sẻ giữa các người dùng. Một PSK thường được nhập vào như một mật khẩu có độ dài lên đến 63 ký tự. Khóa này phải được chia sẻ một cách bảo mật giữa các người dùng, vì nó là cơ sở của sự bảo mật được cung cấp bởi giao thức. PSK được chuyển đổi thành một khóa 256-bit để sau

đó được sử dụng để bảo mật mọi giao tiếp giữa thiết bị và điểm truy cập. PSK có một lỗ hổng đặc biệt: những PSK ngắn và đơn giản có nguy cơ bị tấn công kiểu brute force. Việc giữ cho PSK có độ dài ít nhất 20 ký tự ngẫu nhiên hay dài hơn sẽ giúp giảm nhẹ véc-tơ tấn công này.

Ở chế độ *Enterprise*, các thiết bị sử dụng IEEE 802.1X và một máy chủ xác thực RADIUS để cho phép kết nối. Phương pháp này cho phép sử dụng tên người dùng và mật khẩu và cung cấp các tùy chọn cấp-doanh-nghiệp như tích hợp kiểm soát truy cập mạng (NAC) và nhiều khóa ngẫu nhiên thay cho việc mọi người chia sẻ cùng một PSK. Nếu mọi người đều có cùng một PSK thì bí mật giữa các máy khách bị giới hạn ở các phương tiện khác và trong trường hợp một máy khách bị lỗi, những máy khách khác có thể bị xâm phạm.

Trong các hệ thống dựa-trên-WEP, sẽ có hai tùy chọn: xác thực Hệ thống Mở và xác thực khóa chia sẻ. *Xác thực Hệ thống Mở* không phải là xác thực thực sự mà thay vào đó, nó chỉ đơn thuần là chia sẻ khóa bí mật dựa trên SSID. Quá trình này rất đơn giản: ứng dụng di động đổi chiều SSID với điểm truy cập và yêu cầu khóa (được gọi là xác thực) cho điểm truy cập. Sau đó, điểm truy cập tạo ra mã xác thực (khóa, vì không có xác thực cụ thể của máy khách), là một số ngẫu nhiên chỉ được sử dụng trong phiên đó. Máy khách di động sử dụng mã xác thực và tham gia vào mạng. Phiên tiếp tục cho đến khi ngắt kết nối theo yêu cầu hoặc mất tín hiệu.



**MÁCH NƯỚC CHO KỲ THI** Hãy tìm hiểu về những khác biệt giữa xác thực PSK, Enterprise và Hệ thống Mở.

## Wi-Fi Protected Setup (WPS)

*Wi-Fi Protected Setup (WPS)* là một tiêu chuẩn bảo mật mạng được tạo ra để cung cấp cho người dùng một phương pháp dễ dàng để thiết lập cấu hình mạng không dây. Được thiết kế cho các mạng gia đình và mạng doanh nghiệp nhỏ, tiêu chuẩn này liên quan đến việc sử dụng mã PIN gồm tám-chữ-số để cấu hình các thiết bị không dây. WPS bao gồm một loạt các thông điệp EAP và đã được chứng minh là dễ bị tấn công kiểu brute force. Một cuộc tấn công thành công có thể tiết lộ mã PIN và sau đó là cụm mật khẩu WPA/WPA2 và cho phép các bên trái phép truy cập vào mạng. Hiện tại, biện pháp giảm thiểu hiệu quả duy nhất là tắt WPS. Wi-Fi Alliance, khi không dùng WPS nữa, đã thêm phương pháp Easy Connect để thay thế và loại bỏ các điểm yếu của WPS.

## Captive Portals

*Cổng cố định (captive portal)* đề cập đến một kỹ thuật cụ thể sử dụng một máy khách HTTP để xử lý xác thực trên mạng không dây. Thường được sử dụng tại các điểm truy cập công cộng, một cổng cố định sẽ mở trình duyệt web đi đến một trang xác thực. Việc này xảy ra trước khi người dùng được cấp quyền truy cập vào mạng. Điểm truy cập sử dụng cơ chế đơn giản này bằng cách chặn tất cả các gói và trả lại trang web để đăng nhập. Máy chủ web thực sự cung cấp trang xác thực có thể nằm trong phần ngăn cách của mạng, chặn quyền truy cập vào Internet cho đến khi người dùng xác thực thành công.



## MÁCH NƯỚC CHO KỲ THI

Các cổng cố định là rất phổ biến trong các quán cà phê, sân bay, khách sạn và cửa hàng. Người dùng chấp thuận các điều kiện, lượt xem, và quảng cáo được đề xuất, cung cấp một địa chỉ email hoặc yêu cầu xác thực khác và được cấp quyền truy cập vào cổng.

## Những Cân nhắc Cài đặt

Hệ thống không dây không chỉ là các giao thức. Việc lắp đặt một hệ thống không dây chức năng trong một ngôi nhà cũng dễ dàng như cắm một điểm truy cập không dây và tiến hành kết nối. Tuy nhiên, trong một doanh nghiệp, nơi cần có nhiều điểm truy cập, việc cấu hình sẽ mất nhiều công sức hơn. Khảo sát địa điểm là điều cần thiết để xác định điểm truy cập và vị trí đặt ăng-ten thích hợp, cũng như các kênh và mức công suất cần thiết.

Các yếu tố phải được xem xét dựa trên sự lan truyền và giao thoa của tín hiệu. Truyền tín hiệu là một chức năng của ăng-ten, cường độ tín hiệu và bối cảnh vật lý của một cơ sở vật chất, bao gồm cả các cấu trúc can thiệp. Tất cả những điều này đều được giải quyết bằng cách sử dụng khảo sát địa điểm, máy phân tích Wi-Fi và phần mềm để tối ưu hóa vị trí lắp đặt điểm truy cập.

## Khảo sát Địa điểm

Khi phát triển bản đồ phạm vi cho một địa điểm xây dựng phức tạp, bạn cần phải tính đến nhiều yếu tố - đặc biệt là các bức tường, các nguồn gây nhiễu và sơ đồ mặt bằng. *Khảo sát địa điểm* bao gồm một số bước: lập bản đồ sơ đồ mặt bằng, kiểm tra nhiễu sóng RF, kiểm tra vùng phủ sóng RF và phân tích vật liệu qua phần mềm. Phần mềm có thể đề xuất vị trí của các điểm truy cập. Đây là một ví dụ về một phân tích khảo sát địa điểm dự đoán.

Sau khi triển khai các AP, bạn khảo sát lại địa điểm, lập bản đồ kết quả so với phân tích dự đoán trong khi xem xét cường độ tín hiệu và tỷ-lệ-nhiễu-tín-hiệu. Một trong những kết quả của việc này là bản đồ nhiệt, hoặc biểu diễn đồ họa của cường độ tín hiệu. Điều này sẽ được thảo luận trong phần tiếp theo, và Hình 20-1 minh họa phần bản đồ nhiệt của một cuộc khảo sát địa điểm trông sẽ như thế nào. Quá trình phân tích cường

độ tín hiệu thực tế này được gọi là khảo sát địa điểm phân tích tại chỗ và được sử dụng để xác nhận kết quả của phân tích dự đoán. Nếu cần thiết, các điểm truy cập có thể được di chuyển để cải thiện cường độ tín hiệu trong những khu vực đang có vấn đề.

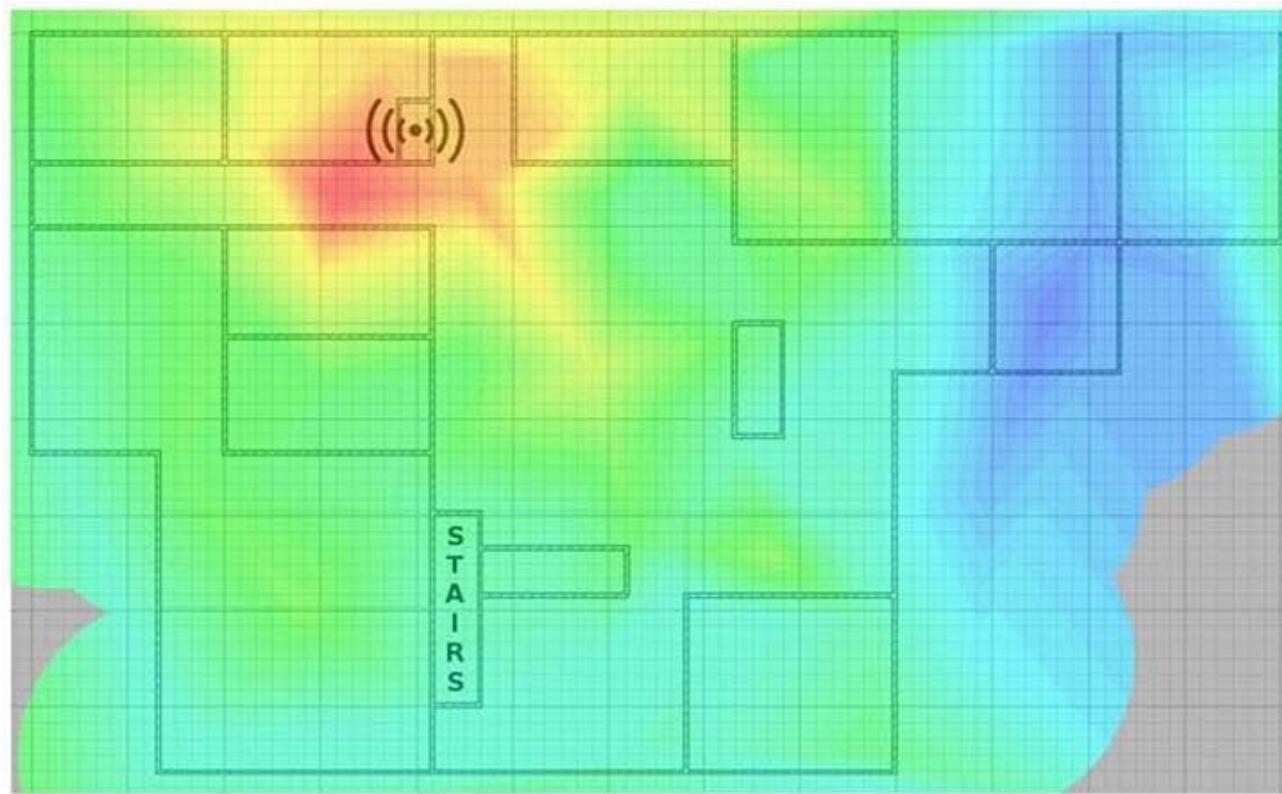
Một công dụng quan trọng khác của khảo sát địa điểm là kiểm tra các mạng không dây hiện có để tìm ra các khu vực có hiệu suất bị suy giảm hoặc thậm chí là các điểm truy cập giả mạo. Cả hai trường hợp này đều đại diện cho những rủi ro đối với mạng không dây và cách duy nhất để tìm ra các tình trạng này là theo dõi chúng một cách định kỳ.



**MÁCH NƯỚC CHO KỲ THI** Các mạng không dây phụ thuộc vào tín hiệu sóng radio để hoạt động. Điều quan trọng là phải tìm hiểu kiểu ăng-ten, lắp đặt, và các khảo sát địa điểm được sử dụng để đảm bảo độ bao phủ thích hợp của một địa điểm, bao gồm những khu vực bị chặn bởi các bức tường, nhiễu tín hiệu và tiếng vọng.

### Bản đồ Nhiệt

Một *bản đồ nhiệt* không dây là một bản đồ về phạm vi và cường độ bao phủ của tín hiệu không dây. Thông thường, một bản đồ nhiệt thể hiện sơ đồ bố trí của một căn phòng, một tầng, hay cơ sở vật chất được phủ bởi một trình bày dạng đồ họa của tín hiệu không dây. Các bản đồ nhiệt được tạo ra bằng cách sử dụng một trình phân tích không dây và một phần mềm để hỗ trợ phân tích cường độ tín hiệu không dây dưới dạng một sơ đồ bố trí đồ họa. Điều này cho phép quản trị viên mạng tìm kiếm những khu vực có tín hiệu yếu và cân nhắc vị trí lắp đặt các điểm truy cập thay thế. Một ví dụ về một bản đồ nhiệt được minh họa trong Hình 20-1. Các sắc thái khác nhau cho biết cường độ tín hiệu, chỉ ra nơi tiếp nhận sóng mạnh và nơi nào là yếu.



**Hình 20-1** Một mẫu bản đồ nhiệt Không dây



### MÁCH NƯỚC CHO KỲ THI

Một khảo sát địa điểm là một quá trình xác định cường độ [tín hiệu mạng] không dây, bản đồ nhiệt là một bản đồ là kết quả và là một phần của quá trình khảo sát.

### Bộ phân tích Wi-Fi

Bộ phân tích Wi-Fi cung cấp một phương tiện để xác định cường độ tín hiệu và sự nhiễu kênh. Một bộ phân tích Wi-Fi là một thiết bị RF được sử dụng để đo lường cường độ và chất lượng của tín hiệu. Nó có thể xác định xem liệu cường độ tín hiệu Wi-Fi có đầy đủ không, và liệu có những thiết bị nào đang cạnh tranh trên một kênh cụ thể không. Điều này cho phép một kỹ sư phân bổ tín hiệu về cả cường độ lẫn kênh để cải thiện hiệu suất Wi-Fi.

## Chồng chéo Kênh

Tín hiệu vô tuyến Wi-Fi tồn tại ở những tần số cụ thể: 2,4 GHz và 5,0 GHz. Mỗi tín hiệu này được chia thành một loạt các kênh và việc truyền dữ liệu thực tế diễn ra trên các kênh này. Các phiên bản Wi-Fi của IEEE 802.11 (a, b, g, n) hoạt động với tần số kênh 2400 MHz và 2500 MHz, do đó có thuật ngữ 2,4 GHz cho hệ thống. 100 MHz ở giữa được chia thành 14 kênh mỗi kênh 20 MHz. Kết quả là, mỗi kênh chồng chéo được với tối đa bốn kênh khác. Nếu bạn đã sử dụng các kênh lân cận, sự chồng chéo này làm cho thông lượng mạng không dây khá kém. Vì lý do này, hầu hết các hệ thống 2,4 GHz sử dụng các kênh 1, 6 và 11. Khi nhiều điểm truy cập ở gần nhau, có thể có vấn đề với các tín hiệu cạnh tranh nhau. Trong một căn hộ, nếu bạn nhận thấy hàng xóm của mình đang sử dụng kênh 2 và 10, thì bạn nên chuyển thiết bị của mình sang kênh 6 để cải thiện cường độ tín hiệu trong kênh của mình. Hầu hết các bộ định tuyến không dây sử dụng chức năng tự động để quản lý chức năng này, nhưng trong trường hợp sự tắc nghẽn đang xảy ra, việc tìm hiểu cách phân phối tín hiệu thông qua khảo sát địa điểm và phân vùng thiết bị của bạn thành các kênh có sẵn sẽ cải thiện được hiệu suất.

Ngoài việc chỉ cải thiện các vấn đề về chồng chéo kênh, Liên minh Wi-Fi (Wi-Fi Alliance) đã cải thiện thông lượng hệ thống thông qua việc sử dụng các tiêu chuẩn mới hơn, bao gồm 802.11ac và 802.11ax. Các hệ thống này sử dụng một tập hợp các cơ chế mã hóa khác nhau và phân bổ tần số để tăng thông lượng trong môi trường Wi-Fi dày đặc chẳng hạn như các cuộc tụ tập công cộng lớn. Các phương pháp này được gọi là Wi-Fi 6, hoặc, trong trường hợp cụ thể là 802.11ax, Không dây Hiệu quả Cao (High Efficiency Wireless - HEW).

## Lắp đặt Điểm Truy cập Không dây (WAP)

Vị trí lắp đặt điểm truy cập không dây (WAP) trông có vẻ đơn giản. Thực hiện khảo sát địa điểm, xác định vị trí tối ưu dựa trên cường độ tín hiệu RF, và bạn đã hoàn thành. Nhưng không nhanh như vậy đâu. Các điểm truy cập cũng cần nguồn điện, do đó, việc cung cấp nguồn điện cho vị trí lắp đặt cũng có thể là một vấn đề. Và nếu điểm truy cập sẽ được kết nối với mạng, thì tính khả dụng của kết nối mạng cũng là một vấn đề cần cân nhắc. Những vấn đề này thực sự có thể khó khăn hơn trong môi trường gia đình vì người dùng gia đình không có khả năng phải gánh chịu chi phí chạy nguồn và kết nối mạng chuyên dụng tới điểm truy cập. Để giúp giải quyết vấn đề này trong các mạng gia đình và mạng nhỏ, nhiều nhà cung cấp có bộ mở rộng Wi-Fi dựa-trên-lưới (mesh-based) cho phép mở rộng tín hiệu tần số vô tuyến Wi-Fi (RF) thông qua rơ-le, nhưng điều này có thể phải trả giá bằng thông lượng nếu mạng trở nên bị tắc nghẽn với các thiết bị.

Vì lý do bảo mật, bạn nên biết rằng tín hiệu Wi-Fi đi xuyên qua các bức tường, vì vậy việc đặt các điểm truy cập ở nơi chúng tạo ra vùng phủ sóng lớn nằm bên ngoài cơ sở có thể dẫn đến việc người ngoài truy cập được vào hệ thống của bạn. Việc bảo vệ điểm truy cập khỏi sự truy cập vật lý cũng rất quan trọng. Phối hợp vị trí lắp đặt AP với khảo sát địa điểm là điều quan trọng để giải quyết các vấn đề về vị trí kém dẫn đến phạm vi phủ sóng kém, tín hiệu bị chiếm đoạt và chi phí thông lượng liên quan đến việc bổ sung thêm quá nhiều AP hoặc bộ mở rộng.

## Bộ kiểm soát và Bảo mật Điểm Truy cập

Các điểm truy cập không dây là những kết nối vật lý với cơ sở hạ tầng mạng của bạn và nên được bảo vệ giống như vậy. Việc cung cấp *bộ kiểm soát và bảo mật điểm truy cập* thích hợp bao gồm cả các biện pháp phòng ngừa bảo mật về mặt vật lý và luận lý. Trường hợp bảo mật về mặt luận

lý là trọng tâm chính của chương này, ngăn chặn người dùng trái phép truy cập vào các kênh. Bảo mật vật lý cũng quan trọng như vậy, nếu không muốn nói là hơn thế, và các thiết bị và kết nối mạng thực tế phải được đặt ở một vị trí mà kẻ tấn công không thể tiếp cận được. Điều này đặc biệt đúng đối với các kết nối bên ngoài, nơi không ai có thể quan sát thấy một ai đó đang thao tác về mặt vật lý trên thiết bị.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với bảo mật không dây. Chương được mở đầu bằng việc xem xét một số giao thức mật mã được sử dụng trong giao tiếp không dây, bao gồm các giao thức WPA2, WPA3, CCMP và SAE. Phần tiếp theo là về các giao thức xác thực. Trong phần này, chúng ta đã khám phá một loạt các giao thức EAP, bao gồm PEAP, EAP-FAST, EAP-TLS và EAP-TTLS. Tiếp theo là IEEE 802.1X và RADIUS.

Phần tiếp theo của chương kiểm tra các phương pháp thiết lập cấu hình các dịch vụ không dây. Trong phần này, các chủ đề về khóa chia-sẻ-trước, Enterprise so với Open, thiết lập Wi-Fi được bảo vệ và cổng cố định đã được đề cập. Chương này đã kết thúc bằng một phần về những cân nhắc khi lắp đặt, bao gồm khảo sát địa điểm, bản đồ nhiệt và bộ phân tích Wi-Fi. Chồng chéo kênh, vị trí điểm truy cập không dây, và các vấn đề liên quan đến bộ điều khiển và bảo mật điểm truy cập đã kết thúc chương này.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Sử dụng một mã PIN 6-số để thiết lập một kết nối không dây là một phần của điều nào dưới đây?

  - A. WPA
  - B. SAE
  - C. WPA3
  - D. WPS.
2. Vai trò của EAP trong các kết nối không dây là gì?

  - A. Đây là một khuôn khổ để thiết lập kết nối.
  - B. Đây là một khuôn khổ để chuyển thông tin xác thực.
  - C. Đây là một khuôn khổ để bảo mật quá trình xác thực.
  - D. Đây là một phương pháp mã hóa thực tế được sử dụng trong quá trình xác thực.
3. Điểm khác biệt chính giữa WPA2-Personal và WPA2-Enterprise là gì?

  - A. Sử dụng bí mật được-chia-sẻ-trước
  - B. Số lượng người dùng được hỗ trợ đồng thời
  - C. Chi phí cấp phép trên cơ sở theo-người-dùng
  - D. Sử dụng SAE cho các kết nối.
4. Bạn đang thiết lập một Wi-Fi hotspot cho khách viếng thăm. Phương pháp tốt nhất để thiết lập kết nối là gì?

  - A. Truy cập mở
  - B. Mật khẩu đã được đăng sẵn có tại địa điểm một cách trực quan
  - C. Sử dụng một giải pháp PSK
  - D. Cổng cố định.

5. Biện pháp bảo mật nhất để thiết lập kết nối với một điểm truy cập Wi-Fi là gì?
  - A. CCMP
  - B. Giao thức SAE
  - C. WPA2
  - D. IEEE 802.1X.
6. Một khảo sát địa điểm sẽ tiết lộ tất cả những điều gì dưới đây, ngoại trừ một điều?
  - A. Vị trí lắp đặt điểm truy cập tối ưu
  - B. Vị trí cổng cố định
  - C. Phân bổ kênh
  - D. Tốc độ kết nối trên toàn bộ địa điểm.
7. Chuyển tiếp bảo mật tồn tại đối với những giao thức nào dưới đây?
  - A. WPS
  - B. WPA2
  - C. WPA3
  - D. Tất cả.
8. Sếp của bạn đã yêu cầu bạn thiết lập kết nối không dây tại một địa điểm mới của công ty. Tuy nhiên, cô ấy lo lắng về việc lập kế hoạch, phạm vi phủ sóng và bảo mật liên quan đến việc bố trí AP. Cô ấy muốn bạn đảm bảo phạm vi bao phủ và giải quyết các lo ngại về bảo mật. Bạn nên cân nhắc sử dụng tùy chọn nào sau đây khi thiết lập vị trí mới này? (Hãy chọn ba).
  - A. Liên kết RADIUS
  - B. Khảo sát địa điểm
  - C. Bộ phân tích Wi-Fi
  - D. Bản đồ nhiệt.

- 9.** Bạn đang sử dụng EAP-TTLS, trong đó bao gồm những khía cạnh độc đáo nào?
- A.** Nó không thể được sử dụng trong WPA3.
  - B.** Nó yêu cầu các chứng chỉ phía-máy-khách.
  - C.** Nó không thể được sử dụng cùng với CHAP.
  - D.** Nó dễ thiết lập hơn các lược đồ EAP cũ hơn.
- 10.** Giao thức nào cho phép chuyển các giao thức xác thực kế thừa như PAP, CHAP và MS-CHAP?
- A.** EAP-TTLS
  - B.** EAP-TLS
  - C.** SAE
  - D.** CCMP.

## Đáp án

1. **D.** Thiết lập Wi-Fi được Bảo vệ (WPS) sử dụng mã PIN gồm tám chữ số để thiết lập kết nối giữa các thiết bị.
2. **C.** EAP chỉ là một khuôn khổ để bảo mật quá trình xác thực, không phải là một phương pháp mã hóa thực tế.
3. **A.** WPA2-Personal sử dụng PSK, trong khi WPA2-Enterprise thì không.
4. **D.** Một cổng cố định là một phương pháp yêu cầu người dùng đăng nhập vào hệ thống của bạn. Những thứ này thường thấy ở các quán cà phê, sân bay, khách sạn và cửa hàng.
5. **B.** Việc sử dụng SAE, một phần của WPA3, hiện là cách an toàn nhất để thiết lập kết nối qua mạng không dây.
6. **B.** Cổng cố định là các vị trí theo-hướng-phần-mềm mà người dùng được trỏ đến, không phải là một phần của cấu hình Wi-Fi vật lý.
7. **C.** Bí mật chuyển tiếp chỉ khả dụng thông qua WPA3. Điều này là do phương pháp thiết lập kết nối không thể quan sát được.
8. **B, C, và D.** Khảo sát địa điểm chuyên nghiệp, các bộ phân tích Wi-Fi và bản đồ nhiệt đối với các cài đặt mạng không dây và vị trí lắp đặt điểm truy cập thích hợp được sử dụng để đảm bảo phạm vi bao phủ và các mối quan tâm về bảo mật. Câu trả lời A không chính xác vì liên kết RADIUS cho phép người dùng sử dụng thông tin đăng nhập bình thường của họ trên các mạng đáng tin cậy.
9. **D.** EAP-TTLS dễ thiết lập hơn các mạng EAP khác vì khả năng hoạt động mà không cần chứng chỉ phía máy khách của nó.
10. **A.** Giao thức EAP-TTLS tạo đường hầm cho phía máy khách của xác thực, cho phép sử dụng các giao thức xác thực kế thừa như Giao thức Xác thực Mật khẩu (PAP), Giao thức Xác thực Bắt tay Thử thách (CHAP), MS-CHAP và MS-CHAP-V2.

## Chương 21 Các Giải pháp Bảo mật Di động

### Các Giải pháp Bảo mật Di động

Trong chương này bạn sẽ

- Tìm hiểu các phương pháp kết nối các thiết bị di động,
- Tìm hiểu các kiểu thiết bị di động khác nhau và sự quản lý chúng,
- Được giới thiệu về các chính sách và thủ tục đối với thiết bị di động,
- Xem xét một số mô hình triển khai các thiết bị di động.

Đã có một sự hội tụ đáng kinh ngạc giữa việc sử dụng thiết bị di động của doanh nghiệp và cá nhân. Sự hội tụ của năng lực lưu trữ đám mây và Phần mềm như một Dịch vụ (SaaS) đang thay đổi đáng kể bối cảnh sử dụng thiết bị di động. Sự hiện diện phổ biến của các thiết bị di động và nhu cầu truy cập dữ liệu liên tục trên nhiều nền tảng đã dẫn đến những thay đổi đáng kể trong cách thức các thiết bị di động đang được sử dụng cho các mục đích cá nhân và công việc. Trước đây, các công ty cung cấp thiết bị di động cho nhân viên của họ để sử dụng chủ yếu cho công việc, nhưng chúng sẵn sàng để sử dụng cho mục đích cá nhân. Với các thiết bị liên tục xuất hiện và công nghệ thay đổi liên tục, nhiều công ty đang cho phép nhân viên mang theo thiết bị của riêng họ để sử dụng cho cả mục đích cá nhân lẫn công việc.

**Mục tiêu Chứng nhận** Chương này bao gồm mục tiêu 3.5 của kỳ thi CompTIA Security+: Đưa ra một kịch bản, hãy triển khai các giải pháp di động bảo mật.

## Các Phương pháp và Bộ Nhận Kết nối

Các thiết bị di động, do bản chất di động của chúng, đòi hỏi một phương tiện không-dây để kết nối tới một mạng. Thông thường, kết nối này về phía doanh nghiệp là thông qua Internet, nhưng về phía thiết bị di động là một loạt các tùy chọn đang tồn tại. Vị trí và cách thức các thiết bị di động kết nối với mạng có thể được quản lý bởi doanh nghiệp bằng cách kiến trúc nên khía cạnh kết nối di động của mạng không dây của nó. Phần này sẽ đề cập đến các phương thức kết nối phổ biến, bao gồm di động, Wi-Fi, Bluetooth, NFC, hồng ngoại và USB. Các phương thức kết nối điểm-đến-điểm và điểm-đến-đa-điểm sẽ được giải thích. Bộ thu chuyên dụng, chẳng hạn như GPS và RFID, sẽ được đề cập đến ở cuối phần này.

### Mạng di động (cellular)

Các kết nối *di động* sử dụng các mạch điện thoại di động, ngày nay thường là thế hệ thứ tư (4G) hoặc LTE về bản chất, mặc dù một số dịch vụ 3G vẫn còn tồn tại. Một trong những điểm mạnh của mạng di động là các mạng lưới rộng khắp trên toàn quốc đã được triển khai, khiến cho tín hiệu mạnh sẵn có ở hầu hết mọi nơi có mật độ dân số hợp lý. Điểm yếu tương ứng là khoảng cách trong dịch vụ di động vẫn còn tồn tại ở các vùng sâu vùng xa.

Khi quyển sách này đang được viết, thế giới viễn thông đang chuyển sang 5G, hình thức di động mới nhất. Sự thay đổi này sẽ xảy ra trước tiên ở những khu vực đông dân cư và sau đó sẽ lan tỏa ra khắp toàn cầu. 5G không chỉ là một mạng mới hơn, nhanh hơn mà nó còn là một tái thiết kế để cải thiện giao tiếp mạng thông qua thông lượng lớn hơn, độ trễ thấp hơn, kiểm soát chất-lượng-dịch-vụ tốt hơn và sự khác biệt của dịch vụ. Nó được thiết kế để xử lý việc tải xuống những video trực tuyến, cuộc gọi âm thanh tiêu chuẩn và truyền dữ liệu từ vô số thiết bị Internet of Things (IoT) nhỏ hơn, tất cả đều sẽ có mức dịch vụ phù hợp. 5G sẽ hỗ

trợ cho các dịch vụ mạng tạo điều kiện cho việc chuyển sang kết nối và truyền dữ liệu rộng rãi qua các mạng di động. 5G không chỉ là một chiếc điện thoại di động tốt hơn, nó còn là mạng cho kỷ nguyên kết nối dữ liệu.

## **Wi-Fi**

*Wi-Fi* đề cập đến các phương thức liên lạc vô tuyến được phát triển theo Wi-Fi Alliance. Các hệ thống này tồn tại trên dải phổ tần số 2,4 và 5 GHz và các mạng được xây dựng bởi cả doanh nghiệp bạn được liên kết và các bên-thứ-ba. Phương pháp truyền thông này rất phổ biến với các nền tảng máy tính và tương đối dễ triển khai và an toàn. Bảo mật mạng Wi-Fi được đề cập rất nhiều trong Chương 20, "Bảo mật Không dây".

## **Bluetooth**

*Bluetooth* là một giao thức không dây công-suất-thấp, tầm ngắn-đến-trung-bình, truyền ở dải tần 2,4 GHz, nghĩa là cùng băng tần được sử dụng cho 802.11. Ý tưởng ban đầu cho giao thức không dây tầm-ngắn (khoảng 32 feet) này là truyền dữ liệu trong mạng khu vực cá nhân (personal area network - PAN). Bluetooth truyền và nhận dữ liệu từ một loạt các thiết bị khác nhau, phổ biến nhất là điện thoại di động, máy tính xách tay, máy in và thiết bị âm thanh. Điện thoại di động đã thúc đẩy sự phát triển của Bluetooth rất nhiều và thậm chí đã phổ biến Bluetooth vào những kiểu ô tô mới như một bộ điện thoại di động rảnh-tay. Những tiến bộ trong công suất máy phát, độ lợi ăng ten và việc sử dụng môi trường hoạt động đã mở rộng phạm vi lên đến 3,800 mét trong một số ứng dụng ngoài trời.

Bluetooth đã trải qua một số bản phát hành. Phiên bản 1.1 đã là phiên bản thành công về mặt thương mại đầu tiên, với phiên bản 1.2 được phát hành vào năm 2007 và khắc phục một số vấn đề được tìm thấy trong 1.1. Phiên bản 1.2 cho phép tốc độ lên đến 721 Kbps và cải thiện khả năng chống nhiễu. Phiên bản 1.2 tương thích ngược với phiên bản 1.1. Với tốc

độ tiến bộ và tuổi thọ của hầu hết các mặt hàng công nghệ, Bluetooth 1 series về cơ bản đã tuyệt chủng. Bluetooth 2.0 giới thiệu tốc độ dữ liệu nâng cao (enhanced data rate - EDR), cho phép truyền tải lên đến 3.0 Mbps. Bluetooth 3.0 có khả năng sử dụng kênh 802.11 để đạt tốc độ lên đến 24 Mbps. Phiên bản hiện tại là tiêu chuẩn Bluetooth 4.0, hỗ trợ ba chế độ: Cổ điển, Tốc độ Cao và Năng lượng Thấp.

Bluetooth 4 đã giới thiệu một phương pháp mới để hỗ trợ cho việc thu thập dữ liệu từ các thiết bị tạo ra dữ liệu với tốc độ rất thấp. Một số thiết bị, chẳng hạn như các thiết bị y tế, chỉ có thể thu thập và truyền dữ liệu với tốc độ thấp. Tính năng này, được gọi là Bluetooth Năng lượng Thấp (Bluetooth Low Energy - BLE), được thiết kế để tổng hợp dữ liệu từ các cảm biến khác nhau như máy đo nhịp tim, nhiệt kế, v.v... và có tên thương mại là Bluetooth Smart. Bluetooth 5 tiếp tục những cải tiến của BLE, cải thiện phạm vi và tốc độ dữ liệu của BLE.

Khi Bluetooth trở nên phổ biến, mọi người bắt đầu cỗ gắng tìm ra những lỗ hổng trong đó. Bluetooth có tính năng thiết lập cấu hình thiết bị dễ dàng để cho phép giao tiếp mà không cần các địa chỉ mạng hoặc cổng. Bluetooth sử dụng ghép nối (pairing) để thiết lập nên mối quan hệ tin cậy giữa các thiết bị. Để thiết lập sự tin tưởng đó, các thiết bị quảng bá các khả năng và yêu cầu mã xác nhận. Để giúp duy trì bảo mật, hầu hết các thiết bị đều yêu cầu nhập mã khóa vào cả hai thiết bị, và điều này ngăn chặn một cuộc tấn công kiểu-mật-mã mặc định. Quảng cáo giao thức của Bluetooth về các dịch vụ và thuộc tính ghép nối là nơi bắt đầu một số vấn đề bảo mật. Bluetooth phải luôn tắt chế độ có thể phát hiện trừ khi bạn đang cố tình ghép nối với một thiết bị. Bảng dưới đây hiển thị các phiên bản và tốc độ Bluetooth.

Phiên bản Bluetooth	Phạm vi Tối đa	Tốc độ Dữ liệu Tối đa
3.0 (Cổ điển)	< 200 feet	25 Mbps
4.X	200 feet/60 mét	25 Mbps
5.X	985 feet/300 mét	50 Mbps

Trong Bluetooth phiên bản 5.X, tốc độ dữ liệu khác nhau tương ứng với phạm vi khác nhau, với tốc độ cao hơn ở phạm vi thấp hơn hỗ trợ nhiều thiết bị giàu-dữ-liệu hơn và tốc độ thấp hơn có phạm vi dài hơn để hỗ trợ cho các thiết bị IoT có tốc-độ-dữ-liệu-thấp-hơn. Bluetooth 5 sử dụng một dải phổ tần số khác, đòi hỏi phần cứng mới và bị hạn chế khả năng tương thích ngược, nhưng nó được thiết kế cho các mạng cục bộ trong tương lai với mức tiêu thụ điện năng thấp, phần cứng rẻ tiền, triển khai nhỏ và tốc độ dữ liệu có thể mở rộng so với các cân nhắc về phạm vi.

## NFC

*Giao tiếp trường lân cận (near field communication – NFC)* là một tập hợp các công nghệ không dây cho phép các điện thoại thông minh và các thiết bị khác thiết lập liên lạc vô tuyến khi chúng ở gần nhau - thường là trong phạm vi 10 cm (3,9 in) trở xuống. Công nghệ này đã không được sử dụng nhiều cho đến gần đây, khi nó bắt đầu được sử dụng để chuyển dữ liệu giữa các điện thoại di động và trong các hệ thống thanh toán di động. NFC có khả năng sẽ trở thành một công nghệ được sử dụng nhiều trong những năm tới khi công nghệ này có nhiều ứng dụng và thẻ điện thoại thông minh tiếp theo chắc chắn sẽ bao gồm điều này như một chức năng tiêu chuẩn. Hiện tại, NFC phụ thuộc rất nhiều vào phạm vi bảo mật rất ngắn của nó, mặc dù các ứng dụng sử dụng nó cũng có các cơ chế bảo mật riêng.

## Hồng ngoại

*Hồng ngoại (IR)* là một dải năng lượng điện từ nằm ngay bên ngoài điểm cuối màu đỏ của quang phổ màu mà mắt thường có thể nhìn thấy được. IR đã được sử dụng trong các thiết bị điều khiển từ xa trong rất nhiều năm qua. IR ra mắt lần đầu trong mạng máy tính như một phương pháp không dây để kết nối với máy in. Giờ đây, bàn phím không dây, chuột không dây và các thiết bị di động trao đổi dữ liệu qua IR, nó dường như có mặt ở khắp mọi nơi. IR cũng có thể được sử dụng để kết nối các thiết bị trong cấu hình mạng, nhưng khá chậm so với các công nghệ không dây khác. IR không thể xuyên qua các bức tường mà thay vào đó sẽ bật ra khỏi chúng. Nó cũng không thể xuyên qua các vật thể rắn khác, do đó, nếu bạn xếp một vài món đồ trước bộ thu phát, tín hiệu sẽ bị mất. Bởi vì IR có thể được nhìn thấy bởi tất cả những gì đang nằm trong phạm vi nên bất kỳ bảo mật mong muốn nào đều phải nằm trên cơ chế truyền dẫn cơ sở.

## USB

*Universal Serial Bus (USB)* đã trở thành tiêu chuẩn phổ biến để kết nối các thiết bị bằng cáp. Điện thoại di động có thể truyền dữ liệu và sạc pin qua USB. Máy tính xách tay, máy tính để bàn, thậm chí cả máy chủ đều có cổng USB dành cho nhu cầu kết nối dữ liệu khác nhau. Nhiều thiết bị, chẳng hạn như điện thoại, máy tính bảng và thiết bị IoT, cũng sử dụng cổng USB, mặc dù nhiều thiết bị đang chuyển sang đầu nối USB loại C (USB-C), mới hơn và nhỏ hơn. Cổng USB đã mở rộng đáng kể khả năng của người dùng để kết nối thiết bị với máy tính. Cổng USB tự động nhận dạng thiết bị đang được cắm vào hệ thống và thường hoạt động mà người dùng không cần thêm trình điều khiển hoặc thiết lập cấu hình phần mềm. Điều này đã tạo ra một quân đoàn các thiết bị USB, từ máy nghe nhạc đến thiết bị ngoại vi cho đến thiết bị lưu trữ - hầu như bất cứ thứ gì có thể sử dụng hoặc cung cấp dữ liệu được kết nối qua USB.

Điều thú vị nhất trong số các thiết bị này là, vì mục đích bảo mật, các thiết bị lưu trữ đều dựa trên bộ nhớ flash USB. Các ổ USB, về cơ bản là bộ nhớ flash với giao diện USB trong thiết bị thường có kích thước bằng ngón tay cái của bạn, mang lại một cách thức để di chuyển tập tin một cách dễ dàng từ máy tính này sang máy tính khác. Khi được cắm vào cổng USB, các thiết bị này sẽ tự động hoạt động và hoạt động giống như bất kỳ ổ đĩa nào khác được gắn vào máy tính. Kích thước nhỏ và dung lượng tương đối lớn, cùng với khả năng đọc-ghi tức thời, làm滋生 các vấn đề về bảo mật. Chúng có thể được sử dụng bởi một cá nhân một cách dễ dàng với mục đích xấu để che giấu việc xóa các tập tin hoặc dữ liệu khỏi tòa nhà hoặc để đưa các tập tin độc hại vào tòa nhà và vào mạng công ty.

Các đầu nối USB có nhiều kích cỡ và hình dạng. Đối với việc sử dụng di động, có USB mini, USB micro và bây giờ là USB-C, nhanh hơn và có thể đảo ngược (không cần quan tâm đến mặt nào). Ngoài ra còn có các đầu nối loại A và loại B, với các yếu tố hình thức khác nhau. USB nguyên thủy cung cấp tốc độ dữ liệu lên đến 480 Mbps, với USB 3 tăng lên 5 Gbps, 3,1 đến 10 Gbps và 3,2 đến 20 Gbps. USB 4 cung cấp tốc độ lên đến 40 Gbps.

### **Điểm-tới-Điểm**

Tín hiệu vô tuyến truyền ra ngoài từ một ăng-ten phát, và cuối cùng được nhận bởi một ăng-ten thu. Giao tiếp *điểm-đến-điểm* được định nghĩa là giao tiếp với một điểm cuối ở mỗi đầu - một máy phát duy nhất nói chuyện với một máy thu duy nhất. Thuật ngữ này được chuyển sang kết nối mạng, trong đó một kênh liên lạc giữa hai thực thể tách biệt được gọi là *điểm-đến-điểm*. Ví dụ về giao tiếp điểm-đến-điểm bao gồm Bluetooth, trong đó điều này là bắt buộc bởi giao thức và USB, trong đó nó bị bắt buộc bởi các kết nối vật lý.

## Điểm-tới-Đa-điểm

Giao tiếp *điểm-đến-đa-điểm* có nhiều máy thu cho một tín hiệu được truyền đi. Khi một thông điệp được gửi đi ở chế độ quảng bá, nó có nhiều người nhận và được gọi là giao tiếp *điểm-đến-đa-điểm*. Hầu hết các hệ thống mạng và *dựa-trên-vô-tuyến* đều có khả năng là *điểm-đến-đa-điểm*, từ một máy phát đến nhiều máy thu, chỉ bị giới hạn bởi các giao thức.



## MÁCH NƯỚC CHO KỲ THI

Hãy nhớ rằng một kết nối *điểm-đến-điểm*

là giữa hai thiết bị (một thiết bị tới một thiết bị) trong khi các kết nối *điểm-đến-đa-điểm* là một (thiết bị) đến nhiều (thiết bị).

## Hệ thống Định vị Toàn cầu (GPS)

*Hệ thống Định vị Toàn cầu (GPS)* là một loạt các vệ tinh cung cấp phạm vi phủ sóng gần như toàn cầu của các tín hiệu thời gian có độ chính xác cao, và khi nhiều tín hiệu được kết hợp, có thể tạo ra dữ liệu về vị trí chính xác trong cả ba chiều. Máy thu GPS, hoạt động ở dải băng tần 6 GHz, nhỏ, rẻ và đã được thêm vào nhiều thiết bị di động, đã trở nên phổ biến. Khả năng có được thời gian chính xác, vị trí chính xác và sử dụng phép toán vi phân, tốc độ chính xác đã chuyển đổi nhiều năng lực của thiết bị di động. GPS cho phép xác định vị trí địa lý, định vị địa lý và một loạt các khả năng khác.

## RFID

*Thẻ nhận dạng tần số vô tuyến (radio frequency identification - RFID)* được sử dụng trong một loạt các trường hợp sử dụng. Từ thiết bị theo dõi đến khóa theo dõi, sự tuần tự hóa độc đáo của các thiết bị cảm biến từ xa này đã khiến cho chúng trở nên hữu ích trong nhiều ứng dụng. Thẻ RFID có nhiều dạng khác nhau và có thể được phân loại là chủ động hoặc thụ động. Các thẻ chủ động có một nguồn điện, trong khi các thẻ thụ

động sử dụng năng lượng RF được truyền cho chúng để tạo ra năng lượng. Thẻ RFID được sử dụng như một phương tiện nhận dạng và có lợi thế hơn mã vạch là không cần phải nhìn thấy chúng, chỉ trong phạm vi sóng vô tuyến - thường từ vài cm đến 200 mét, tùy thuộc vào loại thẻ. Thẻ RFID được sử dụng trong một loạt các tình huống bảo mật, bao gồm cả các hệ thống nhận dạng không tiếp xúc như thẻ thông minh.

Thẻ RFID có nhiều mối quan tâm về bảo mật, đầu tiên và quan trọng nhất, vì chúng được kết nối thông qua năng lượng RF nên an ninh vật lý là một thách thức. Bảo mật đã được công nhận là một vấn đề quan trọng đối với hệ thống thẻ RFID vì chúng tạo thành một phương tiện nhận dạng và cần phải xác thực và giữ tính bảo mật cho việc truyền tải dữ liệu. Một số tiêu chuẩn có liên quan đến việc đảm bảo luồng dữ liệu RFID, bao gồm ISO/IEC 18000 và ISO/IEC 29167 cho các phương pháp mật mã để hỗ trợ tính bảo mật, không thể truy nguyên, xác thực thẻ và đầu đọc, và quyền riêng tư qua-mạng-không-dây, trong khi ISO/IEC 20248 chỉ định cấu trúc dữ liệu chữ ký kỹ thuật số để sử dụng trong các hệ thống RFID.

Một số kiểu tấn công khác nhau có thể được thực hiện đối với các hệ thống RFID. Đầu tiên là chống lại chính các thiết bị RFID - các chip và đầu đọc. Hình thức tấn công thứ hai là chống lại kênh giao tiếp giữa thiết bị và đầu đọc. Loại tấn công thứ ba là chống lại người đọc và hệ thống back-end. Loại cuối cùng này là một cuộc tấn công CNTT/Hệ thống Thông tin tiêu chuẩn, tùy thuộc vào các giao diện được sử dụng (web, cơ sở dữ liệu, v.v...) và do đó không được đề cập thêm. Các cuộc tấn công vào kênh giao tiếp tương đối dễ dàng bởi vì các tần số vô tuyến đã được biết và các thiết bị tồn tại để giao tiếp với các thẻ. Hai cuộc tấn công chính là phát lại và nghe trộm. Trong một cuộc tấn công phát lại, thông tin RFID được ghi lại và sau đó phát lại sau đó, đối với trường hợp huy hiệu truy cập dựa trên RFID, nó có thể được đọc trong nhà hàng từ xa và sau

đó được phát lại tại điểm truy nhập thích hợp để được đi vào cửa. Trong trường hợp nghe trộm, dữ liệu có thể được thu thập, theo dõi chuyển động của các thẻ cho bất kỳ mục đích nào cần thiết bởi một bên trái phép. Cả hai cuộc tấn công này đều dễ dàng bị đánh bại bằng cách sử dụng các tiêu chuẩn bảo mật nói trên.

Nếu nghe trộm là khả thi, vậy còn các cuộc tấn công của người-trung-gian thì sao? Những cuộc tấn công kiểu này chắc chắn có thể xảy ra vì chúng sẽ là sự kết hợp của một hành động đánh hơi (nghe trộm), sau đó là một cuộc tấn công phát lại (giả mạo). Điều này dẫn đến câu hỏi liệu RFID có thể được nhân bản hay không. Và một lần nữa, câu trả lời là có, nếu thông tin RFID không được bảo vệ thông qua một thành phần mật mã.



## MÁCH NƯỚC CHO KỲ THI

Các phương pháp kết nối di động khác nhau rất có ích đối với các câu hỏi dựa-trên-hiệu-suất, có nghĩa là bạn cần chú ý đến tình huống đã được trình bày và chọn phương pháp kết nối tốt nhất. Hãy xem xét tốc độ dữ liệu, mục đích, khoảng cách, v.v... để chọn đáp án tốt nhất.

## Quản lý Thiết bị Di động (MDM)

Kiến thức về khái niệm *quản lý thiết bị di động (MDM)* là điều thiết yếu trong môi trường thiết bị được kết nối ngày nay. MDM bắt đầu như một thuật ngữ thị trường để chỉ một tập hợp các yếu tố bảo vệ thường được sử dụng liên quan đến thiết bị di động. Khi được xem như một tập hợp các tùy chọn bảo mật toàn diện dành cho thiết bị di động, mọi công ty đều phải có và thực thi chính sách MDM. Chính sách nên bắt buộc những điều sau:

- Khóa thiết bị bằng mật khẩu mạnh,
- Mã hóa dữ liệu trên thiết bị,
- Tự động khóa thiết bị sau một khoảng thời gian không hoạt động nhất định,
- Khả năng khóa thiết bị từ xa nếu bị mất hoặc bị đánh cắp,
- Khả năng tự động xóa thiết bị sau một số lần đăng nhập thất bại nhất định,
- Khả năng xóa thiết bị từ xa nếu thiết bị bị mất hoặc bị đánh cắp.

Các chính sách về mật khẩu nên mở rộng cho các thiết bị di động, bao gồm cả khóa thiết bị và, nếu có thể, tự động xóa dữ liệu. Chính sách của công ty về mã hóa dữ liệu trên thiết bị di động nên nhất quán với chính sách về mã hóa dữ liệu trên máy tính xách tay. Nói cách khác, nếu bạn không yêu cầu mã hóa máy tính xách tay, thì bạn có nên yêu cầu mã hóa cho thiết bị di động không? Không có câu trả lời thống nhất cho câu hỏi này bởi vì trên thực tế, số lượng thiết bị di động di động nhiều hơn so với máy tính xách tay và dễ bị thất lạc hơn. Cuối cùng, đây là một câu hỏi rủi ro mà cấp quản lý phải giải quyết: rủi ro là gì và chi phí của các phương án được sử dụng là gì? Điều này cũng đặt ra một câu hỏi lớn hơn: thiết bị nào nên có mã hóa như là một cơ chế bảo vệ an ninh cơ bản? Đó là theo kiểu thiết bị hay theo người dùng dựa trên việc dữ liệu nào sẽ gặp rủi ro? May mắn thay, các giải pháp MDM tồn tại, khiến cho các lựa chọn trở thành có thể quản lý được.



**MÁCH NƯỚC CHO KỲ THI** Quản lý thiết bị di động (MDM) là một thuật ngữ thị trường để chỉ một tập hợp các phần tử bảo vệ được sử dụng một cách phổ biến thích hợp với các thiết bị di động. Trong những môi

trường doanh nghiệp, MDM cho phép đăng ký thiết bị, cung cấp, cập nhật, theo dõi, thực thi chính sách, và năng lực quản lý ứng dụng.

### **Quản lý Ứng dụng**

Các thiết bị di động sử dụng các ứng dụng để thực hiện công việc xử lý dữ liệu của chúng. Phương pháp cài đặt, cập nhật, và quản lý các ứng dụng được thực hiện thông qua một hệ thống được gọi là phần mềm *quản lý ứng dụng*. Các nền tảng nhà cung cấp khác nhau có các phương pháp khác nhau để quản lý chức năng này, với hai đối thủ chính là Google Store dành cho các thiết bị Android và Apple App Store dành cho các thiết bị iOS. Cả thiết bị Apple và Android đều có các hoạt động được tích-hợp như một phần của hệ điều hành (OS) để đảm bảo sự tích hợp liền mạch với các kho ứng dụng tương ứng và các giải pháp MDM khác.

### **Quản lý Nội dung**

Các ứng dụng không phải là thông tin duy nhất di chuyển đến thiết bị di động. Nội dung cũng đang di chuyển và các tổ chức cần có một phương tiện để quản lý nội dung cho thiết bị di động. Ví dụ, có thể tốt nếu có được và chỉnh sửa một số loại thông tin trên thiết bị di động, trong khi những thông tin khác nhạy cảm hơn sẽ bị chặn khỏi quyền truy cập của thiết bị di động. *Quản lý nội dung* là tập hợp các hành động được sử dụng để kiểm soát các vấn đề về nội dung, bao gồm nội dung nào có sẵn và cho ứng dụng nào trên thiết bị di động. Hầu hết các tổ chức đều có chính sách sở hữu dữ liệu thiết lập rõ ràng quyền sở hữu của họ đối với dữ liệu, bất kể dữ liệu được lưu trữ trên thiết bị thuộc sở hữu của tổ chức hay thiết bị do nhân viên sở hữu. Tuy nhiên, quản lý nội dung doanh nghiệp còn tiến xa hơn một bước, kiểm tra nội dung nào thuộc về các thiết bị cụ thể và sau đó sử dụng các cơ chế để thực thi các quy tắc này. Một lần nữa, các giải pháp MDM tồn tại để hỗ trợ vấn đề bảo mật này liên quan đến thiết bị di động.

## Làm sạch Từ xa

Ngày nay, các thiết bị di động có mặt ở khắp mọi nơi và rất dễ dàng bị mất và bị đánh cắp. Khi dữ liệu của doanh nghiệp tồn tại trên các thiết bị này, việc quản lý dữ liệu, ngay cả khi thiết bị bị mất, thực sự là một mối quan tâm. Hơn nữa, không có khả năng một thiết bị bị mất hoặc bị đánh cắp có thể được khôi phục bởi chủ sở hữu, do đó, ngay cả dữ liệu đã mã hóa được lưu trữ trên thiết bị cũng dễ bị giải mã hơn. Nếu kẻ trộm có thể có thiết bị của bạn trong một thời gian dài, chúng có thể sử dụng tất cả thời gian mà chúng muốn để cố gắng giải mã dữ liệu của bạn. Do đó, nhiều công ty thích làm sạch từ xa một thiết bị bị mất hoặc bị đánh cắp. Việc *làm sạch từ xa* các thiết bị di động thường xóa dữ liệu được lưu trữ trên thiết bị và đặt lại thiết bị về cài đặt gốc. Có một tình huống khó xử trong việc sử dụng các thiết bị BYOD lưu trữ cả dữ liệu cá nhân và dữ liệu doanh nghiệp. Việc làm sạch thiết bị thường xóa tất cả dữ liệu, cả dữ liệu cá nhân và doanh nghiệp. Do đó, một chính sách của công ty yêu cầu làm sạch thiết bị đã mất có thể đồng nghĩa với việc người dùng thiết bị sẽ mất những dữ liệu và hình ảnh cá nhân. Phần mềm kiểm soát các vùng chứa dữ liệu riêng biệt, một cho doanh nghiệp và một dành cho cá nhân, đã được đề xuất nhưng vẫn chưa phải là một lựa chọn chính.

Đối với hầu hết các thiết bị, làm sạch từ xa chỉ có thể được quản lý thông qua các ứng dụng trên thiết bị, chẳng hạn như Outlook cho e-mail, lịch và danh bạ cũng như các giải pháp MDM cho tất cả dữ liệu. Đối với các thiết bị Apple và Android, hệ điều hành cũng có khả năng thiết lập thiết bị để khóa từ xa và khôi phục lại cài đặt gốc, giúp làm sạch thiết bị một cách hiệu quả.

## Hàng rào địa lý (Geofencing)

*Hàng rào địa lý* là việc sử dụng hệ thống định vị toàn cầu (GPS) và/hoặc công nghệ nhận dạng tần số vô tuyến (RFID) để tạo ra một hàng rào ảo

xung quanh một vị trí cụ thể và phát hiện khi nào thì các thiết bị di động vượt qua hàng rào. Điều này cho phép thiết bị được nhận ra bởi những người khác, dựa trên vị trí, và thực hiện các hành động. Hàng rào địa lý được sử dụng trong tiếp thị để gửi thông điệp đến các thiết bị ở một khu vực cụ thể, chẳng hạn như gần điểm bán hàng hoặc chỉ để đếm số lượng khách hàng tiềm năng. Hàng rào địa lý đã được sử dụng cho những người làm việc từ xa, thông báo cho cấp quản lý khi họ đến địa điểm làm việc từ xa, cho phép những thứ như kết nối mạng được kích hoạt cho họ. Việc sử dụng hàng rào địa lý thực sự chỉ bị giới hạn bởi trí tưởng tượng của một người nào đó.

Có thể tắt tính năng hàng rào địa lý thông qua thiết bị. Trên các thiết bị của Apple, chỉ cần tắt dịch vụ định vị. Mặc dù vậy, để ngăn chặn hoàn toàn việc theo dõi thiết bị, bạn phải tắt radio bằng Chế độ trên máy bay.

### **Định vị trí địa lý**

Hầu hết các thiết bị di động giờ đây có khả năng sử dụng GPS để theo dõi vị trí của thiết bị. Rất nhiều ứng dụng phụ thuộc rất nhiều vào vị trí GPS, chẳng hạn như các dịch vụ định-vị-thiết-bị, các ứng dụng bản đồ, ứng dụng giám sát lưu lượng giao thông, và các ứng dụng định vị doanh nghiệp lân cận như các trạm xăng và các nhà hàng. Những công nghệ như vậy có thể bị khai thác để theo dõi chuyển động và vị trí của thiết bị di động, vốn được gọi là *định vị trí địa lý*. Việc theo dõi này có thể được sử dụng để hỗ trợ khôi phục thiết bị bị mất.

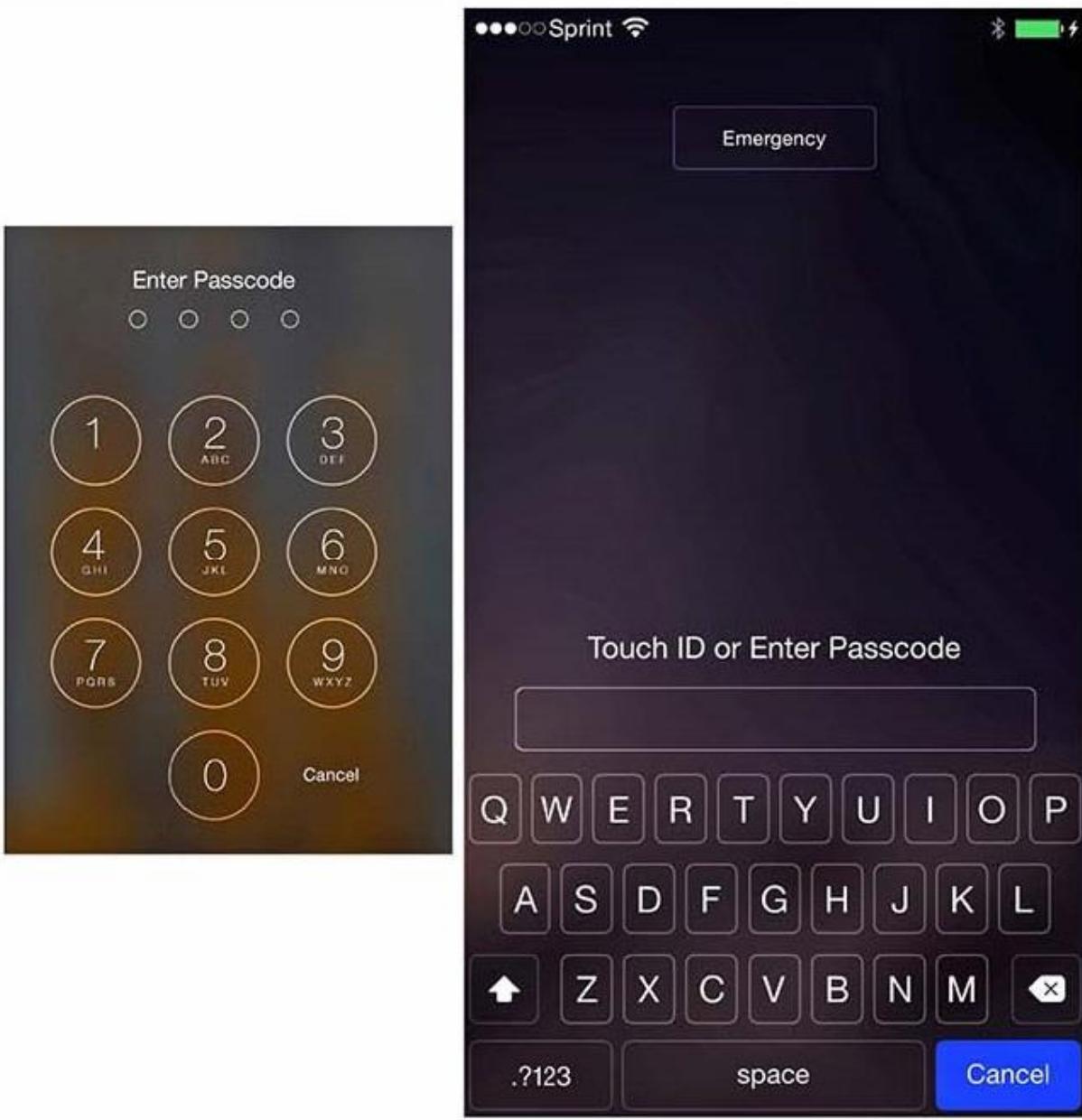


**MÁCH NƯỚC CHO KỲ THI** Hãy hiểu được sự khác biệt giữa hàng rào địa lý và định vị trí địa lý. Chúng sẽ khiến cho bạn bị nhiễu.

## Khóa Màn hình

Hầu hết các chính sách doanh nghiệp liên quan đến các thiết bị di động đều bắt buộc sử dụng khả năng *khóa-màn-hình* của các thiết bị di động. Điều này thường bao gồm việc nhập một mật mã hoặc mã PIN để mở khóa thiết bị. Chúng tôi khuyên bạn nên thực thi việc khóa màn hình cho tất cả các thiết bị di động. Chính sách của bạn liên quan đến chất lượng của mật mã phải nhất quán với chính sách mật khẩu của công ty của bạn. Tuy nhiên, nhiều công ty chỉ thực thi việc sử dụng khóa-màn-hình. Do đó, người dùng có xu hướng sử dụng mật mã tiện lợi hoặc dễ-nhớ. Một số thiết bị cho phép các mật mã phức tạp. Như được minh họa trong Hình 21-1, màn hình thiết bị bên trái chỉ hỗ trợ một mật mã iOS đơn giản, giới hạn ở bốn số, trong khi màn hình thiết bị bên phải hỗ trợ mật mã có độ dài không xác định và có thể chứa các ký tự chữ và số.

Một số hình thức khóa màn hình được nâng cao sẽ hoạt động kết hợp với tính năng làm sạch thiết bị. Nếu như mật mã được nhập sai một số lần đã được chỉ định, thiết bị sẽ được làm sạch một cách hoàn toàn tự động. Apple đã biến điều này thành một tùy chọn trên các thiết bị iOS. Apple cũng cho phép khóa thiết bị từ xa từ tài khoản iCloud của người dùng. Thiết bị Android có một loạt các tùy chọn, bao gồm cả việc sử dụng ứng dụng làm khóa màn hình.



**Hình 21-1** Khóa màn hình của iOS



## MÁCH NƯỚC CHO KỲ THI

Các thiết bị di động yêu cầu các cơ chế bảo mật cơ bản về khóa màn hình, khóa (lockout), làm sạch thiết bị, và mã hóa để bảo vệ những thông tin nhạy cảm chứa trong thiết bị.

## Các Dịch vụ Thông báo Đẩy

*Dịch vụ thông báo đẩy* là những dịch vụ cung cấp thông tin đến thiết bị di động mà không cần một yêu cầu cụ thể từ thiết bị. Những thông báo đẩy được nhiều ứng dụng trên thiết bị di động sử dụng để cho biết nội dung đã được cập nhật. Các phương pháp thông báo đẩy thường là duy nhất cho nền tảng, với dịch vụ Thông báo Đẩy của Apple dành cho các thiết bị của Apple và Android Tin nhắn từ Đám mây đến Thiết bị (Cloud to Device Messaging) là những ví dụ. Nhiều dịch vụ máy chủ back-end khác có các dịch vụ máy chủ tương tự để cập nhật nội dung của chúng. Vì thông báo đẩy cho phép di chuyển thông tin từ các nguồn bên ngoài đến thiết bị nên điều này sẽ có một số tác động đến bảo mật, chẳng hạn như vị trí thiết bị và khả năng tương tác với thiết bị. Ví dụ, có thể đẩy thiết bị để phát ra âm thanh, ngay cả khi âm thanh đó bị tắt tiếng trên thiết bị.

## Mật khẩu và mã PIN

*Mật khẩu và mã PIN* là những biện pháp bảo mật phổ biến được sử dụng để bảo vệ thiết bị di động khỏi việc bị sử dụng trái phép. Đây là những công cụ thiết yếu và nên được sử dụng trong mọi trường hợp và được bắt buộc bởi chính sách của công ty. Các quy tắc về mật khẩu đã được đề cập đến trong suốt quyển sách này cũng áp dụng cho các thiết bị di động, trong thực tế, thậm chí có thể còn nhiều hơn vậy. Một thao tác vuốt màn hình dựa-trên-cử-chỉ đơn giản có thể được khám phá bằng cách nhìn vào hình mẫu dấu trên màn hình. Nếu thao tác vuốt là duy nhất để mở khóa điện thoại thì hình mẫu để mở khóa có thể bị nhìn thấy, và tính bảo mật sẽ bị mất thông qua phương pháp này. Làm sạch hoặc làm bẩn toàn bộ màn hình là giải pháp rõ ràng.

## Sinh trắc học

*Sinh trắc học* được sử dụng trên nhiều loại thiết bị di động như một phương tiện để kiểm soát truy cập. Rất nhiều thiết bị trong số này có khả

năng nhận dạng kém-hoàn-hảo, và các cảm biến sinh trắc học khác nhau đã được chứng minh là có thể bẻ khóa được, như đã được chứng minh trong nhiều bài thuyết trình về bảo mật tại các hội nghị. Những phương pháp sinh trắc học mới nhất, nhận dạng bằng khuôn mặt, dựa trên hình ảnh camera chụp lại khuôn mặt của người dùng khi họ đang cầm điện thoại. Vì các cảm biến sinh trắc học này đã được chứng minh là có thể vượt qua được, chúng nên được coi là tính năng tiện lợi chứ không phải tính năng bảo mật. Các chính sách quản lý phải phản ánh thực tế này và phải quy định rằng các phương pháp này không được dựa vào để bảo mật những dữ liệu quan trọng.

### **Xác thực Nhận-biết-Ngữ-cảnh**

*Xác thực theo ngữ cảnh (Context-aware authentication)* là việc sử dụng thông tin theo ngữ cảnh - người dùng này là ai, họ đang yêu cầu tài nguyên nào, máy họ đang sử dụng, cách họ được kết nối, v.v... - để đưa ra quyết định xác thực xem có cho phép người dùng truy cập tới tài nguyên được yêu cầu hay không. Mục đích là ngăn người dùng cuối, thiết bị hoặc kết nối mạng trái phép có thể truy cập vào dữ liệu của công ty. Phương pháp tiếp cận này có thể được sử dụng, chẳng hạn, để cho phép người dùng đã được cấp phép truy cập vào tài nguyên dựa trên mạng từ bên trong văn phòng nhưng từ chối cùng một người dùng truy cập nếu họ đang kết nối qua một mạng Wi-Fi công cộng.

### **Ngăn vùng chứa (Containerization)**

*Containerization* trên thiết bị di động đề cập đến việc chia thiết bị thành một loạt các ngăn chứa (container) - một ngăn chứa tài liệu liên quan đến công việc, ngăn còn lại chứa đồ vật cá nhân. Các ngăn chứa có thể tách biệt các ứng dụng, dữ liệu - hầu như mọi thứ trên thiết bị. Một số giải pháp quản lý thiết bị di động (MDM) hỗ trợ việc kiểm soát từ xa đối với ngăn chứa công việc. Điều này cho phép một trường hợp sử dụng

mạnh mẽ hơn nhiều để pha trộn các vấn đề về công việc và cá nhân trên một thiết bị duy nhất. Hầu hết các giải pháp MDM đều cung cấp khả năng mã hóa các ngăn chứa, đặc biệt là ngăn chứa liên quan đến công việc, do đó cung cấp thêm một lớp bảo vệ khác cho dữ liệu.

### **Phân đoạn Lưu trữ**

Trên các thiết bị di động, có thể sẽ rất khó để giữ cho dữ liệu cá nhân tách biệt với dữ liệu công ty. *Phân đoạn lưu trữ* tương tự như containerization, trong đó nó thể hiện sự phân tách về mặt logic của bộ lưu trữ trong đơn vị. Một số công ty đã phát triển khả năng tạo các ngăn chứa ảo riêng biệt để giữ cho dữ liệu cá nhân tách biệt với dữ liệu và ứng dụng của công ty. Đối với các thiết bị được sử dụng để xử lý dữ liệu công ty có độ nhạy cảm cao, hình thức bảo vệ này rất được khuyến khích.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng containerization và phân đoạn lưu trữ là những công nghệ giữ cho dữ liệu cá nhân tách biệt khỏi dữ liệu công ty trên các thiết bị.

### **Mã hóa Toàn bộ Thiết bị**

Cũng giống như máy tính xách tay nên được bảo vệ bằng mã hóa toàn bộ ổ đĩa để bảo vệ dữ liệu trong trường hợp bị mất hoặc bị đánh cắp, bạn có thể cần xem xét việc *mã hóa toàn bộ thiết bị* (*full device encryption - FDE*) cho các thiết bị di động đang được sử dụng bởi nhân viên của tổ chức của bạn. Các thiết bị di động có nhiều khả năng bị mất hoặc bị đánh cắp hơn, vì vậy bạn nên cân nhắc việc mã hóa dữ liệu trên thiết bị di động của tổ chức mình. Ngày càng có nhiều thiết bị di động được sử dụng để truy cập và lưu trữ dữ liệu quan trọng của doanh nghiệp hoặc thông tin nhạy cảm khác. Việc bảo vệ thông tin trên thiết bị di động đang trở thành điều bắt buộc trong doanh nghiệp. Đây là một công nghệ mới nổi,

vì vậy, bạn sẽ cần phải hoàn thành một số phân tích thị trường nghiêm túc để xác định sản phẩm thương mại nào đáp ứng được nhu cầu của bạn.

### **Các Thiết bị Di động**

Các thiết bị di động có thể mang lại nhiều lợi ích cho doanh nghiệp về mặt chức năng kinh doanh, nhưng với việc gia tăng tiện ích này đi kèm với những rủi ro bổ sung. Có nhiều cách khác nhau để quản lý rủi ro, bao gồm việc sử dụng mã hóa và các biện pháp bảo vệ điểm đầu cuối đã được thiết kế cho các thiết bị di động. Bạn có thể sử dụng một số phương pháp luận khác nhau để quản lý các thiết bị di động và những phương pháp này sẽ được đề cập trong các phần sau đây.

### **Mô-đun Bảo mật Phần cứng MicroSD (HSM)**

*MicroSD HSM (MicroSD Hardware Security Module)* là một mô-đun bảo mật phần cứng ở dạng MicroSD. Thiết bị này cho phép bạn một phương tiện lưu trữ an toàn có thể di động cho nhiều loại khóa mật mã. Các thiết bị này đi kèm với một ứng dụng quản lý các chức năng HSM điển hình tương ứng với các khóa, bao gồm sao lưu, khôi phục và rất nhiều chức năng PKI.

### **MDM/Quản lý Thiết bị đầu cuối Hợp nhất (UEM)**

Phần mềm *MDM* là một ứng dụng chạy trên thiết bị di động và, khi đã được kích hoạt, có thể quản lý các khía cạnh của thiết bị, bao gồm kết nối và các chức năng. Mục đích của một ứng dụng MDM là để biến thiết bị thành một thiết bị mà chức năng bị hạn chế theo chính sách doanh nghiệp. *Quản lý thiết bị đầu cuối hợp nhất (UEM)* là một giải pháp quản lý thiết bị đầu cuối cấp-doanh-nghiệp có thể bao gồm mọi thiết bị điểm đầu cuối, từ máy tính để bàn đến máy tính xách tay, từ điện thoại đến các thiết bị di động khác, máy tính bảng và thậm chí một số thiết bị đeo được trên người. Ý tưởng đằng sau UEM là mở rộng bộ chức năng từ MDM để bao gồm tất cả các thiết bị điểm đầu cuối, kể cả việc mang lại nhiều

chức năng hơn dưới sự kiểm soát của doanh nghiệp. UEM có thể quản lý việc triển khai các tài nguyên của công ty vào một điểm đầu cuối, cung cấp quyền kiểm soát những thứ như truy cập ứng dụng và tài nguyên, kiểm soát các thiết bị từ xa và giám sát hoạt động của thiết bị. Các giải pháp MDM và UEM cũng hỗ trợ quản lý tài sản, bao gồm cả vị trí và theo dõi.

### **Quản lý Ứng dụng Di động (MAM)**

Thiết bị di động mang rất nhiều ứng dụng cùng với chúng vào một doanh nghiệp. Mặc dù các giải pháp MDM có thể bảo vệ doanh nghiệp khỏi các ứng dụng được cài đặt trên thiết bị nhưng cũng cần phải quản lý các ứng dụng của công ty trên thiết bị. Việc triển khai, cập nhật và thiết lập cấu hình các ứng dụng trên thiết bị đòi hỏi một giải pháp doanh nghiệp có khả năng mở rộng và cung cấp cho việc cài đặt, cập nhật và quản lý các ứng dụng nội bộ trên một bộ thiết bị di động. Bộ công cụ *quản lý ứng dụng di động (MAM)* cung cấp những khả năng này trong doanh nghiệp.



**MÁCH NƯỚC CHO KỲ THI** Việc phân biệt giữa các ứng dụng MDM, UEM, và MAM được thực hiện theo chức năng. MAM kiểm soát các ứng dụng nội-bộ trên thiết bị. MDM kiểm soát dữ liệu trên thiết bị, tách biệt nó khỏi những dữ liệu chung trên thiết bị. UEM là một giải pháp kiểm soát thiết bị đầu cuối hoàn chỉnh hoạt động trên hầu hết mọi hình thức thiết bị điểm đầu cuối, bất kể chúng có di động hay không.

### **SEAndroid**

*Android* được *Tăng cường Bảo mật (Security Enhanced Android – SEAndroid)* là một phiên bản di động của bản phân phối Linux được Tăng cường Bảo mật (SELinux) để thực thi kiểm soát truy cập bắt buộc mandatory access control – MAC) trên tất cả các tiến trình, kể cả các tiến

trình đang chạy với đặc quyền root/superuser. SELinux có một nguyên tắc bao trùm: từ chối theo mặc định. Điều này có nghĩa rằng bất kỳ thứ gì không được cho phép một cách rõ ràng sẽ bị từ chối.

### **Thực thi và Giám sát**

Các chính sách của tổ chức của bạn liên quan đến thiết bị di động nên nhất quán với các chính sách bảo mật máy tính hiện có của bạn. Các chương trình đào tạo của bạn nên bao gồm những hướng dẫn về bảo mật thiết bị di động. Các biện pháp kỷ luật phải nhất quán. Các chương trình giám sát của bạn nên được tăng cường để bao gồm cả việc giám sát và kiểm soát các thiết bị di động.

### **Kho lưu trữ Ứng dụng Bên-Thứ-ba**

Rất nhiều thiết bị di động có các kho ứng dụng của nhà-sản-xuất-tương-ứng, từ đó có thể tải ứng dụng xuống các thiết bị tương ứng của chúng. Các kho ứng dụng này được doanh nghiệp coi là *kho ứng dụng của bên-thứ-ba*, vì nội dung mà họ cung cấp không đến từ phía người dùng và doanh nghiệp. Hiện tại có hai kho ứng dụng chính: Apple App Store dành cho thiết bị iOS và Google Play dành cho thiết bị Android. Apple App Store được xây dựng trên nguyên tắc độc quyền và các yêu cầu bảo mật nghiêm ngặt được thực thi rất chặt chẽ đối với các ứng dụng được cung cấp. Google Play có ít hạn chế hơn, và điều này đã dẫn đến một số vấn đề về bảo mật bắt nguồn từ ứng dụng. Việc quản lý những ứng dụng mà người dùng có thể thêm vào thiết bị là điều thiết yếu vì rất nhiều ứng dụng trong số này có thể gây ra rủi ro về bảo mật cho tổ chức. Vấn đề này trở nên phức tạp hơn đáng kể với các thiết bị do nhân-viên-sở-hữu và quyền truy cập vào các kho dữ liệu của công ty. Các tùy chọn phân đoạn đã được thảo luận trước đó để tách biệt giữa không gian công việc và không gian cá nhân được cung cấp trên một số lượng hạn chế các thiết bị di động, do đó, khả năng kiểm soát quyền truy cập này trở nên có vấn đề.

Hầu như tất cả việc phân đoạn đều được thực hiện thông qua một ứng dụng bổ sung - giải pháp MDM. Các thiết bị được phép truy cập vào thông tin nhạy cảm của công ty nên được giới hạn ở các thiết bị thuộc-quyền-sở-hữu-của-công-ty, cho phép kiểm soát chặt chẽ hơn.

### **Rooting/Jailbreaking**

Một cách tấn công phổ biến liên quan đến thiết bị di động là bẻ khóa (jailbreak). *Bẻ khóa* là một quá trình mà theo đó, người dùng leo thang đặc quyền của họ, vượt qua các kiểm soát và giới hạn của hệ điều hành. Người dùng vẫn có đầy đủ chức năng của thiết bị, nhưng cũng có thêm các năng lực bổ sung, bỏ qua những hạn chế người dùng do hệ-điều-hành-áp-đặt. Có một số trường phái suy nghĩ liên quan đến tính tiện ích của việc bẻ khóa, nhưng vẫn đề quan trọng từ quan điểm bảo mật là việc chạy bất kỳ thiết bị nào có đặc quyền nâng cao đều có thể dẫn đến lỗi gây ra nhiều thiệt hại hơn, vì các biện pháp kiểm soát bảo mật thông thường thường đã bị bỏ qua. Việc bẻ khóa thiết bị iOS của Apple cũng có thể làm mất hiệu lực bảo hành của nhà sản xuất cũng như khiến thiết bị không còn sử dụng được với App Store.

*Root* một thiết bị là một quá trình mà theo đó, các biện pháp kiểm soát của hệ điều hành bị bỏ qua và đây là thuật ngữ thường được sử dụng cho các thiết bị Android. Dù thiết bị đã được root hay đã jailbreak thì hiệu quả là như nhau: các biện pháp kiểm soát của hệ điều hành được thiết kế để hạn chế các hoạt động sẽ không còn tác dụng nữa và thiết bị có thể thực hiện những điều mà nó không bao giờ được dự định để thực hiện, dù tốt hay xấu.



### **MÁCH NƯỚC CHO KỲ THI**

Việc root một thiết bị được sử dụng để bỏ qua các biện pháp kiểm soát của Hệ điều hành trên Android, và

jailbreak được sử dụng để leo thang đặc quyền và thực hiện điều tương tự trên các thiết bị iOS. Cả hai tiến trình đều ngừng các biện pháp kiểm soát của Hệ điều hành ngăn cản những hành vi của người dùng.

### **Sideload**

*Sideload* là quá trình bổ sung thêm ứng dụng vào thiết bị di động mà không cần sử dụng kho [ứng dụng] đã được ủy quyền tương ứng với thiết bị đó. Hiện tại, tính năng sideload chỉ hoạt động trên các thiết bị Android, vì Apple vẫn chưa cho phép thực thi bất kỳ ứng dụng nào ngoại trừ những ứng dụng đến từ App Store. Sideload là một phương tiện thay thế để khởi tạo ứng dụng trên thiết bị mà không cần phải lưu trữ ứng dụng đó trên kho ứng dụng cần thiết. Nhược điểm, nói một cách đơn giản, là rằng khi không có việc sàng lọc kho ứng dụng của nhà cung cấp, người ta có nhiều nguy cơ cài đặt phải phần mềm độc hại dưới vỏ bọc của một ứng dụng được mong muốn.

### **Firmware Tùy chỉnh**

*Firmware tùy chỉnh* là firmware cho thiết bị đã được thay đổi so với những thiết lập cài đặt gốc của nhà sản xuất. Firmware này có thể cung cấp chức năng bổ sung, nhưng nó cũng có thể dẫn đến các lỗ hổng bảo mật. Firmware tùy chỉnh chỉ nên được sử dụng trên các thiết bị không có quyền truy cập vào thông tin quan trọng.

### **Mở khóa Sóng**

Hầu hết các thiết bị di động ở Hoa Kỳ đều bị khóa với một nhà cung cấp dịch vụ, trong khi ở các nơi khác trên thế giới, chúng được mở khóa, dựa vào một mô-đun nhận dạng thuê bao (SIM) để kết nối và thông tin thanh toán. Đây là sản phẩm phụ của các quyết định thị trường kinh doanh được đưa ra sớm trong vòng đời thị trường điện thoại di động và cho đến nay vẫn còn tương đối đúng. Nếu bạn có một thiết bị bị-khóa-với-nhà-cung-cấp-dịch-vụ và bạn cố gắng sử dụng SIM của một nhà cung cấp dịch vụ

khác, thiết bị sẽ không chấp nhận nó trừ khi bạn mở khóa thiết bị. *Mở khóa nhà cung cấp dịch vụ (mở khóa sóng)* là quá trình lập trình để thiết bị tự tách bản thân nó khỏi nhà cung cấp dịch vụ. Điều này thường được thực hiện thông qua việc nhập một chuỗi phím đặc biệt để mở khóa thiết bị.

### Các cập nhật Firmware OTA

Firmware về cơ bản là phần mềm. Nó có thể được lưu trữ trong một con chip, nhưng cũng giống như tất cả các phần mềm, đôi khi nó đòi hỏi phải được cập nhật. Theo nghĩa đen, thiết bị di động ở khắp mọi nơi, quy mô không cho phép hỗ trợ việc đưa thiết bị đến vị trí trung tâm hoặc có kết nối để được cập nhật. *Cập nhật firmware OTA (over-the-air)* là một giải pháp cho vấn đề này. Tương tự như việc thêm hoặc cập nhật ứng dụng từ kho ứng dụng, bạn có thể nhấn vào tùy chọn menu trên một thiết bị di động để kết nối với kho ứng dụng và cập nhật firmware cho thiết bị. Tất cả các nhà sản xuất thiết bị lớn đều hỗ trợ mô hình này vì nó là giải pháp khả thi thực sự duy nhất.

### Sử dụng Camera

Nhiều thiết bị di động bao gồm các máy ảnh trên-bo-mạch và những hình ảnh/video chúng chụp được có thể tiết lộ thông tin. Thông tin này có thể được liên kết với bất kỳ thứ gì mà máy ảnh có thể chụp ảnh - bảng trắng, tài liệu và thậm chí cả vị trí của thiết bị khi ảnh/video được chụp thông qua gắn-thẻ-địa-lý (sẽ được thảo luận trong phần "Gắn thẻ GPS" sắp tới). Một thách thức khác gây ra bởi các thiết bị di động là khả năng chúng sẽ được sử dụng cho các mục đích bất hợp pháp. Điều này có thể tạo ra trách nhiệm pháp lý cho công ty nếu đó là thiết bị thuộc sở hữu của công ty. Bất chấp tất cả các mối quan tâm pháp lý tiềm ẩn, có thể mối quan tâm lớn nhất của người dùng thiết bị di động là ảnh cá nhân của họ sẽ bị mất trong quá trình xóa thiết bị được khởi nguồn bởi công ty.

## **SMS/Dịch vụ Tin nhắn Đa phương tiện (MMS)/Các Dịch vụ Liên lạc Phong phú (RCS)**

*Dịch vụ Tin nhắn Ngắn (SMS) và Dịch vụ Nhắn tin Đa phương tiện (MMS)* là các giao thức tiêu chuẩn được sử dụng để gửi tin nhắn, bao gồm nội dung đa phương tiện trong trường hợp MMS, đến và đi từ các thiết bị di động thông qua mạng di động. SMS được giới hạn trong các tin nhắn chỉ bao gồm văn bản ngắn, có độ dài dưới 160 ký tự và được truyền qua đường truyền tín hiệu của mạng di động khi dữ liệu báo hiệu không được gửi đi. SMS đã có từ những ngày đầu của điện thoại di động vào những năm 1980, trong khi MMS là một sự phát triển gần đây hơn được thiết kế để hỗ trợ cho việc gửi nội dung đa phương tiện đến và đi từ các thiết bị di động. Do các kết nối nội dung có thể được gửi qua MMS nói riêng và SMS trong một số trường hợp nhất định, điều quan trọng là ít nhất phải xác định các kênh liên lạc này trong các chính sách có liên quan.

*Dịch vụ Liên lạc phong phú (RCS)* là một giao thức hiện đang được sử dụng cùng với SMS và MMS. RCS hoạt động giữa thiết bị di động và nhà cung cấp dịch vụ và yêu cầu các ứng dụng hỗ trợ RCS ở cả hai đầu của giao tiếp. RCS hỗ trợ các phương pháp giao tiếp hiện đại, như thêm các tính năng mà người-dùng-mong-muốn như tích hợp với nhãn dán, video, hình ảnh, nhóm và các định dạng dữ liệu di động hiện đại khác. RCS cuối cùng được thiết kế để thay thế cho cả SMS và MMS.

### **Phương tiện Bên ngoài**

*Phương tiện bên ngoài* đề cập đến bất kỳ vật phẩm hoặc thiết bị nào có thể lưu trữ dữ liệu. Từ ổ đĩa flash đến ổ cứng, máy nghe nhạc, điện thoại thông minh, và thậm chí cả đồng hồ thông minh, nếu nó có thể lưu trữ dữ liệu thì nó là một con đường cho sự lọt dữ liệu. Phương tiện bên ngoài cũng có thể đưa những phần mềm độc hại vào trong doanh nghiệp. Rủi ro là hiển nhiên: những thiết bị này có thể mang dữ liệu vào và ra khỏi doanh nghiệp, nhưng chúng đã trở thành đồng nghĩa với nhân viên công

nghệ ngày nay. Điều then chốt là phát triển được một chính sách xác định nơi các thiết bị này có thể tồn tại và nơi nào chúng nên bị cấm, sau đó thực hiện theo kế hoạch với sự giám sát và thực thi.

### **USB On-The-Go (USB OTG)**

Universal Serial Bus là một phương pháp phổ biến để kết nối thiết bị di động với máy tính và các nền tảng dựa-trên-máy-vật-chủ khác. Việc kết nối các thiết bị di động với nhau một cách trực tiếp bắt buộc phải có những thay đổi đối với kết nối USB. Hãy xem xét USB *On-The-Go (USB OTG)*, một phần mở rộng của công nghệ USB tạo điều kiện kết nối trực tiếp giữa các thiết bị di động hỗ-trợ-USB-OTG. USB OTG cho phép các thiết bị đó chuyển đổi qua lại giữa các vai trò của máy chủ và thiết bị, bao gồm việc quyết định cái nào cung cấp năng lượng (máy vật chủ) và cái nào tiêu thụ điện năng trên giao diện. USB OTG cũng cho phép kết nối các thiết bị ngoại vi dựa trên USB, chẳng hạn như bàn phím, chuột và bộ nhớ ngoài, với các thiết bị di động. Mặc dù USB OTG tương đối mới nhưng hầu hết các thiết bị di động được sản xuất kể từ năm 2015 đều tương thích với USB OTG.

### **Ghi âm Microphone**

Ngày nay, rất nhiều thiết bị điện tử - từ điện thoại thông minh và đồng hồ thông minh đến các thiết bị như trợ lý trực tuyến của Amazon và Google và thậm chí cả đồ chơi - đều có khả năng ghi lại thông tin âm thanh. Việc *ghi âm microphone* có thể được sử dụng để ghi lại các cuộc trò chuyện, thu thập những dữ liệu nhạy cảm mà các bên không quan sát được, thậm chí không hề hay biết về hoạt động. Cũng giống như các tiện ích công nghệ cao khác, điều then chốt là xác định được chính sách về nơi có thể sử dụng microphone ghi âm và các quy tắc sử dụng microphone.

## Gắn nhãn GPS

Ảnh đã được chụp trên thiết bị di động hoặc bằng máy ảnh có chức năng GPS có thể có những thông tin về vị trí được nhúng vào trong ảnh kỹ thuật số. Đây được gọi là *gắn thẻ GPS (GPS tagging)* bởi CompTIA và *gắn-thẻ-địa-lý (geo-tagging)* bởi những người khác. Việc đăng ảnh có gắn thẻ địa lý có công dụng của nó, nhưng nó cũng có thể bất ngờ xuất bản những thông tin mà người dùng có thể sẽ không muốn chia sẻ. Ví dụ, nếu bạn sử dụng điện thoại thông minh để chụp ảnh ô tô trên đường lái xe và sau đó đăng ảnh lên Internet nhằm bán ô tô của mình, nếu tính năng gắn thẻ địa lý đã được bật trên điện thoại thông minh thì vị trí của bức ảnh đã được chụp được nhúng dưới dạng siêu dữ liệu trong ảnh kỹ thuật số. Việc đăng tải như vậy có thể vô tình làm lộ nơi ở của bạn. Đã có nhiều cuộc thảo luận công khai về chủ đề này và việc gắn-thẻ-địa-lý có thể được tắt trên hầu hết các thiết bị di động. Bạn nên tắt tính năng này trừ khi bạn có lý do cụ thể khiến thông tin vị trí được nhúng vào trong ảnh.

## Wi-Fi Trực tiếp/Đặc biệt

Thông thường, Wi-Fi kết nối thiết bị Wi-Fi với mạng thông qua một điểm truy cập không dây. Các phương pháp khác tồn tại, cụ thể là Wi-Fi trực tiếp và Wi-Fi đặc biệt. Trong *Wi-Fi trực tiếp*, hai thiết bị Wi-Fi kết nối với nhau qua kết nối một-bước (single-hop). Về bản chất, một trong hai thiết bị đóng vai trò như một điểm truy cập cho thiết bị kia. Yếu tố then chốt là bản chất một-bước của kết nối Wi-Fi trực tiếp. Wi-Fi trực tiếp chỉ kết nối hai thiết bị, nhưng hai thiết bị này có thể được kết nối với tất cả các tiện ích ưa thích của mạng không dây hiện đại, bao gồm cả WPA2.

Wi-Fi trực tiếp sử dụng một số dịch vụ để thiết lập kết nối an toàn giữa hai thiết bị. Đầu tiên là Khám phá Thiết bị và Dịch vụ Wi-Fi Trực tiếp (Wi-Fi Direct Device and Service Discovery). Giao thức này cung cấp một cách để các thiết bị phát hiện ra nhau dựa trên các dịch vụ mà chúng hỗ

trợ trước khi kết nối. Một thiết bị có thể tìm kiếm tất cả các thiết bị tương thích trong khu vực và sau đó thu hẹp danh sách xuống còn chỉ những thiết bị cho phép một dịch vụ cụ thể (giả sử in ấn) trước khi hiển thị cho người dùng danh sách các máy in có sẵn để ghép nối. Giao thức thứ hai được sử dụng là WPA2. Giao thức này được sử dụng để bảo vệ các kết nối và ngăn việc các bên trái phép ghép nối với các thiết bị Wi-Fi trực tiếp hoặc chặn liên lạc từ các thiết bị được ghép nối.

Sự khác biệt chủ yếu với *Wi-Fi đặc biệt* là trong một mạng đặc biệt, nhiều thiết bị có thể giao tiếp với nhau, với mỗi thiết bị có khả năng giao tiếp với tất cả các thiết bị khác. WPA2 cũng như các tiêu chuẩn Wi-Fi khác được đề cập chi tiết trong Chương 20.

### **Chia sẻ kết nối (Tethering)**

*Chia sẻ kết nối* liên quan đến việc kết nối thiết bị với một thiết bị di động có phương tiện truy cập mạng nhằm mục đích chia sẻ quyền truy cập mạng. Kết nối điện thoại di động với máy tính xách tay để sạc pin của điện thoại không phải là chia sẻ kết nối. Kết nối điện thoại di động với máy tính xách tay để máy tính xách tay có thể sử dụng điện thoại để kết nối Internet là chia sẻ kết nối. Khi bạn kết nối một thiết bị, bạn sẽ tạo thêm các kết nối mạng bên ngoài.

### **Điểm phát sóng (Hotspot)**

Thuật ngữ *điểm phát sóng* có thể đề cập đến một phần cụ thể của thiết bị mạng, một điểm đầu cuối cho giải pháp không dây, hoặc theo các khía cạnh khác là khu vực vật lý mà nó cung cấp kết nối. Thông thường, một điểm đầu cuối Wi-Fi, một điểm phát sóng cung cấp cho một nhóm người dùng một phương thức kết nối mạng. Chúng có thể được sử dụng cho nhân viên, khách hàng, khách viếng thăm hoặc các kết hợp của chúng dựa trên cơ chế kiểm soát truy cập được sử dụng tại thiết bị điểm đầu cuối. Một kỹ sư mạng sẽ đề cập đến điểm phát sóng như là thiết bị vật

lý cung cấp dịch vụ trên một khu vực địa lý cụ thể, trong khi người dùng sẽ coi nó là nơi họ có thể kết nối với mạng.

---



**MÁCH NƯỚC CHO KỲ THI** Chia sẻ kết nối liên quan đến một kết nối giữa một thiết bị với một thiết bị di động để có được kết nối mạng. Một điểm phát sóng có thể được chia sẻ nếu thiết bị thực tế là thiết bị di động, nhưng nếu thiết bị là cố định thì đây không phải là chia sẻ kết nối.

### Các Phương pháp Thanh toán

Hai mươi năm trước, *các phương thức thanh toán* là tiền mặt, séc hoặc phí. Ngày nay, chúng ta có các phương tiện trung gian mới: các thiết bị thông minh có giao tiếp trường lân cận (NFC) được liên kết với thẻ tín dụng cung cấp một hình thức thanh toán thay thế rất thuận tiện. Mặc dù thanh toán thực tế vẫn tính vào thẻ tín dụng/thẻ ghi nợ, nhưng con đường thanh toán là thông qua thiết bị kỹ thuật số. Khi sử dụng các tính năng bảo mật của thiết bị, NFC và sinh trắc học/mã PIN, hình thức thanh toán này có một số lợi thế so với các phương thức khác vì nó cho phép các biện pháp bảo mật cụ thể bổ sung, chẳng hạn như phê duyệt dựa-trên-sinh-trắc-học cho giao dịch, trước khi truy cập vào phương thức thanh toán.

---



**MÁCH NƯỚC CHO KỲ THI** Phần này bao gồm các chủ đề có thể được kiểm tra bằng các câu hỏi dựa-trên-hiệu-suất. Chỉ đơn giản là học thuộc các thuật ngữ liên quan đến tài liệu là chưa đủ. Bạn nên làm quen với cách thức xác định giải pháp giám sát và thực thi chính xác dựa trên một kịch bản nhất định. Kịch bản sẽ cung cấp thông tin cần thiết để xác định

đáp án tốt nhất cho câu hỏi. Bạn nên tìm hiểu sự khác biệt giữa các hạng mục - từ kho ứng dụng, bảo vệ hệ điều hành, đến các tùy chọn kết nối - đủ để có khả năng chọn đúng mục dựa trên tình huống đã nêu.

### Các Mô hình Triển khai

Khi xác định cách thức để kết hợp các thiết bị di động một cách bảo mật trong tổ chức của mình, bạn cần phải xem xét rất nhiều vấn đề, bao gồm cách bảo mật sẽ được thực thi, cách tất cả các chính sách sẽ được thực thi, và cuối cùng, những thiết bị nào sẽ được hỗ trợ. Bạn có thể chọn từ nhiều mô hình triển khai thiết bị khác nhau để hỗ trợ cho chiến lược bảo mật của mình, từ mô hình hoàn toàn do nhân-viên-sở-hữu (BYOD) đến mô hình nghiêm ngặt do công-ty-sở-hữu, với một số mô hình kết hợp ở giữa. Mỗi mô hình này đều có những ưu và nhược điểm.



**MÁCH NƯỚC CHO KỲ THI** Hãy chuẩn bị cho những câu hỏi dựa-trên-hiệu-suất yêu cầu bạn phải xác định mô hình triển khai di động đúng đắn dựa trên một kịch bản nhất định.

### Mang Thiết bị Cá nhân (BYOD)

Mô hình triển khai *mang thiết bị của riêng bạn (BYOD)* có rất nhiều lợi thế trong kinh doanh, và không chỉ nằm ở góc độ giảm thiểu chi phí thiết bị cho tổ chức. Người dùng có xu hướng thích có một thiết bị duy nhất hơn là mang theo nhiều thiết bị. Người dùng có ít kiến thức về việc học trên các thiết bị mà họ đã biết cách sử dụng hoặc có hứng thú trong việc học tập. Mô hình này khá phổ biến ở các công ty nhỏ và các tổ chức sử dụng nhiều lao động tạm thời. Điểm bất lợi lớn là nhân viên sẽ không muốn bị giới hạn việc sử dụng thiết bị cá nhân của họ dựa trên các chính sách của công ty, do đó sự kiểm soát của công ty sẽ bị hạn chế.

## Công-ty-Sở-hữu, Cho phép Sử dụng cá nhân (COPE)

Trong mô hình triển khai *công-ty-sở-hữu, cho phép sử dụng cá nhân* (COPE), nhân viên được cung cấp một thiết bị di động do tổ chức lựa chọn và thanh toán nhưng họ được phép sử dụng thiết bị đó cho các hoạt động cá nhân. Tổ chức có thể quyết định mức độ lựa chọn và quyền tự do của nhân viên đối với việc sử dụng thiết bị cho mục đích cá nhân. Điều này cho phép tổ chức kiểm soát chức năng bảo mật trong khi giải quyết sự không hài lòng của nhân viên liên quan đến phương thức cung cấp thiết bị truyền thống, sở-hữu-của-công-ty, sử dụng cho mục đích công việc (corporate-owned, business only - COBO).

## Chọn Thiết bị Cá nhân (CYOD)

Mô hình triển khai *chọn thiết bị sở hữu cá nhân của bạn* (*choose your own device* – CYOD) tương tự như BYOD về mặt khái niệm ở chỗ nó cho phép người dùng lựa chọn loại thiết bị. Trong hầu hết các trường hợp, tổ chức hạn chế những lựa chọn này chỉ trong danh sách các thiết bị có thể được chấp nhận để có thể được hỗ trợ trong tổ chức. Vì thiết bị thuộc sở hữu của tổ chức nên tổ chức có tính linh hoạt cao hơn trong việc áp đặt những hạn chế đối với việc sử dụng thiết bị về ứng dụng, dữ liệu, bản cập nhật, v.v...

## Công-ty-Sở-hữu

Trong mô hình triển khai *do công-ty-sở-hữu*, còn được gọi là chỉ dành cho mục đích công việc (COBO), công ty cung cấp cho nhân viên một thiết bị di động bị hạn chế chỉ-sử-dụng-trong-công-ty. Nhược điểm của mô hình này là nhân viên phải mang theo hai thiết bị – một cá nhân và một cho công việc – và sau đó phân tách các chức năng giữa các thiết bị dựa trên mục đích sử dụng trong từng trường hợp. Ưu điểm là công ty có toàn quyền kiểm soát các thiết bị của mình và có thể áp dụng bất kỳ biện pháp kiểm soát bảo mật nào mong muốn mà không bị ảnh hưởng bởi chức năng của thiết bị khác.



**MÁCH NƯỚC CHO KỲ THI** Hãy dự kiến trước các câu hỏi dựa-trên-hiệu-suất cho các mô hình triển khai khác nhau: BYOD, CYOD, COPE và do-công-ty-sở-hữu. Đáp án chính xác cho câu hỏi sẽ nằm ở chi tiết của kịch bản, vì vậy hãy xem xét các chi tiết một cách cẩn trọng để xác định đáp án tốt nhất.

### **Cơ sở hạ tầng Máy tính để bàn Ảo (VDI)**

Mặc dù có vẻ như các mô hình triển khai chỉ được liên kết với điện thoại, nhưng thực tế không phải như vậy, vì máy tính cá nhân cũng có thể là những thiết bị di động bên ngoài yêu cầu kết nối. Trong trường hợp máy tính xách tay, giải pháp *cơ sở hạ tầng máy tính để bàn ảo (virtual desktop infrastructure - VDI)* có thể mang lại quyền kiểm soát môi trường di động liên quan đến thiết bị không-thuộc-sở-hữu-của-công-ty. Doanh nghiệp có thể thiết lập các máy ảo hoàn toàn tuân thủ bảo mật và chứa tất cả các ứng dụng cần thiết mà nhân viên cần và sau đó cho phép nhân viên truy cập vào máy ảo thông qua kết nối ảo hoặc kết nối máy tính từ xa. Điều này có thể giải quyết hầu hết nếu không muốn nói là tất cả các vấn đề về bảo mật và chức năng ứng dụng liên quan đến thiết bị di động. Nó đòi hỏi một nhân viên CNTT phải có khả năng thiết lập, duy trì và quản lý VDI trong tổ chức, vốn không nhất thiết là một tác vụ nhỏ, tùy thuộc vào số lượng trường hợp cần thiết. Việc tương tác với các VDI này có thể được thực hiện dễ dàng trên nhiều thiết bị di động ngày nay vì màn hình tiên tiến và sức mạnh tính toán của chúng.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các yếu tố cần thiết để triển khai các thiết bị di động một cách an toàn. Chương này mở đầu với một mô tả về các phương thức kết nối giao tiếp khác nhau. Cụ thể, chương này đề cập đến các phương thức kết nối di động, Wi-Fi, Bluetooth, NFC, hồng ngoại và USB. Các phương pháp điểm-đến-điểm và điểm-đến-đa-điểm cũng đã được đề cập. Công nghệ định vị toàn cầu và RFID cũng được bao gồm.

Từ đó, chương khám phá những khái niệm về quản lý thiết bị di động. Trong phần này, các chủ đề bao gồm quản lý ứng dụng và nội dung, làm sạch từ xa, hàng rào địa lý và định vị địa lý, khóa màn hình, dịch vụ thông báo đẩy, mật khẩu và mã PIN, sinh trắc học, xác thực theo ngữ cảnh, lưu trữ, phân đoạn bộ nhớ và mã hóa toàn bộ thiết bị. Phần tiếp theo xem xét các giải pháp MicroSD HSM, MDM/UEM, MAM và hệ thống SEAndroid.

Chương tiếp theo đã xem xét các yêu cầu thực thi và giám sát đối với các kho ứng dụng của bên thứ ba, root/jailbreak, sideloading, firmware tùy chỉnh, mở khóa nhà cung cấp dịch vụ, cập nhật firmware OTA, sử dụng camera, SMS/MMS, phương tiện bên ngoài, USB OTG, ghi âm microphone, gắn thẻ GPS, Wi-Fi trực tiếp/đặc biệt, chia sẻ kết nối, điểm phát sóng và phương thức thanh toán. Chương này khép lại với phần thảo luận về các mô hình triển khai, bao gồm BYOD, CYOD, COPE, do-công-ty-sở-hữu và VDI.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

- 1.** Đâu là điểm yếu của công nghệ di động trong số những điều dưới đây?
  - A.** Rất nhiều nhà cung cấp trong một mạng quy mô quốc gia
  - B.** Tính khả dụng thấp trong những khu vực hẻo lánh
  - C.** Rất nhiều tháp tín hiệu di động gần nhau trong các khu vực đô thị
  - D.** Tín hiệu mạnh trong những khu vực đông dân cư.
- 2.** Bluetooth sử dụng dải phổ tần số nào?
  - A.** 1,7 GHz
  - B.** 2,4 GHz
  - C.** 5 GHz
  - D.** 6,4 GHz
- 3.** Bạn cần sử dụng khóa mật mã giữa một số thiết bị. Điều nào sau đây có thể quản lý tác vụ này?
  - A.** Các giải pháp MAM
  - B.** Cập nhật firmware OTA
  - C.** USB OTG
  - D.** MicroSD HSM
- 4.** Ba chế độ nào sau đây được Bluetooth 4.0 hỗ trợ?
  - A.** Cổ điển, Tốc độ thấp, Năng lượng cao
  - B.** Tốc độ Dữ liệu Nâng cao, Tương thích Ngược, Năng lượng Cao
  - C.** Cổ điển, Tốc độ Cao, Năng lượng Thấp
  - D.** Đồng bộ, Tốc độ Cao, Năng lượng Thấp
- 5.** Công dụng chính của giao tiếp trường gần (NFC) là gì?

- A.** Thiết lập liên lạc vô tuyến trong một khoảng cách ngắn
- B.** Giao tiếp ở những vùng dân cư thưa thớt
- C.** Kết nối đường-dài
- D.** Giao tiếp trong môi trường công nghiệp ồn ào
- 6.** Bạn cần quản lý toàn bộ các thiết bị đầu cuối khác nhau trong doanh nghiệp, bao gồm thiết bị di động, iPad, máy in, PC và điện thoại. Giải pháp nào sau đây là giải pháp toàn diện nhất?
- A.** Các giải pháp dựa trên COPE
- B.** Giải pháp MAM
- C.** Các giải pháp MDM
- D.** Giải pháp UEM
- 7.** Nhược điểm của công nghệ hồng ngoại (IR) là gì?
- A.** Nó có tốc độ dữ liệu cao.
- B.** Nó không thể xuyên qua vật rắn.
- C.** Nó có thể xuyên qua tường.
- D.** Nó sử dụng một công nghệ mã hóa chậm.
- 8.** Mỗi quan tâm chính về bảo mật với công nghệ Universal Serial Bus (USB) là gì?
- A.** Nó kết nối với điện thoại di động để sạc pin dễ dàng.
- B.** Nó sử dụng mã hóa độc quyền.
- C.** Nó tự động hóa và hoạt động giống như một ổ cứng gắn vào máy tính.
- D.** Nó sử dụng công nghệ mã hóa cũ hơn.
- 9.** Tại sao việc thiết lập các chính sách quản lý việc làm sạch từ xa các thiết bị di động lại là điều quan trọng?
- A.** Các thiết bị di động thường không kết hợp dữ liệu cá nhân và dữ liệu của doanh nghiệp.
- B.** Các thiết bị di động được bảo mật dễ dàng hơn.
- C.** Kẻ trộm không thể giải mã thiết bị di động.

**D.** Chúng dễ bị thất thoát hơn các thiết bị khác.

**10.** Mục đích của hàng rào địa lý là gì?

**A.** Có thể được sử dụng để làm sạch từ xa một thiết bị đã mất.

**B.** Khiến cho việc bảo mật thiết bị di động trở nên đơn giản hơn.

**C.** Cho phép các thiết bị được nhận dạng theo vị trí và thực hiện các hành động.

**D.** Có thể thực thi khóa thiết bị bằng một mật khẩu mạnh.

## Đáp án

1. **B.** Một điểm yếu của công nghệ di động là nó ít khả dụng ở các vùng nông thôn.
2. **B.** Bluetooth sử dụng dải phổ tần số 2,4 GHz.
3. **D.** MicroSD HSM hỗ trợ chức năng HSM thông qua kết nối MicroSD. Nó có thể được kết nối thông qua một bộ chuyển đổi với bất kỳ thiết bị USB nào.
4. **C.** Ba chế độ được hỗ trợ bởi Bluetooth 4.0 là Cổ điển, Tốc độ Cao và Năng lượng Thấp.
5. **A.** Công dụng chính của NFC là thiết lập liên lạc vô tuyến trong một khoảng cách ngắn.
6. **D.** Các giải pháp UEM (quản lý điểm đầu cuối hợp nhất) có thể giải quyết nhiều loại thiết bị theo cách toàn diện hơn so với các giải pháp MDM và MAM.
7. **B.** Một nhược điểm của công nghệ IR là không thể xuyên qua những vật thể rắn.
8. **C.** Mỗi quan tâm chính về bảo mật với công nghệ USB là nó tự động hóa và hoạt động giống như một ổ cứng được gắn vào máy tính.
9. **D.** Điều quan trọng là phải thiết lập các chính sách quản lý việc làm sạch từ xa các thiết bị di động vì chúng dễ bị mất hơn các thiết bị khác.
10. **C.** Mục đích của hàng rào địa lý là cho phép các thiết bị được nhận dạng theo vị trí và thực hiện các hành động.

## Chương 22 Triển khai Bảo mật Đám mây

---

### Triển khai Bảo mật Đám mây

Trong chương này bạn sẽ

- Khám phá các biện pháp kiểm soát bảo mật đám mây,
  - So sánh và đối chiếu các giải pháp bảo mật đám mây,
  - Tìm hiểu về các biện pháp kiểm soát đám-mây-tự-nhiên so với các giải pháp bên-thứ-ba.
- 

Điện toán đám mây đang trở nên ngày càng phổ biến hơn do rất nhiều yếu tố kinh doanh. Nó có những ưu điểm về mặt kinh tế và kỹ thuật so với CNTT truyền thống trong rất nhiều trường hợp sử dụng, nhưng điều đó không có nghĩa là nó không có vấn đề. Việc bảo mật các hệ thống đám mây về một khía cạnh không hề khác biệt gì so với một hệ thống CNTT truyền thống: bảo vệ dữ liệu khỏi bị đọc và thao túng trái phép. Tuy nhiên các công cụ, kỹ thuật và thủ tục rất khác so với CNTT tiêu chuẩn, và mặc dù các đám mây có thể được bảo mật, đó là vì việc áp dụng chính xác bộ các biện pháp kiểm soát chứ không phải là điều ngẫu nhiên.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 3.6 của kỳ thi CompTIA Security+: Đưa ra một tình huống, áp dụng các giải pháp an ninh mạng cho đám mây.

## Các Biện pháp kiểm soát Bảo mật Đám mây

Kiểm soát bảo mật đám mây là một vấn đề được chia sẻ - một vấn đề chung giữa người dùng và nhà cung cấp đám mây. Tùy thuộc vào các điều khoản dịch vụ của bạn với nhà cung cấp dịch vụ đám mây, bạn sẽ chia sẻ trách nhiệm về cập nhật phần mềm, kiểm soát truy cập, mã hóa và các kiểm soát bảo mật quan trọng khác. Trong phần "Các mô hình Đám mây" ở Chương 10, Hình 10-1 đã minh họa các mức độ khác nhau của trách nhiệm chung trong các mô hình đám mây khác nhau. Điều quan trọng cần phải nhớ là hãy xác định các yêu cầu từ trước và viết chúng vào thỏa thuận dịch vụ với nhà cung cấp dịch vụ đám mây, bởi vì trừ khi chúng là một phần của gói dịch vụ, chúng sẽ không xảy ra.

## Tính sẵn sàng Cao Trên các Vùng

Môi trường điện toán đám mây có thể được thiết lập cấu hình để cung cấp tính khả dụng gần như toàn-thời-gian (nghĩa là, một hệ thống có tính khả dụng cao). Điều này được thực hiện bằng cách sử dụng phần cứng và phần mềm dự phòng giúp hệ thống trở nên sẵn sàng, bất chấp các lỗi thành phần riêng lẻ. Khi một cái gì đó gặp lỗi hoặc bị hư hỏng, quá trình chuyển đổi dự phòng sẽ di chuyển tiến trình xử lý đang được thực hiện bởi thành phần bị lỗi sang thành phần dự phòng ở nơi khác trong đám mây. Quá trình này càng minh bạch với người dùng càng tốt, tạo ra hình ảnh về một hệ thống có tính khả dụng cao đối với người dùng. Việc xây dựng nền các thành phần chuyển đổi dự phòng này giữa các vùng mang lại *tính khả dụng cao trên các vùng*. Như với tất cả các vấn đề về bảo mật đám mây, các chi tiết nằm trong điều khoản dịch vụ của bạn với nhà cung cấp dịch vụ đám mây của bạn, bạn không thể chỉ giả định rằng nó [đám mây] sẽ có tính khả dụng cao. Nó phải được chỉ định trong điều khoản của bạn và được xây dựng bởi nhà cung cấp.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng các vùng có thể được sử dụng để nhân bản và mang lại sự cân bằng tải cũng như tính khả dụng cao.

### Các Chính sách Tài nguyên

Các nguồn tài nguyên dựa-trên-đám-mây được kiểm soát thông qua một bộ các chính sách. Về cơ bản, đây là mô hình ủy quyền của bạn được chiếu vào không gian đám mây. Các nhà cung cấp đám mây khác nhau có các cơ chế khác nhau để xác định các nhóm, loại tài nguyên được phép và phân công theo vị trí hoặc các ngăn riêng biệt. Sự tích hợp giữa hệ thống quản lý truy cập danh tính doanh nghiệp (IAM) và hệ thống IAM dựa-trên-đám-mây là thành phần cấu hình có tầm quan trọng hàng đầu khi thiết lập môi trường đám mây. Các chính sách thiết lập nên quyền hạn cho các đối tượng đám mây. Khi các chính sách tài nguyên từ doanh nghiệp đã được mở rộng vào môi trường đám mây và được thiết lập, chúng phải được duy trì. Mức độ tích hợp giữa hệ thống IAM dựa-trên-đám-mây và hệ thống IAM dựa-trên-doanh-nghiệp sẽ xác định mức độ công việc cần thiết cho các hoạt động bảo trì định kỳ.

### Quản lý Bí mật

Dữ liệu trong đám mây vẫn là dữ liệu trên một máy chủ và do đó, theo định nghĩa, có thể truy cập được từ xa. Vì vậy, điều quan trọng là phải bảo mật dữ liệu bằng cách sử dụng mã hóa. Một sai lầm phổ biến là để dữ liệu không được mã hóa trên đám mây. Có vẻ như hầu như không có một tuần nào trôi qua mà không có một báo cáo về dữ liệu đã không được mã hóa bị lộ ra từ một phiên bản đám mây. Ngón tay luôn trở đến nhà cung cấp đám mây, nhưng trong hầu hết các trường hợp, lỗi là ở người dùng đầu cuối. Các nhà cung cấp dịch vụ đám mây cung cấp các công cụ

mã hóa và dịch vụ quản lý, nhưng rất nhiều công ty không triển khai chúng, và điều này tạo ra bối cảnh cho sự xâm phạm dữ liệu.

*Quản lý bí mật* là thuật ngữ dùng để chỉ các chính sách và thủ tục được sử dụng để kết nối các hệ thống IAM của doanh nghiệp và đám mây để cho phép giao tiếp với dữ liệu. Việc lưu trữ dữ liệu nhạy cảm - hoặc trong hầu hết các trường hợp, hầu như là bất kỳ dữ liệu nào - trên đám mây mà không đưa ra các biện pháp kiểm soát thích hợp để ngăn chặn việc truy cập vào dữ liệu là hành động vô trách nhiệm và nguy hiểm. Mã hóa là một biện pháp bảo vệ dự phòng - ngay cả khi cấu hình bảo mật không thành công và dữ liệu rơi vào tay một bên trái phép, dữ liệu sẽ không thể được đọc hoặc sử dụng nếu không có các khóa. Điều quan trọng là phải duy trì quyền kiểm soát các khóa mã hóa. Bảo mật của các khóa, vốn có thể được thực hiện bên ngoài phiên bản đám mây chính và ở những nơi khác trong doanh nghiệp, là cách bí mật được quản lý.

Quản lý bí mật là một khía cạnh quan trọng của việc duy trì bảo mật đám mây. Các bí mật được sử dụng để truy cập từ-hệ-thống-đến-hệ-thống phải được duy trì một cách tách biệt với dữ liệu cấu hình khác và được xử lý theo các nguyên tắc bảo mật nghiêm ngặt nhất vì những bí mật cho phép truy cập vào dữ liệu trên đám mây.



**MÁCH NƯỚC CHO KỲ THI** Sử dụng một trình quản lý bí mật có thể cho phép quản lý bí mật bằng cách cung cấp một vị trí lưu trữ đáng tin cậy tập trung dành cho các chứng chỉ, mật khẩu, và thậm chí các khóa của giao diện lập trình ứng dụng (API).

## Tích hợp và Kiểm toán

Việc tích hợp mức độ và số lượng thích hợp của các biện pháp kiểm soát bảo mật là một chủ đề luôn luôn được kiểm toán. Các biện pháp kiểm soát có phù hợp không? Chúng có được thiết lập và sử dụng một cách đúng đắn không? Quan trọng nhất, chúng có hiệu quả không? Đây là các yếu tố kiểm toán CNTT tiêu chuẩn trong doanh nghiệp. Việc di chuyển các tài nguyên điện toán lên đám mây không làm thay đổi nhu cầu hoặc mục đích của các chức năng kiểm toán.

Kiểm toán điện toán đám mây đã trở thành một tiêu chuẩn khi các doanh nghiệp nhận thức được rằng các rủi ro dựa-trên-đám-mây độc đáo tồn tại khi dữ liệu của họ đang được lưu trữ bởi các tổ chức khác. Để giải quyết những rủi ro này, các tổ chức đang sử dụng những cuộc kiểm toán điện toán đám mây cụ thể để đạt được sự đảm bảo và tìm hiểu rủi ro về việc thông tin của họ bị mất hoặc bị tiết lộ cho các bên trái phép. Các cuộc kiểm toán cụ thể trên đám mây này có hai nhóm yêu cầu: một là hiểu biết về môi trường bảo mật đám mây như đã được triển khai và thứ hai là liên quan đến các yêu cầu bảo mật dữ liệu. Kết quả là kiểm toán điện toán đám mây có thể ở các hình thức khác nhau, chẳng hạn như báo cáo SOC 1 và SOC 2, HITRUST, PCI và FedRAMP. Đối với từng khuôn khổ bảo mật dành riêng cho dữ liệu này, các chi tiết bổ sung dựa trên các đặc điểm cụ thể của môi trường đám mây và các chi tiết cụ thể của các biện pháp kiểm soát bảo mật được cả doanh nghiệp và nhà cung cấp đám mây sử dụng.

## Lưu trữ

*Lưu trữ* dữ liệu dựa-trên-đám-mây đã là một trong số những hình thức sử dụng đầu tiên của điện toán đám mây. Các yêu cầu bảo mật liên quan đến lưu trữ trong môi trường đám mây trong thực tế đều dựa vào những nguyên tắc nền tảng như trong môi trường doanh nghiệp. Quyền truy cập

và sửa đổi dữ liệu cần phải được định nghĩa, thiết lập và thực thi. Một phương tiện để bảo vệ dữ liệu khỏi sự truy cập trái phép nói chung là cần thiết, và mã hóa chính là câu trả lời chính, giống như trong môi trường doanh nghiệp. Việc nhân bản dữ liệu trên nhiều hệ thống khác nhau như một phần của triển khai đám mây và những khía cạnh về các thành phần có tính sẵn sàng cao của một môi trường đám mây có thể làm phức tạp thêm việc bảo mật dữ liệu.

## **Quyền**

*Quyền* truy cập và sửa đổi dữ liệu được xử lý theo cùng một cách thức như trong môi trường CNTT tại-chỗ. Các hệ thống quản lý truy cập danh tính (IAM) được sử dụng để quản lý những chi tiết như ai có thể thực hiện việc gì với từng đối tượng. Chìa khóa để quản lý việc này trên đám mây là sự tích hợp của hệ thống IAM-tại-chỗ với hệ thống IAM-dựa-trên-đám-mây.

## **Mã hóa**

*Mã hóa* dữ liệu trên đám mây là một phần tử nền tảng để bảo mật dữ liệu của mọi người khi nó đang ở trên một hệ thống khác. Dữ liệu nên được mã hóa khi được lưu trữ trên đám mây, và các khóa nên được duy trì bởi doanh nghiệp, không phải bởi nhà cung cấp đám mây. Các khóa cũng nên được quản lý với một mức độ tương xứng của các khóa được cung cấp trong doanh nghiệp.

## **Nhân bản**

Dữ liệu có thể nhân bản trên đám mây như một phần của nhiều hoạt động dựa-trên-đám-mây khác nhau. Từ môi trường được chia sẻ đến các hệ thống có tính sẵn sàng cao, bao gồm cả hệ thống sao lưu của chúng, dữ liệu trong đám mây dường như có thể linh hoạt, di chuyển trên nhiều hệ thống vật lý. Mức độ *nhân bản* này là một lý do khác khiến dữ liệu phải được mã hóa để bảo mật. Hành động nhân bản dữ liệu trên nhiều hệ

thống là một phần của khả năng phục hồi của đám mây, trong đó các điểm đơn lỗi sẽ không có những tác động tương tự xảy ra trong doanh nghiệp CNTT tiêu chuẩn. Do đó, đây là một trong những ưu điểm của đám mây.

### Tính sẵn sàng Cao

Hệ thống lưu trữ có *tính sẵn sàng cao* hoạt động theo cách thức tương tự như các hệ thống có tính sẵn sàng cao đã được mô tả trước đó trong chương. Việc có nhiều hệ thống vật lý khác nhau cùng hoạt động để đảm bảo dữ liệu của bạn được dự phòng và lưu trữ với khả năng phục hồi cao là một trong những lợi thế của đám mây. Hơn nữa, hệ thống IAM dựa-trên-đám-mây có thể sử dụng các biện pháp bảo vệ mã hóa để giữ bí mật cho dữ liệu của bạn, trong khi tính sẵn sàng cao vẫn giữ được dữ liệu luôn sẵn có.

### Mạng

Các hệ thống dựa-trên-đám-mây được tạo thành từ các máy được kết nối bằng một mạng. Thông thường, mạng này nằm dưới sự kiểm soát của nhà cung cấp dịch vụ đám mây (CSP). Mặc dù bạn có thể được cung cấp thông tin mạng, bao gồm cả các địa chỉ, nhưng các mạng mà bạn nhìn thấy thực sự có thể được đóng gói trên một mạng khác được duy trì bởi nhà cung cấp dịch vụ. Theo xu hướng này, rất nhiều nhà cung cấp dịch vụ đám mây cung cấp một mạng ảo cung cấp các chức năng cần thiết mà không cung cấp quyền truy cập trực tiếp vào môi trường mạng thực tế.

### Mạng ảo

Hầu hết kết nối mạng trong môi trường đám mây là thông qua một mạng ảo đang hoạt động trong một lớp phủ bên trên một mạng vật lý. *Mạng ảo* có thể được sử dụng và thao tác bởi người dùng, trong khi mạng thực bên dưới thì không. Điều này mang lại cho nhà cung cấp dịch vụ đám mây khả năng quản lý và cung cấp chức năng mạng độc lập với phiên bản đám

mây đối với người dùng. Công nghệ mạng ảo được sử dụng trong môi trường đám mây có thể bao gồm mạng do phần-mềm-xác-định (software-defined network - SDN) và ảo hóa chức năng mạng (network function virtualization - NFV) là các yếu tố giúp thực hiện các tác vụ mạng mong muốn trên đám mây dễ dàng hơn.

### **Các mạng con Công khai và Riêng tư**

Cũng giống như các hệ thống CNTT truyền thống, thường có một nhu cầu về các mạng con công-khai, nơi mạng công cộng/Internet có thể tương tác với các máy chủ, chẳng hạn như máy chủ email, máy chủ web, và những thứ tương tự. Cũng có một nhu cầu đối với các mạng con riêng tư, nơi quyền truy cập bị giới hạn ở các địa chỉ cụ thể, ngăn chặn việc truy cập trực tiếp vào các bí mật như kho dữ liệu và các tài sản thông tin quan trọng khác. Đám mây đi kèm với khả năng sử dụng cả mạng con công khai lẫn riêng tư, hay nói cách khác, chỉ vì thứ gì đó nằm "trên đám mây" không làm thay đổi kiến trúc kinh doanh của một số có những máy có kết nối Internet và một số thì không. Bây giờ, trở thành "trong đám mây" có nghĩa là, về một khía cạnh nào đó, Internet được sử dụng cho tất cả các quyền truy cập. Tuy nhiên, trong trường hợp mạng con riêng tư, hệ thống IAM dựa-trên-đám-mây có thể xác định ai được phép truy cập vào phần nào của mạng ảo của đám mây.

### **Phân đoạn**

*Phân đoạn* là tiến trình mạng về việc tách các phần tử mạng thành các phân đoạn và điều tiết lưu lượng giữa các phân đoạn. Sự hiện diện của một mạng được phân đoạn tạo ra các rào cản bảo mật đối với những người truy cập trái phép thông qua việc kiểm tra các gói khi chúng di chuyển từ phân đoạn này sang phân đoạn khác. Điều này có thể được thực hiện theo nhiều cách - thông qua bảng MAC, địa chỉ IP và thậm chí cả đường hầm, với các thiết bị như tường lửa và cổng web bảo mật kiểm

tra ở mỗi kết nối. Điều cuối cùng trong phân đoạn là mô trường zero-trust, nơi mà phân đoạn vi mô được sử dụng để liên tục yêu cầu xác minh các quyền và các biện pháp kiểm soát. Tất cả những điều này đều có thể được thực hiện trong một mạng đám mây. Ngoài ra, cũng như các biện pháp kiểm soát khác đã được trình bày, các chi tiết nằm trong thỏa thuận mức dịch vụ (SLA) với nhà cung cấp dịch vụ đám mây.

### Tích hợp và Kiểm tra API

API là các giao diện phần mềm cho phép các thành phần phần mềm khác nhau để giao tiếp với nhau. Điều này đúng trong đám mây cũng giống như trong các doanh nghiệp CNTT truyền thống. Do bản chất của các môi trường đám mây - chấp nhận hầu như mọi yêu cầu trên web - nên cần phải xác minh thông tin trước khi có thể được sử dụng. Một yếu tố then chốt trong giải pháp này được trình bày ở phần sau của chương - cổng web bảo mật thế-hệ-kế-tiếp. Hệ thống này phân tích thông tin chuyển giao tại lớp ứng dụng để xác minh tính xác thực và đúng đắn.

*Kiểm tra nội dung* đề cập đến việc kiểm tra nội dung của một yêu cầu đối với một API bằng cách áp dụng các quy tắc để xác định xem liệu một yêu cầu có hợp pháp và có nên được chấp nhận hay không. Khi các API hoạt động để tích hợp một ứng dụng này với ứng dụng khác, các lỗi trong một ứng dụng có thể được truyền sang các thành phần khác, do đó tạo ra những vấn đề lớn hơn. Việc sử dụng *kiểm tra nội dung API* là một biện pháp tích cực để ngăn chặn lỗi lan truyền qua hệ thống và gây ra sự cố.



**MÁCH NƯỚC CHO KỲ THI** Các biện pháp bảo mật đám mây cũng cung cấp những tính năng tương tự như các biện pháp bảo mật mạng bình thường, chúng chỉ thực hiện những tính năng đó trong một môi trường khác. Đám mây không phải là một hệ thống không có kiểm soát.

## Điện toán

Đám mây đã trở thành một hoạt động dịch vụ nơi các ứng dụng có thể được triển khai, cung cấp một hình thức điện toán dựa-trên-đám-mây. Những khía cạnh *điện toán* của một hệ thống đám mây cũng có các vấn đề bảo mật giống như một hệ thống CNTT truyền thống, hay nói cách khác, thực tế là một phần tử máy tính nằm trong đám mây không khiến cho nó trở nên bảo mật nhiều hơn hoặc kém hơn. Những gì phải xảy ra là các yêu cầu bảo mật cần phải được giải quyết khi dữ liệu đến và đi từ phần tử máy tính.

## Các Nhóm Bảo mật

Các *nhóm bảo mật* được cấu thành từ một tập hợp các quy tắc và chính sách tương ứng với một phiên bản đám mây. Các quy tắc này có thể là quy tắc về mạng, chẳng hạn như quy tắc vượt qua tường lửa, hoặc chúng có thể là quy tắc IAM liên quan đến việc ai có quyền truy cập hoặc tương tác với một đối tượng trên hệ thống. Các nhóm bảo mật được mỗi nhà cung cấp dịch vụ đám mây xử lý một cách khác nhau, nhưng cuối cùng thì chúng cung cấp phương tiện quản lý quyền ở một chế độ chi tiết bị giới hạn. Các nhà cung cấp khác nhau có các giới hạn khác nhau, nhưng mục tiêu cuối cùng là đặt người dùng vào các nhóm hơn là thực hiện từng kiểm tra riêng lẻ cho mọi yêu cầu truy cập. Điều này được thực hiện để quản lý khả năng mở rộng, là một trong những yếu tố nền tảng của điện toán đám mây.

## Phân bổ Tài nguyên Động

Hệ thống dựa-trên-đám-mây có một số đặc điểm phân biệt nổi bật nhất định bên cạnh việc chỉ ở trên một máy tính khác. Giữa những đặc điểm này là cung cấp điện toán có khả năng mở rộng và đáng tin cậy theo cách hiệu-quả-về-chi-phí. Việc có được một hệ thống mà tài nguyên của nó có thể phát triển và thu hẹp khi các yêu cầu tính toán thay đổi mà không

cần phải mua thêm máy chủ mới hay mở rộng hệ thống, v.v..., là một trong những lợi thế chính của đám mây. Các nhà cung cấp dịch vụ đám mây không chỉ cung cấp phần cứng đơn thuần. Một trong những giá trị tương xứng với đám mây là khả năng phát triển khi tải trọng gia tăng và thu nhỏ (từ đó tiết kiệm chi phí) khi tải trọng giảm. Các nhà cung cấp dịch vụ đám mây quản lý việc này bằng cách sử dụng phần mềm *phân bổ tài nguyên động* để giám sát các mức hiệu suất. Theo thỏa thuận dịch vụ, họ có thể hành động để gia tăng dần nguồn lực khi cần thiết.

### **Nhận biết về phiên bản**

Cũng giống như các doanh nghiệp đã chuyển sang đám mây, thì những kẻ tấn công cũng vậy. Các mạng điều-khiển-và-kiểm-soát (command-and-control) có thể được tạo ra trong môi trường đám mây, giống như chúng đang ở trên phần cứng thực của doanh nghiệp. Điều này tạo ra một tình huống trong đó một đám mây đang giao tiếp với một đám mây khác và làm thế nào để đám mây đầu tiên hiểu được liệu đám mây thứ hai có hợp pháp hay không? *Nhận biết về phiên bản* là tên gọi của một khả năng phải được hỗ trợ trên tường lửa, cổng web an toàn và công ty môi giới bảo mật truy cập đám mây (cloud access security broker - CASB) để xác định xem hệ thống tiếp theo trong chuỗi giao tiếp có hợp pháp hay không. Sử dụng một dịch vụ hỗ-trợ-đám-mây như Google Drive, Microsoft OneDrive hoặc Box hoặc bất kỳ bộ lưu trữ dựa-trên-đám-mây nào khác. Bạn có chặn tất cả chúng không? Hay bạn xác định rằng trường hợp nào là hợp pháp và trường hợp nào không? Đây là một tính năng tương đối mới và được nâng cao, nhưng là một tính năng ngày càng trở nên quan trọng để ngăn chặn việc tiết lộ dữ liệu và các vấn đề khác từ việc tích hợp các ứng dụng đám mây với các điểm đầu cuối trái phép.

### **Điểm đầu cuối Đám mây Riêng tư Ảo (VPC)**

Một *điểm đầu cuối đám mây riêng tư ảo* cho phép các kết nối đến và đi từ một phiên bản đám mây riêng tư ảo. Các điểm đầu cuối VPC là các phần tử ảo có thể mở rộng quy mô. Chúng cũng được dự phòng và thường có tính sẵn sàng cao. Điểm đầu cuối VPC cung cấp một phương tiện để kết nối VPC với các tài nguyên khác mà không cần đi ra ngoài qua Internet. Hãy xem nó như một đường hầm an toàn để truy cập trực tiếp vào những nguồn tài nguyên khác dựa-trên-đám-mây mà không để lộ lưu lượng cho các bên khác. Các điểm đầu cuối VPC có thể được lập trình để cho phép tích hợp với IAM và các giải pháp bảo mật khác, cho phép các kết nối qua-đám-mây một cách bảo mật.



**MÁCH NƯỚC CHO KỲ THI** Một điểm đầu cuối VPC cung cấp một phương tiện để kết nối một VPC với những nguồn tài nguyên khác mà không cần phải đi ra qua Internet. Hay nói cách khác, bạn không cần những công nghệ kết nối VPC bổ sung hoặc thậm chí, một cửa ngõ Internet.

### Bảo mật Vùng chứa

*Bảo mật vùng chứa* là quá trình triển khai các công cụ và chính sách bảo mật để đảm bảo vùng chứa của bạn đang hoạt động như dự kiến. Công nghệ vùng chứa cho phép các ứng dụng và các phần phụ thuộc của chúng được đóng gói lại với nhau thành một phần tử hoạt động. Phần tử này, còn thường được gọi là một *bản kê khai*, có thể được kiểm-soát-phiên-bản, triển khai, nhân bản và quản lý trên một môi trường. Các vùng chứa có thể chứa tất cả các yếu tố Hệ điều hành cần thiết để một ứng dụng có thể hoạt động, chúng có thể được coi là nền tảng máy tính tự-đóng-gói. Bảo mật có thể được thiết kế trong các vùng chứa, cũng như được thực thi trong môi trường mà các vùng chứa đang hoạt động. Việc thực thi các

vùng chứa trong môi trường dựa trên đám mây là một điều phổ biến vì tính dễ quản lý và triển khai các vùng chứa rất phù hợp với mô hình đám mây. Hầu hết các nhà cung cấp dịch vụ đám mây đều có môi trường thân-thiện-với-vùng-chứa hỗ trợ các biện pháp kiểm soát bảo mật môi trường đám mây cần thiết cũng như cho phép vùng chứa tự đưa ra quyết định bảo mật trong vùng chứa.

---



**MÁCH NƯỚC CHO KỲ THI** Điện toán dựa-trên-đám-mây có những yêu cầu để xác định xem ai có thể thực hiện điều gì (các nhóm bảo mật) và điều gì có thể diễn ra và khi nào (phân bổ tài nguyên động) cũng như là để quản lý tính bảo mật của các thực thể được nhúng chẳng hạn như các vùng chứa. Một vài trong số những biện pháp kiểm soát này là giống nhau (các nhóm bảo mật và các vùng chứa) trong khi các biện pháp kiểm soát khác là duy nhất đối với môi trường đám mây (phân bổ tài nguyên động)

### Các Giải pháp

Các giải pháp bảo mật đám mây là tương tự như các giải pháp bảo mật CNTT truyền thống ở một điểm đơn giản: không có giải pháp nào dễ dàng và kỳ diệu. Bảo mật đạt được thông qua rất nhiều hành động được thiết kế để đảm bảo các chính sách bảo mật đang được tuân thủ. Cho dù trong môi trường đám mây hay trong môi trường tại-chỗ, bảo mật yêu cầu nhiều hoạt động, cùng với các chỉ số đo lường, báo cáo, quản lý và kiểm toán để đảm bảo tính hiệu quả. Đối với đám mây, một số yếu tố cụ thể cần phải được xem xét, chủ yếu là trong việc kết nối các nỗ lực bảo mật CNTT của doanh nghiệp hiện có với các phương pháp được sử dụng trong phiên bản đám mây.

## CASB

Một môi giới bảo mật truy cập đám mây (CASB) là một điểm thực thi chính sách bảo mật được đặt giữa người sử dụng dịch vụ đám mây và nhà cung cấp dịch vụ đám mây để quản lý các chính sách bảo mật của doanh nghiệp khi những tài nguyên dựa-trên-đám-mây được truy cập. CASB có thể là một đơn vị tại-chỗ hoặc dựa-trên-đám-mây, điều quan trọng là nó tồn tại giữa nhà cung cấp đám mây và kết nối của khách hàng, do đó cho phép nó làm trung gian cho tất cả các quyền truy cập. Doanh nghiệp sử dụng các nhà cung cấp CASB để giải quyết các rủi ro về dịch vụ đám mây, thực thi các chính sách bảo mật và tuân thủ các quy định. Một giải pháp CASB hoạt động ở bất cứ nơi nào các dịch vụ đám mây được thiết lập, ngay cả khi chúng nằm ngoài phạm vi doanh nghiệp và nằm ngoài tầm kiểm soát trực tiếp của các hoạt động của doanh nghiệp. CASB hoạt động ở cả quy mô lớn và quy mô nhỏ. Chúng có thể được thiết lập cấu hình để chặn một số kiểu truy cập như búa tạ (sledgehammer), đồng thời hoạt động như một con dao mổ, chỉ cắt tỉa các phần tử cụ thể. Chúng đòi hỏi sự đầu tư vào việc phát triển các chiến lược phù hợp dưới dạng chính sách dữ liệu có thể được thực thi khi dữ liệu di chuyển đến và từ đám mây.



## MÁCH NƯỚC CHO KỲ THI

Hãy nhớ rằng một CASB là một điểm thực thi chính sách bảo mật được thiết lập giữa người sử dụng và nhà cung cấp dịch vụ đám mây để quản lý các chính sách bảo mật doanh nghiệp cũng như những nguồn tài nguyên dựa-trên-đám-mây đang được truy cập.

## Bảo mật Ứng dụng

Nhiều ứng dụng được cung cấp bởi đám mây, bảo mật ứng dụng là một phần của phương trình. Một lần nữa, điều này ngay lập tức trở thành vấn đề về khả năng trách nhiệm được chia sẻ dựa trên mô hình triển khai đám mây đã chọn. Nếu khách hàng có trách nhiệm bảo mật các ứng dụng

thì các vấn đề cũng giống như trong doanh nghiệp, với sự bổ sung của việc duy trì phần mềm trên một nền tảng khác - đám mây. Quyền truy cập vào ứng dụng để cập nhật cũng như kiểm toán và các yếu tố bảo mật khác phải được xem xét và đưa vào quyết định kinh doanh đằng sau sự lựa chọn mô hình.

Nếu nhà cung cấp dịch vụ đám mây chịu trách nhiệm, có thể có lợi thế kinh tế về quy mô và các nhà cung cấp có thể thuận tiện khi có quản trị viên của riêng họ để duy trì các ứng dụng. Tuy nhiên, đi kèm với đó là chi phí và các vấn đề kiểm toán để đảm bảo nó đang được thực hiện một cách chính xác. Vào cuối ngày, các khái niệm về những gì cần phải thực hiện đối với bảo mật ứng dụng không thay đổi chỉ vì nó nằm trên đám mây. Những gì thay đổi là ai sẽ chịu trách nhiệm về nó, và nó được thực hiện như thế nào trong môi trường từ xa. Cũng như các yếu tố khác của trách nhiệm được chia sẻ tiềm năng, đây là điều cần được xác định trước khi thỏa thuận đám mây được ký kết, nếu nó không có trong thỏa thuận, thì người dùng hoàn toàn phải cung cấp câu trả lời [*hàm ý người dùng phải chịu trách nhiệm*].

### Cửa ngõ Web Bảo mật Thể-hệ-Kết-tiếp

Một *cửa ngõ web thể-hệ-kết-tiếp (SWG)* là một dịch vụ bảo mật mạng được đặt giữa người dùng và Internet. Các SWG hoạt động bằng cách kiểm tra các yêu cầu web so với chính sách của công ty để đảm bảo rằng các ứng dụng và trang web độc hại đã bị chặn và không thể truy cập được. Một giải pháp SWG bao gồm những công nghệ bảo mật thiết yếu như lọc URL, kiểm soát ứng dụng, ngăn ngừa thất thoát dữ liệu, chống vi-rút, và kiểm tra HTTPS được đưa vào một dịch vụ toàn diện để cung cấp khả năng bảo mật web mạnh mẽ.

Cửa ngõ web bảo mật và tường lửa thể-hệ-kết-tiếp (NGFW) tương tự nhau vì chúng đều cung cấp khả năng bảo vệ mạng nâng cao và có thể xác

định lưu lượng truy cập thân thiện với lưu lượng độc hại. Điểm mạnh của SWG nằm ở khả năng chúng để sử dụng tính năng kiểm tra lớp ứng dụng để xác định và bảo vệ chống lại các cuộc tấn công dựa-trên-Internet tiên tiến.

### **Những cân nhắc về Tường lửa trong Môi trường Đám mây**

Các *tường lửa* cần thiết trong môi trường đám mây cũng giống như cách chúng được cần đến trong môi trường CNTT truyền thống. Trong điện toán đám mây, chu vi mạng về cơ bản đã biến mất, nó là một chuỗi các dịch vụ chạy bên ngoài môi trường CNTT truyền thống và được kết nối thông qua Internet. Đối với đám mây, vị trí thực tế của người dùng và thiết bị mà họ đang sử dụng không còn quan trọng nữa. Đám mây cần có một tường lửa để chặn tất cả các kết nối trái phép đến phiên bản đám mây. Trong một số trường hợp, điều này được tích hợp vào môi trường đám mây, và trong những trường hợp khác, việc cung cấp chức năng này là tùy thuộc vào doanh nghiệp hoặc khách hàng đám mây.

### **Chi phí**

Câu hỏi đầu tiên trong tâm trí của tất cả các nhà quản lý là *chi phí* – việc sẽ làm tôi phải trả tổn chi phí bao nhiêu? Có những môi trường đám mây cơ bản nhất và rẻ tiền, nhưng chúng cũng không đi kèm với bất kỳ tính năng bảo mật được-tích-hợp nào, chẳng hạn như tường lửa, và để tính năng này cho khách hàng cung cấp. Do đó, điều này cần được tính vào bản so sánh chi phí với các môi trường đám mây có chức năng tường lửa được-tích-hợp sẵn. Chi phí cho tường lửa không chỉ nằm ở việc mua sắm mà còn nằm ở việc triển khai và vận hành. Và tất cả các yếu tố này cần phải được tính đến, không chỉ cho tường lửa xung quanh chu vi đám mây, mà còn cả tường lửa nội bộ được sử dụng để phân đoạn.

## Nhu cầu Phân đoạn

Như vừa được thảo luận ở đoạn trên, phân đoạn có thể mang lại thêm cơ hội để kiểm tra bảo mật giữa các phần tử tối quan trọng của hệ thống. Sử dụng các máy chủ cơ sở dữ liệu đang lưu giữ những viên ngọc quý của dữ liệu của công ty, là tài sản trí tuệ (IP), thông tin doanh nghiệp, hồ sơ khách hàng, mỗi doanh nghiệp có đặc thù riêng, nhưng tất cả đều có những hồ sơ quan trọng mà nếu bị mất hoặc bị tiết lộ sẽ là một vấn đề nghiêm trọng. Việc phân đoạn phần tử này của mạng và chỉ cho phép quyền truy cập cho một nhóm nhỏ người dùng đã được xác định tại phân đoạn cục bộ là một biện pháp bảo vệ an ninh mạnh mẽ để chống lại những kẻ tấn công qua mạng của bạn. Nó cũng có thể hoạt động để ngăn chặn phần mềm độc hại và ransomware tấn công những nguồn tài nguyên quan trọng này. Tường lửa được sử dụng để tạo ra các phân đoạn và nhu cầu về chúng phải được quản lý như một phần của gói các yêu cầu đối với việc thiết kế và tạo ra môi trường đám mây.

## Các Lớp [mô hình] Kết nối các Hệ thống Mở (OSI)

Các lớp [*của mô hình*] kết nối hệ thống mở (OSI) hoạt động như một phương tiện mô tả các cấp độ giao tiếp khác nhau trên một mạng. Từ lớp vật lý (lớp 1) đến lớp mạng (lớp 3) là lĩnh vực tiêu chuẩn của kết nối mạng. Lớp 4, lớp truyền tải, là nơi TCP và UDP hoạt động, và qua lớp 7, lớp ứng dụng, là nơi các ứng dụng hoạt động. Điều này có liên quan đến tường lửa vì hầu hết các cuộc tấn công cấp-dộ-d-ứng-dụng hiện đại không xảy ra ở lớp 1 - 3 mà xảy ra ở lớp 4 - 7. Điều này khiến cho các tường lửa CNTT truyền thống đã không được chuẩn bị một cách đầy đủ để xem xét và ngăn chặn hầu hết các cuộc tấn công hiện đại. Tường lửa thế-hệ-kết-tiếp hiện đại và cổng web bảo mật hoạt động cao hơn trong mô hình OSI, bao gồm cả lớp ứng dụng, để đưa ra quyết định truy cập. Các thiết bị này mạnh mẽ hơn và đòi hỏi nhiều thông tin và nỗ lực đáng kể hơn để

sử dụng một cách hiệu quả, nhưng với các hệ thống và khuôn khổ điều phối bảo mật, tự động hóa và phản hồi được tích hợp (security orchestration, automation and response - SOAR), chúng đang dần trở thành các thành phần có giá trị trong hệ thống bảo mật. Bởi vì mạng đám mây là một chức năng được ảo hóa, nhiều cuộc tấn công dựa-trên-mạng cũ sẽ không còn hoạt động trên mạng đám mây, nhưng vẫn có nhu cầu đổi mới với khả năng phát hiện cấp-cao-hơn của các thiết bị thế-hệ-kế-tiếp. Đây là những thiết bị bảo mật và tường lửa điển hình được coi là thiết yếu trong môi trường đám mây.

---



**MÁCH NƯỚC CHO KỲ THI** Các tường lửa và cửa ngõ web bảo mật thế-hệ-kế-tiếp hoạt động cao hơn mô hình OSI, sử dụng dữ liệu của lớp ứng dụng để đưa ra các quyết định truy cập.

### **Biện pháp kiểm soát Đám-mây-tự-nhiên so với Giải pháp Bên-thứ-ba**

Khi ai đó đang xem xét các công cụ điều phối và tự động hóa bảo mật đám mây, họ sẽ có hai nguồn để xem xét. Đầu tiên là bộ công cụ được cung cấp bởi nhà cung cấp dịch vụ đám mây. Các biện pháp kiểm soát đám-mây-tự-nhiên này sẽ khác nhau tùy theo nhà cung cấp và theo dịch vụ cụ thể mà doanh nghiệp đang đăng ký như một phần của thỏa thuận người dùng và giấy phép dịch vụ. Các công cụ của bên-thứ-ba cũng tồn tại để khách hàng có thể được cấp phép và triển khai trong môi trường đám mây. Quyết định này nên dựa trên việc xem xét một cách toàn diện các yêu cầu, bao gồm cả khả năng và chi phí sở hữu. Đây không phải là một lựa chọn nhị phân A hoặc B đơn giản vì có rất nhiều chi tiết cần phải xem xét. Mỗi loại sẽ tích hợp với môi trường bảo mật hiện tại như thế nào? Hoạt động sẽ được xử lý như thế nào, và ai sẽ phải học những công cụ nào để đạt được các mục tiêu? Đây là một bản đánh giá đầy đủ về con



người, quy trình và công nghệ, bởi vì bất kỳ một trong số ba điều này đều có thể thực hiện hoặc phá vỡ một trong hai cách triển khai này.

## Tóm tắt Chương

Trong chương này, đầu tiên, bạn làm quen với các kiểm soát bảo mật đám mây. Trong phần đầu tiên, các chủ đề về tính sẵn sàng cao giữa các khu vực, các chính sách tài nguyên, quản lý bí mật, tích hợp và kiểm toán đã được đề cập. Tiếp theo là vấn đề lưu trữ với những cân nhắc về quyền hạn, mã hóa, sao chép và tính sẵn sàng cao. Tiếp theo là một cuộc thảo luận về mạng, với các phần phụ về mạng ảo, mạng con công cộng và riêng tư, phân đoạn cũng như kiểm tra và tích hợp API. Phần phụ cuối cùng trong các biện pháp kiểm soát bảo mật là về các khía cạnh tính toán của hệ thống đám mây, trong đó các chủ đề về nhóm bảo mật, phân bổ tài nguyên động, nhận thức về phiên bản, điểm đầu cuối đám mây riêng tư ảo và bảo mật vùng chứa được đề cập.

Chương này kết thúc bằng việc xem xét các giải pháp liên quan đến bảo mật đám mây. Trong phần này, điểm trung gian bảo mật truy cập đám mây (CASB), bảo mật ứng dụng, của ngõ web bảo mật thế-hệ-kế-tiếp (SWG) và các cân nhắc về tường lửa trong môi trường đám mây đã được trình bày. Chương này đã khép lại với một phần về các biện pháp kiểm soát đám-mây-tự-nhiên so với các giải pháp của bên-thứ-ba.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Các chính sách và thủ tục được sử dụng để kết nối các hệ thống IAM của doanh nghiệp với đám mây để hỗ trợ cho việc giao tiếp với dữ liệu được gọi là gì?

  - A. Kiểm tra và tích hợp API
  - B. Quản lý bí mật
  - C. Phân bổ tài nguyên động
  - D. Bảo mật vùng chứa.
2. Những thuật ngữ nào dưới đây không liên quan đến bảo mật lưu trữ trên đám mây?

  - A. Quyền hạn
  - B. Tính sẵn sàng cao
  - C. Phân đoạn
  - D. Mã hóa.
3. Các chính sách tài nguyên liên quan đến tất cả những điều dưới đây, ngoại trừ?

  - A. Quyền hạn
  - B. IAM
  - C. Chi phí
  - D. Quyền truy cập.
4. Kết nối mạng ảo trong một môi trường đám mây có thể bao gồm tất cả những điều dưới đây, ngoại trừ?

  - A. Điểm đầu cuối VPC
  - B. Các mạng con công khai
  - C. Các mạng con riêng tư

- D. Ảo hóa chức năng mạng.**
- 5.** Cấu trúc nào được sử dụng để quản lý người dùng trong môi trường đám mây?
- A. Quyền hạn**  
**B. Nhận thức về phiên bản**  
**C. Phân bổ tài nguyên động**  
**D. Các nhóm bảo mật.**
- 6.** Điểm nào sau đây là điểm thực thi chính sách bảo mật được đặt giữa người sử dụng và nhà cung cấp dịch vụ đám mây để quản lý các chính sách bảo mật của doanh nghiệp khi các tài nguyên dựa-trên-đám-mây được truy cập?
- A. SWG**  
**B. Điểm đầu cuối VPC**  
**C. CASB**  
**D. Các chính sách về tài nguyên.**
- 7.** Các cửa ngõ web bảo mật hoạt động bằng cách kiểm tra tại điểm nào trong kênh giao tiếp?
- A. Thành viên nhóm bảo mật**  
**B. Lớp ứng dụng**  
**C. Nhận thức về phiên bản**  
**D. Kiểm tra API.**
- 8.** Những điều nào dưới đây là tối quan trọng trong bảo mật đám mây? (Chọn tất cả đáp án đúng).
- A. Tường lửa**  
**B. Tích hợp và kiểm toán**  
**C. Quản lý bí mật**  
**D. Mã hóa**
- 9.** Tính sẵn sàng cao phụ thuộc vào những điều nào dưới đây?
- A. Quản lý bí mật**

- B.** Phân bổ tài nguyên động
  - C.** Bảo mật vùng chứa
  - D.** CASB
- 10.** Phần tử quan trọng nhất trong việc tìm hiểu tình hình bảo mật đám mây hiện tại của bạn là gì?
- A.** Thỏa thuận dịch vụ đám mây
  - B.** Các biện pháp kiểm soát bảo mật mạng
  - C.** Mã hóa
  - D.** Bảo mật ứng dụng.

## Đáp án

1. **B.** Quản lý bí mật là tên gọi được sử dụng để biểu thị các chính sách và thủ tục được sử dụng để kết nối các hệ thống IAM của doanh nghiệp và đám mây để cho phép giao tiếp với dữ liệu.
2. **C.** Phân đoạn là một vấn đề mạng, tách biệt với lưu trữ.
3. **C.** Chi phí không phải là một phần của các chính sách tài nguyên. Các chính sách tài nguyên mô tả cách thức các phần tử của IAM, cả trong doanh nghiệp lẫn trong đám mây, hoạt động cùng nhau để cung cấp tài nguyên.
4. **A.** Các điểm cuối VPC không phải là một phần của mạng ảo; mặc dù chúng là các ứng dụng ảo, nhưng chúng không phải là một phần của mạng.
5. **D.** Nhóm bảo mật được sử dụng để quản lý người dùng trong môi trường đám mây.
6. **C.** Định nghĩa của điểm trung gian bảo mật truy cập đám mây (CASB) là một điểm thực thi chính sách bảo mật được đặt giữa người sử dụng và nhà cung cấp dịch vụ đám mây để quản lý các chính sách bảo mật của doanh nghiệp khi các tài nguyên dựa-trên-đám-mây được truy cập.
7. **B.** SWGs hoạt động ở lớp ứng dụng, giúp xác định mức độ phù hợp của lớp ứng dụng.
8. **A, B, C và D.** Tất cả đều đóng vai trò quan trọng trong việc bảo mật môi trường đám mây.
9. **B.** Tính sẵn sàng cao phụ thuộc vào khả năng của đám mây để phân bổ lại tài nguyên trong trường hợp có sự cố, đây là một trong những chức năng của phân bổ tài nguyên động.
10. **A.** Mặc dù rất nhiều thứ liên quan đến bảo mật đám mây, nhưng tất cả đều bắt nguồn từ nền tảng của thỏa thuận dịch vụ đám mây, trong đó mô tả tất cả các điều khoản dịch vụ.

## Chương 23 Các Biện pháp kiểm soát Quản lý Tài khoản và Danh tính

---

### Các Biện pháp kiểm soát Quản lý Danh tính và Tài khoản

Trong chương này bạn sẽ

- Xem xét các khái niệm và thực tiễn về danh tính,
  - Xem xét về các kiểu tài khoản,
  - Đánh giá các chính sách tài khoản khác nhau được sử dụng để quản lý các tài khoản,
  - Đưa ra một kịch bản, triển khai các biện pháp kiểm soát quản lý tài khoản và danh tính.
- 

Danh tính hình thành nên nền tảng cơ bản của sự xác thực trong các hệ thống máy tính. Phần thứ hai của nền tảng cơ bản này là việc sử dụng các tài khoản được quản lý bởi một loạt các chính sách để thực thi một mức độ rủi ro tương ứng với việc sử dụng chúng [các tài khoản]. Chương này khám phá những chủ đề về danh tính, tài khoản, và các chính sách liên quan để quản lý những thực thể này trong doanh nghiệp.

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 3.7 của kỳ thi CompTIA Security+: Đưa ra một kịch bản, hãy triển khai các biện pháp kiểm soát quản lý tài khoản và danh tính.

## Danh tính

Nhận dạng là quá trình chỉ định một ID máy tính cho một người dùng, máy tính, thiết bị mạng hoặc một tiến trình máy tính cụ thể. Quá trình nhận dạng thường chỉ được thực hiện một lần, khi một ID người dùng được cấp cho một người dùng cụ thể. Nhận dạng người dùng cho phép xác thực và cấp phép để tạo cơ sở cho trách nhiệm giải trình. Vì mục đích trách nhiệm giải trình, ID người dùng không nên được chia sẻ và vì mục đích bảo mật, ID người dùng không được mô tả chức năng công việc. Thực tiễn này cho phép bạn theo dõi các hoạt động đối với người dùng riêng lẻ hoặc các tiến trình máy tính riêng lẻ để người dùng có thể chịu trách nhiệm về các hành động của họ. Nhận dạng thường có dạng ID đăng nhập hoặc ID người dùng. Một đặc điểm bắt buộc của các ID đó là chúng phải là duy nhất.

## Nhà cung cấp Danh tính (IdP)

Thuật ngữ *nha cung cap danh tinh (IdP)* được sử dụng để biểu thị một hệ thống hoặc dịch vụ tạo ra, duy trì và quản lý những thông tin nhận dạng. IdP có thể đa dạng về quy mô và phạm vi - từ hoạt động cho một hệ thống đơn lẻ đến hoạt động trên quy mô toàn doanh nghiệp. Ngoài ra, chúng có thể được vận hành cục bộ, phân tán hoặc liên kết, tùy thuộc vào giải pháp cụ thể. Rất nhiều tiêu chuẩn đã được sử dụng để đạt được những dịch vụ này, bao gồm cả những tiêu chuẩn được xây dựng trên Ngôn ngữ Đánh dấu Xác nhận Bảo mật (SAML), OpenID và OAuth. Các tiêu chuẩn này được đề cập trong Chương 24, "Triển khai Xác thực và Cấp phép".



## MÁCH NƯỚC CHO KỲ THI

Nhà cung cấp danh tính (IdP) tạo ra, quản lý và chịu trách nhiệm cho việc xác thực danh tính.

## Các Thuộc tính

Bạn sẽ mô tả các phần tử của một danh tính như thế nào? Các *thuộc tính* nhận dạng là những đặc điểm cụ thể của danh tính – tên gọi, phòng ban, vị trí, ID đăng nhập, số nhận dạng, địa chỉ e-mail, v.v... - được sử dụng để mô tả một thực thể cụ thể một cách chính xác. Những phần tử này là cần thiết nếu muốn lưu trữ thông tin nhận dạng trong một số dạng danh bạ, chẳng hạn như danh bạ LDAP. Các chi tiết của lược đồ cần được xem xét để bao gồm các thuộc tính đối với con người, thiết bị (các máy chủ và thiết bị) và dịch vụ (các ứng dụng và chương trình), vì bất kỳ thứ nào trong số này đều có thể đã có danh tính trong hệ thống. Chi tiết của các lược đồ đã được xử lý thông qua Active Directory, các IdP khác nhau, v.v..., vì vậy đây không phải là thứ cần phải được tạo ra, tuy nhiên, nó cần phải được tìm hiểu.

## Các Chứng nhận

Xác thực dựa-trên-*chứng-nhận* là một phương tiện chứng minh danh tính thông qua việc xuất trình một chứng nhận. Các chứng nhận cung cấp một phương pháp thiết lập tính xác thực của các đối tượng cụ thể như khóa công khai của một cá nhân hoặc phần mềm đã được tải xuống. Một *chứng nhận kỹ thuật số* là một tập tin kỹ thuật số được gửi dưới dạng tập tin đính kèm cho một thông điệp và được sử dụng để xác minh rằng thư thực sự đến từ thực thể mà nó tuyên bố là đến từ đó. Việc sử dụng chứng nhận kỹ thuật số là một phương tiện có thể xác minh được để thiết lập quyền sở hữu một mục (cụ thể là chứng nhận). Khi chứng nhận được giữ trong một cửa hàng để ngăn chặn việc giả mạo hoặc khai thác, điều này sẽ trở thành một phương tiện nhận dạng đáng tin cậy, đặc biệt khi được kết hợp với một yếu tố bổ sung như điều gì đó mà bạn biết hoặc sinh trắc học. Các chi tiết kỹ thuật đằng sau chứng nhận kỹ thuật số được đề cập trong Chương 25, "Cơ sở hạ tầng Khóa Công khai".

## Token

Một *mã thông báo* (*token*) truy cập là một đối tượng vật lý xác định các quyền truy cập cụ thể và trong xác thực, nó thuộc về yếu tố "thứ gì đó mà bạn có". Ví dụ, chìa khóa nhà của bạn là một mã thông báo truy cập vật lý cơ bản cho phép bạn đi vào nhà của mình. Mặc dù chìa khóa đã được sử dụng để mở khóa thiết bị trong nhiều thế kỷ qua, nhưng chúng vẫn có một số hạn chế. Chìa khóa được ghép nối riêng với một ổ khóa hoặc một bộ các khóa và chúng không dễ gì thay đổi. Có thể dễ dàng thêm vào một người dùng được cấp phép chỉ bằng cách cấp cho người dùng một bản sao của khóa, nhưng khó hơn rất nhiều khi cấp cho người dùng đó quyền truy cập có chọn lọc trừ khi khu vực cụ thể đó đã được thiết lập một khóa riêng biệt. Cũng rất khó để lấy đi quyền truy cập từ một chìa khóa hoặc người giữ chìa khóa, điều này thường yêu cầu làm lại khóa cho toàn bộ hệ thống.

Trong nhiều doanh nghiệp, xác thực truy cập vật lý đã chuyển sang thẻ tần số vô tuyến không tiếp xúc và các đầu đọc lân cận. Khi được đưa đến gần đầu đọc thẻ, thẻ sẽ gửi mã bằng sóng vô tuyến. Đầu đọc nhận mã này và truyền đến bảng điều khiển. Bảng điều khiển kiểm tra mã so với đầu đọc mà nó đang được đọc từ đó và kiểu quyền truy cập mà thẻ đó đang có trong cơ sở dữ liệu của nó. Ưu điểm của loại hệ thống dựa-trên-mã-thông-báo này bao gồm thực tế là bất kỳ thẻ nào cũng có thể bị xóa khỏi hệ thống mà không gây ảnh hưởng đến bất kỳ thẻ nào khác hoặc phần còn lại của hệ thống. Ngoài ra, tất cả các cửa được kết nối với hệ thống có thể được phân đoạn theo bất kỳ kiểu hoặc hình thức nào để tạo ra nhiều khu vực truy cập, với các quyền hạn khác nhau cho mỗi cửa. Bản thân các mã thông báo cũng có thể được nhóm lại theo nhiều cách để cung cấp các mức độ truy cập khác nhau cho các nhóm người khác nhau. Tất cả các mức độ truy cập hoặc phân đoạn cửa có thể được sửa đổi một cách nhanh chóng và dễ dàng nếu không gian của tòa nhà được bố trí lại.

Những công nghệ mới hơn đang bổ sung thêm các khả năng cho các hệ thống dựa-trên-mã-thông-báo tiêu chuẩn. Thẻ thông minh cũng có thể được sử dụng để mang mã thông báo nhận dạng. Hạn chế chính của xác thực dựa-trên-mã-thông-báo là chỉ có mã thông báo được xác thực. Do đó, việc đánh cắp mã thông báo có thể cấp cho bất kỳ ai đang sở hữu mã thông báo quyền truy cập vào những gì hệ thống đang bảo vệ.

Rủ ro bị đánh cắp mã thông báo có thể được bù đắp bằng cách sử dụng xác thực đa yếu tố (đã được mô tả trong Chương 12, "Xác thực và Cấp phép"). Một trong những cách mà mọi người đã cố gắng đạt được xác thực đa yếu tố là bổ sung thêm yếu tố sinh trắc học vào hệ thống. Một giải pháp thay thế ít tốn kém hơn là sử dụng mã thông báo phần cứng trong quy trình xác thực phản hồi/thử thách. Theo cách này, mã thông báo hoạt động như một cơ chế xác thực "thứ mà bạn có" và "thứ mà bạn biết".

Có một số biến thể trên loại thiết bị này đang tồn tại, nhưng chúng đều hoạt động trên các nguyên tắc về cơ bản là giống nhau. Thiết bị có màn hình LCD và có thể có hoặc không có bàn phím số. Các thiết bị không có bàn phím sẽ hiển thị mật khẩu (thường chỉ là một dãy số) thay đổi trong khoảng thời gian không đổi, thường là khoảng 60 giây một lần. Khi một cá nhân cố gắng đăng nhập vào một hệ thống, họ sẽ nhập số ID người dùng của chính họ và sau đó nhập số được hiển thị trên màn hình LCD. Hai số này được nhập riêng biệt hoặc được nối với nhau. Số ID riêng của người dùng là bí mật và điều này ngăn chặn việc ai đó sử dụng thiết bị đã mất. Hệ thống biết người dùng có thiết bị nào và được đồng bộ hóa với thiết bị đó để nó biết số lẽ ra phải được hiển thị. Vì con số này liên tục thay đổi, kẻ tấn công tiềm năng đã từng có thể nhìn thấy dãy số này sẽ không thể sử dụng nó sau đó, vì mã sẽ thay đổi. Các thiết bị có bàn phím hoạt động theo cách tương tự (và cũng có thể được thiết kế để hoạt

động như một máy tính đơn giản). Cá nhân muốn đăng nhập vào hệ thống trước tiên sẽ nhập mã số định danh cá nhân của mình vào máy tính. Sau đó, họ sẽ cố gắng đăng nhập. Tiếp theo, hệ thống sẽ đưa ra một thử thách, người dùng sẽ phải nhập thử thách đó vào máy tính và nhấn một phím chức năng đặc biệt. Máy tính sau đó sẽ xác định câu trả lời chính xác và hiển thị nó. Người dùng cung cấp phản hồi cho hệ thống mà họ đang cố gắng đăng nhập và hệ thống xác minh rằng đây là phản hồi chính xác. Vì mỗi người dùng chỉ có một mã PIN khác nhau, hai cá nhân nhận được cùng một thử thách cũng sẽ có phản hồi khác nhau. Thiết bị cũng có thể sử dụng ngày hoặc giờ làm biến số để tính toán phản hồi để cùng một thử thách tại các thời điểm khác nhau sẽ đưa ra các phản hồi khác nhau, ngay cả đối với cùng một cá nhân.

### **Khóa SSH**

Các *khóa SSH* là những thông tin đăng nhập truy cập được sử dụng bởi giao thức Secure Shell (SSH). Chúng hoạt động giống như tên người dùng và mật khẩu, nhưng các khóa SSH chủ yếu được sử dụng cho các quy trình và dịch vụ được tự động hóa. Các khóa SSH cũng được sử dụng trong việc triển khai các hệ thống đăng nhập một-lần (SSO) được sử dụng bởi các quản trị viên hệ thống. Các khóa SSH được trao đổi bằng cách sử dụng mật mã khóa công khai, và chính bản thân các khóa là những khóa kỹ thuật số. Khái niệm về mật mã khóa công khai được đề cập trong Chương 16, "Những Khái niệm về Mật mã".

### **Thẻ Thông minh**

Các *thẻ thông minh* là những thiết bị lưu trữ mã thông báo (token) mật mã được liên kết với một danh tính. Hình thức thực tế thường là một thẻ vật lý, có kích thước bằng thẻ tín dụng, có chứa một con chip được nhúng bao gồm các thành phần điện tử khác nhau để hoạt động như một vật thể mang thông tin vật lý.

Chính phủ liên bang Hoa Kỳ có một số giải pháp thẻ thông minh để nhận dạng nhân sự. Thẻ Xác minh Danh tính Cá nhân (Personal Identity Verification - PIV) là một thẻ thông minh của chính phủ Hoa Kỳ có chứa dữ liệu thông tin xác thực của chủ thẻ được sử dụng để xác định quyền truy cập vào các cơ sở và hệ thống thông tin của liên bang. Thẻ Truy cập Chung (Common Access Card - CAC) là một thẻ thông minh được sử dụng bởi Bộ Quốc phòng Hoa Kỳ (DoD) dành cho quân nhân tại ngũ, các thành viên của Quân nhân dự bị Được chọn, dân thường DoD và các nhà thầu đủ điều kiện. Giống như thẻ PIV, nó được sử dụng để mang dữ liệu thông tin đăng nhập của chủ thẻ, dưới dạng chứng nhận và để xác định quyền truy cập vào các cơ sở và hệ thống thông tin của liên bang.



**MÁCH NƯỚC CHO KỲ THI** Hãy ghi nhớ các kiểu sử dụng khác nhau đối với các mã thông báo, khóa và thẻ thông minh. Một mã thông báo truy cập là một đối tượng vật lý xác định quyền truy cập cụ thể, và trong xác thực, được gọi là yếu tố “thứ gì đó mà bạn có”. Các khóa SSH được sử dụng chủ yếu cho các quy trình và dịch vụ được tự động hóa. Một thẻ PIV là một thẻ thông minh được sử dụng cho các nhân viên liên bang và các nhà thầu. Các thẻ CAC được sử dụng cho quân nhân tại ngũ, các thành viên của Quân nhân dự bị Được chọn, và các nhà thầu đủ điều kiện.

### Các Kiểu Tài khoản

Để quản lý đặc quyền của rất nhiều người khác nhau một cách hiệu quả trên cùng một hệ thống, một cơ chế tách biệt mọi người thành những thực thể (người dùng) khác nhau là điều bắt buộc, từ đó bạn có thể kiểm soát quyền truy cập ở cấp độ cá nhân. Sẽ rất tiện lợi và hiệu quả khi có thể tập hợp người dùng lại cùng nhau khi cấp cho nhiều người (các nhóm) khác nhau quyền truy cập vào tài nguyên cùng một lúc. Tại những thời

điểm khác, sẽ rất hữu ích nếu có thể cấp hoặc hạn chế quyền truy cập dựa trên công việc hoặc chức năng của một người trong tổ chức (vai trò). Mặc dù bạn có thể quản lý các đặc quyền trên cơ sở một mình người dùng, nhưng việc quản lý người dùng, nhóm và phân công vai trò cùng nhau sẽ thuận tiện và hiệu quả hơn nhiều.

### Tài khoản Người dùng

Thuật ngữ *tài khoản người dùng* đề cập đến thông tin đăng nhập tài khoản được sử dụng khi truy cập vào hệ thống máy tính. Trong quản lý đặc quyền, một người dùng là một cá nhân, chẳng hạn như "John Forthright" hoặc "Sally Jenkins". Đây nói chung là mức thấp nhất được xác định bởi quản lý đặc quyền và là khu vực phổ biến nhất để giải quyết quyền truy cập, quyền hạn và khả năng. Khi truy cập vào hệ thống máy tính, mỗi người dùng thường được cấp một ID người dùng - một mã định danh chữ và số duy nhất mà họ sẽ sử dụng để nhận dạng bản thân khi đăng nhập hoặc truy cập vào một hệ thống. ID người dùng thường dựa trên một số kết hợp của tên, tên đệm và họ của người dùng và cũng thường bao gồm cả các chữ số. Khi phát triển một lược đồ để lựa chọn ID người dùng, bạn nên nhớ rằng ID người dùng phải là duy nhất cho mỗi người dùng, nhưng chúng cũng phải khá dễ nhớ để người dùng có thể ghi nhớ và sử dụng. Vì ID người dùng được sử dụng để xác định người đã thực hiện các hành động cụ thể nên điều quan trọng là không có thông tin đăng nhập chung hoặc được chia sẻ. Một trong hai trường hợp này làm cho việc truy xuất nguồn gốc đối với người dùng được ủy quyền trở nên khó khăn, nếu không muốn nói là không thể.



**MÁCH NƯỚC CHO KỲ THI** Việc có các ID người dùng duy nhất và không được chia sẻ cho tất cả mọi người dùng của một hệ thống là điều quan trọng khi cần phải điều tra về các biện pháp kiểm soát truy cập. Với một số ngoại lệ đáng chú ý, nói chung, một người dùng muốn truy cập vào hệ thống máy tính trước tiên phải có ID người dùng được tạo cho họ trên hệ thống mà họ muốn sử dụng. Điều này thường được thực hiện bởi quản trị viên hệ thống, quản trị viên bảo mật hoặc người dùng có đặc quyền khác và đây là bước đầu tiên trong quản lý đặc quyền - người dùng không nên được phép tạo tài khoản của riêng họ.

Khi tài khoản được tạo và ID người dùng đã được chọn, quản trị viên có thể chỉ định các quyền cụ thể cho người dùng đó. Quyền kiểm soát những gì người dùng được phép thực hiện trên hệ thống - họ có thể truy cập tập tin nào, chương trình nào họ có thể thực thi, v.v... Trong khi máy tính cá nhân thường chỉ có một hoặc hai tài khoản người dùng, các hệ thống lớn hơn như máy chủ và máy tính lớn (mainframe) có thể có đến hàng trăm tài khoản trên cùng một hệ thống.

Thực thi chính sách tài khoản là một phần quan trọng của hệ thống thông tin xác thực người dùng. Việc quản lý thông tin xác thực bắt đầu bằng các chính sách nêu rõ các mục tiêu mong muốn. Các yếu tố chính của chính sách bao gồm việc cấm chia sẻ tài khoản và các tài khoản chung nhưng không được chỉ định cho người dùng. Đối với những người dùng có nhiều vai trò, nhiều tài khoản có thể là cần thiết, nhưng những tài khoản này cần được phân định theo chính sách thay vì theo cơ sở đột xuất. Các quy tắc quản lý thông tin xác thực, chẳng hạn như chính sách mật khẩu, nên được ban hành, bao gồm các thủ tục khóa và khôi phục tài khoản. Khi người dùng không còn được cấp phép, chẳng hạn như khi

họ rời khỏi công ty hoặc thay đổi công việc, tài khoản của họ nên được vô hiệu hóa chứ không phải bị xóa bỏ.

### **Tài khoản/Thông tin đăng nhập Chung và Được Chia sẻ**

Các *tài khoản* được chia sẻ đi ngược lại tiền đề cụ thể rằng các tài khoản tồn tại để có thể theo dõi hoạt động của người dùng. Điều này cho thấy, có những thời điểm mà tài khoản dùng chung được sử dụng cho các nhóm như khách (tài khoản khách sẽ được đề cập trong phần tiếp theo). Đôi khi các tài khoản được chia sẻ được gọi là *tài khoản chung* và chỉ tồn tại để cung cấp một nhóm chức năng cụ thể, chẳng hạn như trong máy tính cá nhân chạy ở chế độ kiosk, với trình duyệt bị giới hạn trong việc truy cập các trang web cụ thể chỉ dưới dạng hiển thị thông tin. Trong những trường hợp này, việc có thể theo dõi hoạt động của người dùng là không đặc biệt hữu ích.

Một dạng phổ biến của một tài khoản được chia sẻ là một tài khoản được tạo ra để chạy tập lệnh vận hành vào ban đêm. Vì mọi hành động phải được liên kết với một tài khoản người dùng, một tài khoản được chia sẻ dưới tên của một người dùng hàng loạt có thể được sử dụng để chạy các công việc hàng loạt. Đây là một tập hợp các *thông tin đăng nhập chung*, không thực sự được liên kết với một người mà được liên kết với một loại quy trình cụ thể (công việc hàng loạt, sao lưu, v.v...). Những thông tin xác thực này được quản trị viên duy trì nhưng được dành riêng cho các mục đích sử dụng cụ thể, chẳng hạn như thực hiện các công việc hàng loạt. Bởi vì những tài khoản này về bản chất là cục bộ và đang được sử dụng để chạy các tác vụ, chúng có thể bị hạn chế chức năng (chẳng hạn như không được phép đăng nhập), do đó làm giảm tính hữu dụng của chúng đối với một kẻ tấn công.

Một ví dụ điển hình được tìm thấy ở nhiều doanh nghiệp sẽ giống với tình huống sau:

**Vấn đề:** Các tổ chức sử dụng một tài khoản và mật khẩu duy nhất cho rất nhiều người: ví dụ: tài khoản quản trị viên toàn cầu cục bộ cho Office 365 hoặc tài khoản root trong Salesforce.

**Rủi ro:** Các tài khoản dùng chung thường được phân phối và thường thì thông tin đăng nhập (tên người dùng và mật khẩu) được đặt ở một vị trí dùng chung. Đây là một tiêu chuẩn bảo mật nghiêm trọng không-thể-cấm (no-no) bởi vì bạn không thể biết chính xác từ việc kiểm toán rằng ai đã truy cập vào nội dung gì và khi nào họ đã thực hiện điều đó. Bạn có thể nhìn thấy tài khoản, nhưng bạn không biết người dùng nào đang thực hiện các hành động.

**Giải pháp hiện đại:** Quản trị viên Azure AD thiết lập cấu hình ứng dụng nào mà người dùng có thể truy cập bằng cách sử dụng Bảng điều khiển Truy cập (Access Panel) và chọn loại đăng nhập một-lần thích hợp nhất cho ứng dụng đó. Việc sử dụng loại đăng nhập một-lần dựa-trên-mật-khẩu cho phép Azure AD hoạt động như một loại “điểm trung gian (broker)” trong quá trình đăng-nhập cho ứng dụng đó.

### Tài khoản Khách

Các *tài khoản khách* thường được sử dụng trên mạng công ty để cung cấp quyền truy cập cho khách viếng thăm vào Internet và một số tài nguyên công ty phổ biến khác, chẳng hạn như các máy chiếu, máy in trong phòng họp, v.v... Một lần nữa, giống như những tài khoản chung, những kiểu tài khoản này bị giới hạn trong khả năng mạng của chúng chỉ trong một tập hợp các máy đã được xác định, với một bộ quyền truy cập đã được xác định, giống như việc một người dùng ghé thăm một trang web công cộng của một công ty qua Internet. Vì vậy, việc ghi lại nhật ký và theo dõi hoạt động là rất ít hoặc không sử dụng, từ đó, chi phí cho việc thiết lập một tài khoản duy nhất không có ý nghĩa lầm.

## Tài khoản Dịch vụ

Các *tài khoản dịch vụ* là những tài khoản được sử dụng để chạy các tiến trình không đòi hỏi sự tác động của con người để khởi đầu, dừng, hoặc quản lý. Từ việc chạy các công việc hàng loạt trong trung tâm dữ liệu đến thực thi các tác vụ đơn giản mà tổ chức phải hoàn thành vì mục đích tuân thủ quy định, có rất nhiều lý do để chạy các tiến trình với tài khoản dịch vụ không yêu cầu một chủ tài khoản. Xét từ góc độ bảo mật, quản trị viên có thể cấu hình tài khoản dịch vụ để tối thiểu rủi ro liên quan đến chúng. Ví dụ, trong hệ thống Windows, quản trị viên có thể ngăn tài khoản dịch vụ đăng nhập vào hệ thống. Điều này hạn chế một số véc-tơ tấn công có thể được áp dụng cho các tài khoản này. Một điều khoản bảo mật khác có thể được áp dụng cho các tài khoản dịch vụ chạy các công việc hàng loạt vào ban đêm là hạn chế thời điểm chúng có thể chạy. Bất kỳ tài khoản dịch vụ nào phải chạy ở chế độ đặc quyền được nâng cao cũng có thể được chỉ định để nhận thêm giám sát và kiểm soát.



## MÁCH NƯỚC CHO KỲ THI

Các tài khoản dịch vụ hoạt động mà không cần sự tác động của con người và chỉ được cấp quyền hạn vừa đủ để chạy các dịch vụ mà chúng hỗ trợ.

## Các Chính sách Tài khoản

Phương pháp then chốt được sử dụng để kiểm soát hầu hết các hệ thống vẫn là phương pháp dựa trên mật khẩu. Kết hợp với một chính sách mật khẩu bắt buộc mạnh mẽ để ngăn cấm chia sẻ mật khẩu và thông tin đăng nhập, sử dụng những mật khẩu định hình nền nền tảng để hỗ trợ cho ý tưởng rằng mỗi ID người dùng nên có thể truy nguyên được đến hoạt động của một người duy nhất. Mật khẩu cần phải được quản lý để cung cấp mức độ bảo vệ thích hợp. Chúng cần phải đủ mạnh để chống lại các cuộc tấn công, và không quá khó để người dùng nhớ được chúng. Một

chính sách mật khẩu có thể hoạt động để đảm bảo rằng các bước cần thiết đã được thực hiện để ban hành một giải pháp mật khẩu an toàn, bởi cả người dùng lẫn hệ thống cơ sở hạ tầng mật khẩu.

### **Độ phức tạp của Mật khẩu**

Mọi tổ chức nên có các yêu cầu về *độ phức tạp của mật khẩu* được xác định trước mà các mật khẩu cần phải đáp ứng. Các yêu cầu điển hình chỉ định rằng mật khẩu phải đáp ứng yêu cầu về độ dài và có các ký tự từ ít nhất 3 trong số 4 nhóm sau: các ký tự tiếng Anh in hoa ( A đến Z), các ký tự tiếng Anh in thường (từ a đến z), các chữ số (0 đến 9) và những ký tự đặc biệt (chẳng hạn như !,\$,# và %).



**MÁCH NƯỚC CHO KỲ THI** Bạn có thể nhận biết được về nghiên cứu mới từ NIST chỉ ra rằng các quy tắc về độ phức tạp của mật khẩu được thiết kế để bắt buộc thêm entropy vào mật khẩu, do đó việc này có nguy cơ xảy ra các hành vi mật khẩu khác, ít được người dùng mong muốn, chẳng hạn như viết chúng ra hoặc tạo ra các phiên bản của chúng với phần tử số ngày càng tăng . Hướng dẫn mới nhất của NIST (Đặc San 800-63B, tháng 6 năm 2017) là mật khẩu dài cung cấp sự bảo vệ tốt nhất. Tuy nhiên, SP 800-63B đã được xuất bản sau khi CompTIA phát hành các mục tiêu của kỳ thi Security+, vì vậy đối với kỳ thi, bạn nên tìm hiểu các yêu cầu về độ phức tạp của mật khẩu đã được-thử-và-đúng được liệt kê tại đây.



**LƯU Ý** Ngày nay, mật khẩu mạnh là chưa đủ. Năng lực tính toán cho phép tội phạm mạng chạy những chương trình tinh vi để có được hoặc thử một lượng lớn các thông tin đăng nhập. Đây là lý do tại sao việc

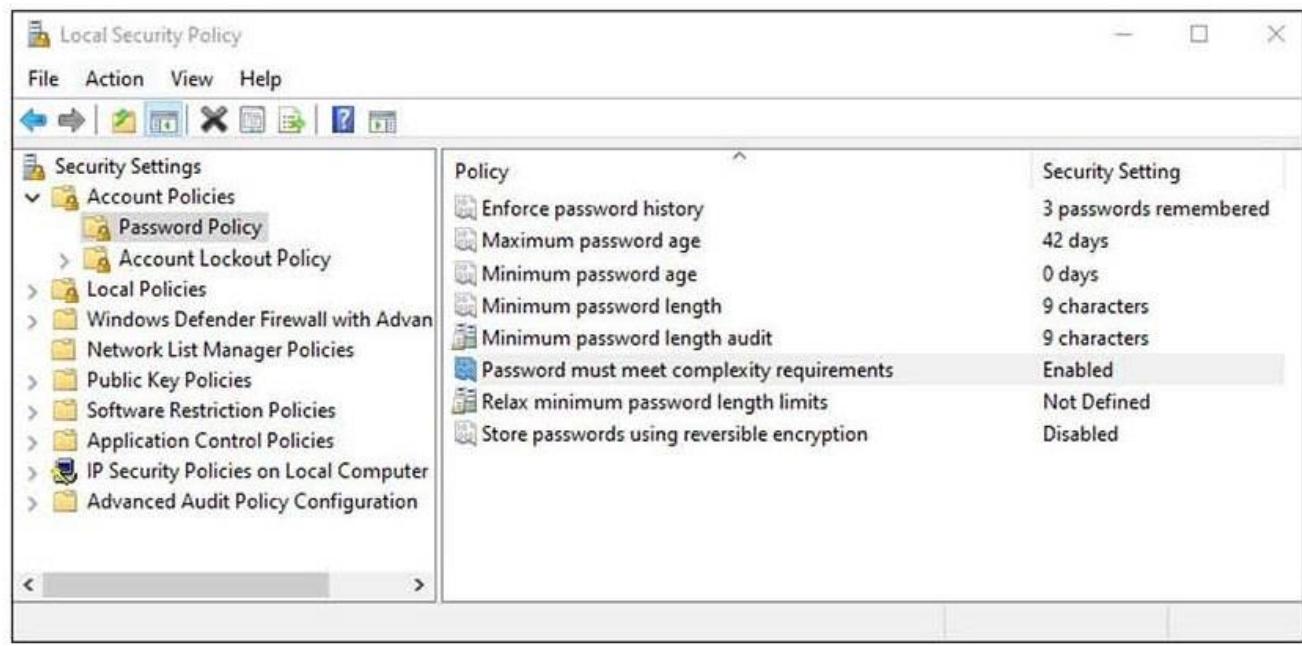
dựa vào một mình mật khẩu không còn đủ nữa. Đặc biệt, các công ty nên áp dụng các công cụ như đăng nhập một-lần (SSO) hoặc xác thực đa yếu tố (MFA), còn được gọi là xác thực hai-yếu-tố.

### Lịch sử của Mật khẩu

*Lịch sử mật khẩu* đề cập đến những mật khẩu trước đây đã từng được sử dụng bởi một tài khoản. Đây là một chính sách bảo mật tốt để ngăn chặn việc tái sử dụng mật khẩu, ít nhất cho một lượng các mật khẩu đã thiết lập. Trong Windows, trong Chính sách Bảo mật Cục bộ (trong các chính sách Nhóm Cục bộ), bạn có thể thiết lập ba yếu tố hoạt động cùng nhau để quản lý lịch sử của mật khẩu:

- **Hiệu lực của lịch sử mật khẩu** Nói cho hệ thống biết được bao nhiêu mật khẩu cần nhớ và không cho phép một người dùng sử dụng lại một mật khẩu cũ trong danh sách này.
- **Tuổi mật khẩu tối đa** Chỉ định số ngày tối đa mà một mật khẩu có thể được sử dụng trước khi nó có thể được thay đổi.
- **Tuổi mật khẩu tối thiểu** Chỉ định số ngày tối thiểu mà một mật khẩu phải được sử dụng trước khi nó có thể được thay đổi một lần nữa.

Tuổi mật khẩu tối thiểu là để ngăn việc người dùng thay đổi mật khẩu của họ 20 lần liên tiếp để quay lại mật khẩu trước đó hoặc mật khẩu hiện tại. Ví dụ về quản lý mật khẩu tài khoản trong Microsoft Windows được hiển thị trong Hình 23-1.



**Hình 23-1** Áp dụng các chính sách mật khẩu bằng GPO

### Tái sử dụng Mật khẩu

*Tái sử dụng mật khẩu* là một ý tưởng tồi ở chỗ nó mở ra khả năng tiếp xúc với kẻ thù, người đã lấy được mật khẩu trước đó. Hướng dẫn chính thức là mật khẩu không nên được sử dụng lại trong ít nhất một năm và cho ít nhất nửa tá thay đổi, tùy theo điều kiện nào đến sau. Trên thực tế, chúng ta không bao giờ nên sử dụng lại mật khẩu - cho một tài khoản hoặc giữa các tài khoản. Vì các vi phạm đã phát hành nhiều email và mật khẩu vào trong miền mở, mọi người đừng bao giờ kỳ vọng rằng các mật khẩu cũ sẽ được bảo mật. Việc áp dụng chính sách không tái sử dụng lại mật khẩu có ý nghĩa tốt từ khía cạnh rủi ro. Điều này là để giảm thiểu cơ hội cho kẻ thù lợi dụng trường hợp tái sử dụng. Như đã mô tả trong phần trước, bạn có thể hạn chế sử dụng lại mật khẩu trong Windows theo các chính sách nhóm cụbộ.



**MÁCH NƯỚC CHO KỲ THI** Các chính sách và thiết lập mật khẩu mạnh mẽ có thể giúp ngăn chặn những nỗ lực bẻ-khóa-mật-khẩu chẳng hạn như các cuộc tấn công kiểu brute force và từ điển.

### Thời gian trong Ngày

Việc tạo ra những giới hạn *thời-gian-trong-ngày* để truy cập có thể giải quyết được rất nhiều vấn đề về quản lý mật khẩu. Đối với phần lớn nhân viên làm việc theo ca, việc có được một hệ thống mà theo đó tài khoản của họ không hoạt động trong giờ không làm việc sẽ làm giảm bẽ mặt của tài khoản người dùng để cho những kẻ tấn công sử dụng. Điều này thậm chí còn quan trọng hơn đối với những người dùng có đặc quyền, vì tài khoản được nâng cao của họ có nguy cơ cao hơn và nếu người dùng được cấp phép của một tài khoản không hoạt động thì không có lý do gì để cấp phép cho tài khoản đó. Cũng như với mọi chính sách, cần có các điều khoản để thay đổi và cho các trường hợp khẩn cấp, theo đó người dùng được cấp phép có thể có quyền truy cập khi cần, ngay cả khi ngoài giờ làm việc bình thường.

Bạn có thể đặt ra giới hạn thời gian đăng nhập cho người dùng trong Windows bằng dấu nhắc lệnh quản trị với cú pháp sau:

```
net user <username> /time:<day>,<time>
```

Ngoài ra, trong một môi trường domain, bạn cũng có thể thiết lập những giới hạn giờ đăng nhập trong Active Directory thông qua Group Policy và Group Policy Objects (GPOs).

### Vị trí Mạng

Việc có được những hạn chế đối với các tài khoản dựa trên *vị trí mạng* có thể là một công cụ rất mạnh mẽ trong việc giới hạn các bẽ mặt tấn

công đối với các tài khoản đặc quyền. Việc cấm các kiểu truy cập cụ thể dựa trên vị trí trên mạng mà người dùng hiện đang được định vị tại đó sẽ ngăn chặn việc ai đó sử dụng thông tin đăng nhập của CFO từ tầng sản xuất hoặc người đứng đầu bộ phận nhân sự từ một ki-ốt ở sảnh. Mặc dù điều này đôi khi có thể ngăn cản người dùng hợp pháp thực hiện các hành động trong những trường hợp này, nhưng đây là một cái giá phải trả khá nhỏ cho việc bảo vệ toàn diện quyền truy cập tài khoản đặc quyền.

### **Hàng rào địa lý**

*Hàng rào địa lý* là việc sử dụng hệ thống định vị toàn cầu (GPS) và/hoặc công nghệ nhận dạng tần số vô tuyến (RFID) để tạo nên một hàng rào ảo xung quanh một vị trí cụ thể và phát hiện khi có thiết bị di động vượt qua hàng rào. Điều này cho phép những người khác nhận ra thiết bị, dựa trên vị trí, và thực hiện các hành động. Hàng rào địa lý được sử dụng trong tiếp thị để gửi thông điệp đến các thiết bị ở một khu vực cụ thể, chẳng hạn như gần điểm bán hàng hoặc chỉ để đếm lượng khách hàng tiềm năng. Hàng rào địa lý đã được sử dụng cho những người làm việc từ xa, thông báo cho ban quản lý khi họ đến địa điểm làm việc từ xa, cho phép những thứ như kết nối mạng được kích hoạt cho họ. Việc sử dụng hàng rào địa lý thực sự chỉ bị giới hạn bởi trí tưởng tượng của một người.

Có thể tắt tính năng định vị địa lý thông qua thiết bị. Trên các thiết bị của Apple, chỉ cần tắt Dịch vụ vị trí. Mặc dù để ngăn chặn hoàn toàn việc theo dõi thiết bị, bạn phải tắt radio bằng Chế độ trên máy bay.

### **Gắn nhãn địa lý**

Gắn nhãn địa lý là quá trình áp dụng các thẻ địa lý (thông tin về vị trí) cho một đề mục cụ thể. Các thẻ địa lý thực tế có thể có nhiều hình thức nhưng thường là một số dạng mã hóa của vĩ độ và kinh độ. Tất cả các loại dữ liệu kỹ thuật số đều có thể được gắn thẻ địa lý, bao gồm nhưng không giới hạn ở ảnh, video, trang web và các mục được đăng trên các

những trang mạng xã hội. Liên quan một cách chặt chẽ là khái niệm về mã hóa địa lý, đề cập đến việc sử dụng các phần tử siêu dữ liệu địa lý không dựa trên tọa độ, chẳng hạn như địa chỉ đường phố hoặc vị trí tòa nhà thực tế. Các yếu tố này kết hợp với nhau có thể cung cấp một mức độ tiện ích đáng kể cho các dịch vụ khác nhau, cho phép họ tùy chỉnh mọi thứ dựa trên vị trí của thiết bị, của dịch vụ hoặc người dùng.

Thẻ địa lý đã được sử dụng trong nhiều cuộc điều tra, vì rất nhiều ảnh có thông tin thẻ địa lý được nhúng trong siêu dữ liệu tại thời điểm chúng được tạo ra. Dữ liệu này có thể được đọc bằng các tiện ích đặc biệt có thể đọc các định dạng tập tin hình ảnh có thể trao đổi (exchangeable image file - EXIF) hoặc nền tảng siêu dữ liệu có thể mở rộng (extensible metadata platform - XMP).

### Vị trí địa lý

Hầu hết các thiết bị di động giờ đây đều có khả năng sử dụng GPS để theo dõi vị trí của thiết bị. Nhiều ứng dụng phụ thuộc rất nhiều vào vị trí GPS, chẳng hạn như các dịch vụ định-vị-thiết-bị, các ứng dụng bản đồ, ứng dụng giám-sát-lưu-lượng, và những ứng dụng định vị các doanh nghiệp lân cận như trạm xăng hoặc nhà hàng. Những công nghệ này có thể bị khai thác để theo dõi chuyển động và vị trí của thiết bị di động, vốn được gọi là "vị trí địa lý". Việc theo dõi này có thể được sử dụng để hỗ trợ việc khôi phục các thiết bị bị mất.



### MÁCH NƯỚC CHO KỲ THI

Hãy tìm hiểu sự khác biệt giữa hàng rào địa lý và vị trí địa lý. Chúng sẽ khiến cho bạn bị nhiễu khi lựa chọn đáp án trong đề thi.

## **Đăng nhập dựa-trên-Thời-gian**

*Đăng nhập dựa-trên-thời-gian* là việc triển khai xác thực dựa trên thời gian và việc triển khai đúng phương pháp này đòi hỏi các chính sách và thủ tục thích hợp. Việc thực hiện đăng nhập dựa-trên-thời-gian hoạt động đúng cách đòi hỏi phải tích hợp thông tin về vị trí cũng như thông tin về thời gian vào một hệ thống tích hợp có thể dẫn đến đảm bảo chi tiết và bảo mật cao về việc người dùng là chính họ. Loại trừ dựa-trên-thời-gian cũng hỗ trợ cho bảo mật và cho việc chặn sử dụng tài khoản ngoài giờ làm việc bình thường.

## **Các Chính sách Truy cập**

Các *chính sách truy cập* là một tập hợp các chính sách để hỗ trợ việc quản lý hệ thống kiểm soát truy cập. Từ các chính sách đơn giản bao gồm sử dụng mật khẩu, độ dài mật khẩu, hết hạn và khóa [tài khoản] cho đến các vấn đề phức tạp hơn như hết hạn, khôi phục và vô hiệu hóa tài khoản, tất cả những chỉ thị này đều cung cấp hướng dẫn cho nhân viên bảo mật để quản lý hệ thống truy cập.

*Chính sách mật khẩu* là cần thiết để bao gồm các chi tiết của các hạng mục như độ dài mật khẩu, độ phức tạp, tái sử dụng và lịch sử của mật khẩu. Độ dài và độ phức tạp của mật khẩu thường như là những mục tiêu ngày-càng-tăng, nhưng việc xác định chúng là điều quan trọng để ngăn mọi người sử dụng những mật khẩu đơn giản và dễ-bé-khóa. Việc có được một chính sách chính thức cấm chia sẻ mật khẩu hoặc đăng nhập vào tài khoản của người khác (ngay cả khi được phép) trông có vẻ dư thừa nhưng sẽ cần thiết khi chính sách này không được áp dụng và xảy ra sự cố. Việc sử dụng lại mật khẩu cho người dùng có cả tài khoản thông thường và tài khoản được gia tăng có thể là một vấn đề, nếu họ sử dụng cùng một mật khẩu cho cả hai tài khoản, liệu có thực sự an toàn không? Một lần nữa, một chính sách sẽ cung cấp hướng dẫn và các quy tắc thích hợp.

Tài khoản hết hạn nên xảy ra khi người dùng không còn được phép sử dụng hệ thống. Điều này đòi hỏi sự phối hợp giữa những người quản lý tài khoản và những người quản lý nhu cầu truy cập. Giải pháp tốt nhất là dành cho người quản lý của những người lao động yêu cầu quyền truy cập để quản lý nhu cầu - họ gần gũi với tình hình, hiểu được nhu cầu và nói chung là những người đầu tiên biết khi nào quyền truy cập không còn cần thiết nữa (ví dụ, khi một nhân viên chuyển công việc hoặc nghỉ việc).

Các nhà quản lý nên là những người đầu tiên thông báo cho nhóm bảo mật về bất kỳ thay đổi nào trong quyền hạn và nhân sự (HR) nên đóng vai trò dự phòng. Việc quản lý tiền tuyển bắt đầu các vấn đề về quyền cũng cho phép sự tiếp tục phù hợp về các quyền khi một người rời đi. Ai sẽ đảm nhận quyền sở hữu đối với các tập tin mà người [người rời đi] trước đó là chủ sở hữu duy nhất?



**MÁCH NƯỚC CHO KỲ THI** Trong Windows, hết hạn tài khoản người dùng là một tính năng tích-hợp cho phép bạn tạo ra một tài khoản người dùng tạm thời mà sẽ hết hạn sử dụng một cách tự động vào một ngày cụ thể. Khi đến ngày hết hạn, tài khoản người dùng sẽ bị hết hạn và người dùng sẽ không thể đăng nhập được vào Windows sau ngày đó. Điều này có thể tốt cho những nhân viên tạm thời và nhân viên hợp đồng.

*Khôi phục tài khoản* có vẻ như là một chủ đề bí truyền cho đến khi bạn mất mật khẩu trên máy tính xách tay của mình và không có cách nào quay lại được. Điều này thậm chí còn nghiêm trọng hơn nếu bạn làm mất mật khẩu tài khoản quản trị viên cho các thành phần chính trong cơ sở hạ tầng của mình. Có được một kế hoạch khôi phục tài khoản trong trường hợp có điều gì đó xảy ra với những người đã biết mật khẩu là điều rất quan trọng để doanh nghiệp tiếp tục hoạt động sau khi mất tài nguyên.

Thay vì tập trung vào tất cả các cách thức mà tổ chức có thể mất tài nguyên - bị sa thải, tự ý rời đi, bước lên trước xe buýt, v.v... - thay vào đó, hãy tập trung vào một phương pháp khôi phục đơn giản như một phong bì chứa danh sách các tài khoản và mật khẩu, được đặt trong một két an toàn được quản lý bởi một giám đốc điều hành cấp cao khác. Hệ thống cơ sở hạ tầng khóa công khai (PKI) có các cơ chế khôi phục khóa có lý do - được sử dụng khi những trường hợp khẩn cấp xảy ra. Khôi phục tài khoản cũng không khác gì: bạn cần phải có một kế hoạch và thực hiện nó để chuẩn bị cho trường hợp khẩn cấp khi bạn cần thực hiện kế hoạch đó. Bởi vì nếu bạn chờ đợi cho đến khi bạn cần một kế hoạch thì đã quá muộn để tạo ra nó.



**MÁCH NƯỚC CHO KỲ THI** Các tài khoản có rất nhiều khía cạnh phải được quản trị về cả hành động lẫn chính sách. Hãy nhớ, chính sách định hướng cho các hành động, và những chi tiết cụ thể của câu hỏi sẽ đưa ra bối cảnh mà theo đó, bạn có thể lựa chọn câu trả lời tốt nhất.

### Quyền hạn Tài khoản

Với chỉ một người dùng và một máy tính, quyền hạn sẽ rất đơn giản: bạn là quản trị viên và có thể truy cập mọi thứ. Nhưng với nhiều người dùng hơn, nhiều máy tính hơn, việc tính toán xem ai nêu có quyền gì đối với đối tượng nào là điều đã dẫn đến các chiến lược kiểm soát truy cập khác nhau được đề cập trong chương tiếp theo (Chương 24). Khi số lượng người dùng và đối tượng tăng lên, các phương pháp kiểm soát truy cập đơn giản trở nên khó quản lý nếu không có sự định hướng. Việc phát triển một chính sách về *quyền hạn tài khoản* chỉ cung cấp hướng dẫn đó cho những người đang triển khai các lược đồ kiểm soát truy cập. Chủ sở hữu dữ liệu có thể sẽ muốn xác định xem ai có quyền gì đối với dữ liệu của

họ, nhưng việc cố gắng cập nhật thông tin chi tiết trên cơ sở từng-tài-khoản là con đường dẫn đến thất bại. Điều này đã dẫn đến việc các nhóm, vai trò và quy tắc được sử dụng để quản lý chi tiết, nhưng tất cả chúng đều được định hướng bởi các chính sách.

Một ví dụ về một chính sách là người dùng đang đóng vai trò quản trị viên cơ sở dữ liệu được chỉ định cho một nhóm quản trị viên cơ sở dữ liệu, để tạo điều kiện quản lý dễ dàng hơn. Khi ở trong nhóm, quyền nhóm sẽ giải quyết chi tiết theo người dùng. Tương tự, quản trị viên hệ thống có thể được chỉ định vào một nhóm, để kiểm soát quyền của họ. Các quản trị viên hệ thống có thể có nhiều nhóm để từ đó, quản trị viên không thể truy cập nhật ký từ hệ thống mà họ có thể truy cập. Những hệ thống đó thuộc về một nhóm quản trị viên khác nhau. Một chính sách tốt có thể thực thi việc phân tách các nhiệm vụ cũng như quản lý chi tiết liên quan đến mức độ chi tiết của các quyền.

Sự khác biệt phổ biến của các loại người dùng là:

- **Quản trị viên** Một tài khoản quản trị viên có toàn quyền kiểm soát các tập tin, thư mục, dịch vụ và các tài nguyên khác trên máy tính cục bộ. Tài khoản quản trị viên có thể tạo ra những người dùng cục bộ khác, chỉ định quyền cho người dùng và phân quyền. Tài khoản quản trị viên có thể kiểm soát các tài nguyên cục bộ bất kỳ lúc nào đơn giản chỉ bằng cách thay đổi các quyền của người dùng. Trong hệ thống Linux, tài khoản root được sử dụng cho mục đích quản trị, trong khi trong Windows, tài khoản này được gọi là Quản trị viên (Administrator) hoặc Quản trị viên Cục bộ (Local Administrator).
- **Người dùng tiêu chuẩn** Các tài khoản tiêu chuẩn là tài khoản cơ bản mà bạn sử dụng cho các công việc bình thường hàng ngày. Là một người dùng thông thường, bạn có thể làm bất cứ điều gì bạn cần làm, chẳng hạn như chạy phần mềm và cá nhân hóa màn hình

của bạn. Người dùng tiêu chuẩn có thể bị hạn chế cài đặt các chương trình mới.

- **Khách** Tài khoản khách nên được vô hiệu hóa theo mặc định khi cài đặt. Tài khoản khách cho phép người dùng không thường xuyên hoặc người dùng một-lần không có tài khoản trên máy tính tạm thời đăng nhập vào máy chủ cục bộ hoặc máy khách với những quyền người dùng bị hạn chế. Tài khoản khách khiến cho việc ghi nhật ký và xác định người dùng trở nên bất khả thi.

Những hệ thống khác có thể có các nhóm người dùng khác, chẳng hạn như người dùng có quyền lực (power users) tồn tại ở khoảng giữa của người dùng và quản trị viên. Mỗi doanh nghiệp có thể tự mình đưa ra những quyết định này và thực thi thông qua các chính sách.

### **Kiểm toán Tài khoản**

*Kiểm toán tài khoản* cũng giống như mọi cuộc kiểm toán khác – chúng là một sự xác minh độc lập về việc rằng các chính sách tương ứng với các tài khoản đang được tuân thủ. Một kiểm toán viên độc lập có thể kiểm tra tất cả các yếu tố của chính sách. Mật khẩu có thể được kiểm tra bằng cách sử dụng trình bẻ khóa mật khẩu – nếu nó [trình bẻ khóa mật khẩu] bẻ khóa được một mật khẩu, nghĩa là đã có người dùng tuân theo các quy tắc. Những hạn chế khác, chẳng hạn như khóa tài khoản và tái sử dụng [mật khẩu] cũng có thể được kiểm tra. Một kiểm toán viên có thể xác minh rằng mọi người dùng đã được cấp phép vẫn đang là việc cho công ty hoặc đang hoạt động trong một phạm vi năng lực đã được cấp phép. Các cuộc kiểm toán hoạt động để đảm bảo việc triển khai các chính sách thực tế đang hoạt động theo những thông số đặc tả kỹ thuật.

### **Thời gian Di chuyển Bất khả thi/Rủi ro Đăng nhập**

Thông tin đăng nhập chính xác vào một tài khoản có thể ghi lại rất nhiều phần tử thông tin, bao gồm cả việc thông tin đăng nhập này đến từ vị trí

nào. "Vị trí" này có thể là một máy trong mạng hoặc thậm chí là một vị trí địa lý. Bằng cách sử dụng siêu dữ liệu này, một số đề mục thú vị có thể được tính toán. Nếu đăng nhập xảy ra từ một vị trí riêng biệt mà người dùng thực sự đã đăng nhập, liệu người dùng có thể ở hai vị trí cùng một lúc không? Tương tự, nếu lần đăng nhập thứ hai xảy ra từ một vị trí địa lý tách biệt, liệu có đủ thời gian để thực sự di chuyển xa đến mức này trong khoảng thời gian giữa các lần đăng nhập không? Đây là tất cả những trường hợp *rủi ro đăng nhập* hoặc ví dụ về *thời gian di chuyển bất khả thi*. Có những ứng dụng có thể phát hiện những điểm bất thường này và hiển thị thông tin này cho bạn để đưa ra quyết định có nên cho phép đăng nhập lần thứ hai hay không. Những gì sẽ chi phối những quyết định này là một chính sách giải quyết cụ thể những điều kiện này.

Các phần tử của chính sách không hề đơn giản, vì trong khi việc đăng nhập từ xa từ một lục địa ở xa có thể dễ bị từ chối, thì điều gì trong số hai phiên đăng nhập trong cùng một tòa nhà lại chồng chéo lên nhau? Có vi phạm chính sách không khi một hệ thống đăng nhập, khóa màn hình rồi chuyển sang một hệ thống khác? Trong một số trường hợp bảo-mật-cao, lần xuất hiện thứ hai này có thể sẽ bị chặn bởi chính sách, trong khi trong các trường hợp bảo mật kém hơn, khả năng sử dụng nhiều lần đăng nhập có thể sẽ được chấp thuận. Đây là lý do tại sao một chính sách là cần thiết - để điều phối sự quản lý trên tất cả các điều kiện khác nhau này, không để cho kỹ thuật viên bảo mật tùy ý quyết định khi họ thiết lập cấu hình cho các thiết bị và các hệ thống kiểm soát truy cập.

## **Lockout**

*Khóa (lockout)* tài khoản cũng giống như vô hiệu hóa, mặc dù khóa thường đề cập đến việc tạm thời chặn khả năng đăng nhập vào hệ thống của người dùng. Ví dụ, nếu người dùng nhập sai mật khẩu của họ một số lần

nhất định, họ có thể buộc phải đợi một khoảng thời gian nhất định trong khi tài khoản của họ bị khóa trước khi cõi găng đăng nhập lại. Các khóa này có thể được tự động hóa trên hầu hết các hệ thống và cung cấp một loạt các trở ngại về thời gian ngày càng gia tăng đối với kẻ tấn công, đồng thời giảm thiểu sự bất tiện cho người dùng hợp pháp gấp vần đề về thông tin xác thực. Người dùng có thể nhập sai mật khẩu của họ một vài lần, vì vậy, tệ nhất là một lần khóa tối thiểu sẽ xảy ra với một người dùng hợp pháp trong trường hợp hiếm hoi. Kẻ tấn công, khi thử một bộ mật khẩu có thể có, sẽ tấn công các khóa nhiều lần. Việc khóa tài khoản sau ba lần thử cho phép tỷ lệ lỗi hợp lý và cân bằng được rủi ro.



**MÁCH NƯỚC CHO KỲ THI** Một chính sách khóa tài khoản được sử dụng để vô hiệu hóa một tài khoản người dùng khi một mật khẩu sai được sử dụng trong một số lần [đăng nhập] đã được xác định trong một khoảng thời gian nhất định. Điều này đặc biệt hữu ích để làm chậm những nỗ lực cưỡng bức khi bẻ khóa một mật khẩu.

### Vô hiệu hóa

*Vô hiệu hóa* tài khoản là một bước nằm giữa tài khoản đang có quyền truy cập và tài khoản đã bị xóa khỏi hệ thống. Bất cứ khi nào một nhân viên rời khỏi công ty, tất cả các tài khoản tương ứng [với nhân viên đó] phải được vô hiệu hóa để ngăn việc nhân-viên-cũ tiếp tục truy cập. Việc vô hiệu hóa được ưu tiên hơn là xóa, vì việc xóa có thể dẫn đến các vấn đề về quyền và quyền sở hữu. Việc xóa bỏ tài khoản có thể làm mất đi các hạng mục còn lại mà không có các hình thức sở hữu khác, khiến cho việc chia sẻ các tập tin của nhân viên cũ trở nên khó khăn hơn. Kiểm tra định kỳ tài khoản người dùng để đảm bảo họ vẫn còn cần quyền truy cập cũng là một biện pháp bảo mật tốt. Việc vô hiệu hóa tài khoản có thể

hoàn nguyên được, nhưng nó sẽ cấm tài khoản đó được sử dụng cho đến khi vẫn đề dẫn đến việc vô hiệu hóa được giải quyết. Vô hiệu hóa tài khoản có thể là một phản ứng tự động từ hệ thống bảo mật nếu hệ thống phát hiện thấy tài khoản đang bị tấn công (giả sử như đoán mật khẩu kiểu brute force).

---



**MÁCH NƯỚC CHO KỲ THI** Các tài khoản có rất nhiều khía cạnh được quản trị bởi cả hành động lẫn chính sách. Hãy nhớ rằng chính sách định hướng cho các hành động, và những chi tiết cụ thể trong câu hỏi sẽ đặt ra bối cảnh mà theo đó, bạn có thể chọn đáp án tốt nhất. Có rất nhiều chi tiết trong phần này, và tất cả đều có thể kiểm tra được theo cách này.

## Tóm tắt Chương

Chương này mở đầu bằng việc xem xét các khái niệm xung quanh danh tính để quản lý tài khoản và kiểm soát truy cập. Trong phần đầu tiên, các chủ đề về nhà cung cấp danh tính (IdP), thuộc tính, chứng nhận và mã thông báo đã được trình bày. Phần này kết thúc với khóa SSH và thẻ thông minh. Phần tiếp theo đã xem xét các loại tài khoản khác nhau, bao gồm tài khoản người dùng, tài khoản/thông tin đăng nhập được chia sẻ và sử dụng chung, tài khoản khách và tài khoản dịch vụ.

Phần lớn của chương được hình thành xoay quanh các chính sách tài khoản. Phần này bắt đầu với các chính sách liên quan đến mật khẩu: độ phức tạp của mật khẩu, lịch sử và việc tái sử dụng mật khẩu. Các chủ đề tiếp theo là chính sách thời-gian-trong-ngày. Các chính sách liên-quan-đến-vị-trí, bao gồm vị trí mạng, hàng rào địa lý, gắn thẻ và định vị địa lý, sẽ được đề cập tiếp theo. Thông tin đăng nhập dựa-trên-thời-gian cũng được giải thích, tiếp theo đó là các chính sách tài khoản nói chung bao gồm các chính sách truy cập, quyền tài khoản và kiểm toán tài khoản.

Chương này kết thúc bằng việc xem xét các vấn đề về thời gian di chuyển bất khả thi/các vấn đề rủi ro khi đăng nhập, tiếp theo là các chính sách về khóa và vô hiệu hóa [tài khoản].

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Một người bạn của bạn đang làm việc trong bộ phận CNTT của một ngân hàng nói với bạn rằng nhân viên thu ngân [của ngân hàng] được phép đăng nhập vào máy trạm đầu cuối của họ trong khoảng thời gian từ 9 giờ sáng đến 5 giờ chiều, từ thứ Hai đến thứ Bảy. Hạn chế này là một ví dụ của?

  - A. Kiểm toán người dùng
  - B. Ít đặc quyền nhất
  - C. Hạn chế thời-gian-trong-ngày
  - D. Xác minh tài khoản.
2. Tổ chức của bạn đang sửa đổi các chính sách quản lý tài khoản của mình và bạn đã được yêu cầu làm rõ sự khác biệt giữa việc vô hiệu hóa tài khoản và khóa tài khoản. Mệnh đề nào dưới đây mô tả đúng nhất sự khác biệt đó?

  - A. Việc vô hiệu hóa tài khoản sẽ xóa người dùng và tất cả các tập tin dữ liệu của họ, không khóa tài khoản.
  - B. Việc khóa tài khoản thường chỉ ảnh hưởng đến khả năng đăng nhập, vô hiệu hóa tài khoản sẽ xóa tất cả các đặc quyền.
  - C. Khóa tài khoản là vĩnh viễn, vô hiệu hóa tài khoản có thể dễ dàng đảo ngược.
  - D. Việc vô hiệu hóa tài khoản yêu cầu các đặc quyền quản trị để thực thi, khóa tài khoản có thể được thực hiện bởi bất kỳ người dùng nào.
3. Chính sách mật khẩu là cần thiết cho tất cả những điều dưới đây ngoại trừ?

- A. Độ phức tạp của mật khẩu**
- B. Lịch sử mật khẩu**
- C. Tái sử dụng mật khẩu**
- D. Ngôn ngữ mật khẩu.**
- 4.** Điều nào dưới đây được sử dụng để xác định khi một thiết bị đang nằm trong một khoảng cách xác định của một vị trí?
- A. Hàng rào địa lý**
- B. Lân cận về địa lý**
- C. Khoảng cách địa lý**
- D. Gắn thẻ địa lý.**
- 5.** Kiểm toán tài khoản được sử dụng cho tất cả những điều sau đây ngoại trừ?
- A. Kiểm tra độ mạnh của mật khẩu**
- B. Xác minh đào tạo người dùng**
- C. Xác minh công việc/Ủy quyền của người dùng**
- D. Kiểm tra việc thực thi chính sách mật khẩu**
- 6.** Điều nào sau đây thể hiện rủi ro lớn nhất khi được sử dụng?
- A. Các tài khoản dịch vụ**
- B. Các tài khoản người dùng**
- C. Các tài khoản khách**
- D. Các tài khoản được chia sẻ.**
- 7.** Khi một yêu cầu đăng nhập mới đến từ một vị trí địa lý xa xôi, đối với người dùng có lịch sử đăng nhập cục bộ gần đây, chính sách nào có thể giúp xác định tính hợp pháp tốt nhất?
- A. Thời gian di chuyển bất khả thi**
- B. Vị trí địa lý**
- C. Vị trí mạng**
- D. Giới hạn thời-gian-trong-ngày**

8. Bạn muốn mã hóa thông tin đăng nhập tài khoản để mọi người có thể mang theo mật khẩu của họ và không phải nhớ hoặc nhập mật khẩu quá dài. Giải pháp tốt nhất sẽ liên quan đến điều nào sau đây?

  - A. Nhà cung cấp danh tính (IdP)
  - B. Các khóa SSH
  - C. Thẻ thông minh
  - D. Trình quản lý mật khẩu
9. Trên giao diện trực diện web, nơi nhân viên của bạn có thể có được quyền truy cập vào mạng, bạn muốn triển khai bảo mật để chống lại các cuộc tấn công kiểu brute force. Một trong những công cụ hiệu-quả-về-chi-phí nhất là thực thi điều nào sau đây?

  - A. Chính sách hàng rào địa lý
  - B. Chính sách về độ phức tạp của mật khẩu
  - C. Chính sách khóa tài khoản
  - D. Giấy chứng nhận
10. Loại chính sách nào đặt ra định hướng cho nhóm bảo mật để quản lý những người có thể truy cập những tài nguyên nào trong hệ thống?

  - A. Chính sách cấp quyền hạn cho tài khoản
  - B. Chính sách đăng nhập dựa-trên-thời-gian
  - C. Chính sách mật khẩu
  - D. Chính sách giới hạn thời-gian-trong-ngày.

## Đáp án

1. **C.** Giới hạn thời-gian-trong-ngày thường được sử dụng để giới hạn số giờ người dùng được phép đăng nhập hoặc truy cập hệ thống. Điều này giúp ngăn chặn việc truy cập trái phép ngoài giờ làm việc bình thường của người dùng đó.
2. **B.** Vô hiệu hóa tài khoản là một bước gỡ bỏ hoàn toàn một tài khoản. Trong khi tài khoản (và các tập tin dữ liệu tương ứng) vẫn tồn tại trên hệ thống thì bản thân tài khoản đó đã bị vô hiệu hóa và không có đặc quyền truy cập vào hệ thống. Việc khóa tài khoản thường chỉ ảnh hưởng đến đặc quyền đăng nhập. Thực hiện khóa tài khoản tạm thời là một cách tiếp cận phổ biến để ngăn chặn các cuộc tấn công đoán mật khẩu kiểu brute force.
3. **D.** Ngôn ngữ được sử dụng để tạo ra mật khẩu không phải là một vấn đề, đặc biệt là khi hầu hết các mật khẩu lý tưởng là các chuỗi ký tự ngẫu nhiên.
4. **A.** Hàng rào địa lý là một chu vi dựa-trên-khoảng-cách điện tử được sử dụng để phát hiện các thiết bị cụ thể khi chúng vượt qua phạm vi một khu vực địa lý nhất định.
5. **B.** Việc đào tạo người dùng sẽ không được kiểm tra trong quá trình kiểm toán tài khoản. Kiểm toán tài khoản tập trung vào các chính sách và triển khai hệ thống xác thực.
6. **D.** Tài khoản được chia sẻ là rủi ro lớn nhất vì bạn không biết ai đang sử dụng chúng.
7. **A.** Khi nhận được yêu cầu truy cập tài khoản tiếp theo và không có đủ thời gian để người dùng chuyển đến địa điểm mới, đó có thể là một nỗ lực gian lận.
8. **C.** Thẻ thông minh cho phép nhân viên dễ dàng mang theo các khóa mật mã.

- 9. C.** Khóa tài khoản là một biện pháp tạm thời để làm chậm những nỗ lực bẻ khóa mật khẩu theo kiểu thô bạo (brute force).
- 10. A.** Việc phát triển một chính sách quyền hạn của tài khoản cung cấp định hướng cho những người đang triển khai các lược đồ kiểm soát truy cập.

## Chương 24 Triển khai Xác thực và Cấp phép

### Triển khai Xác thực và Cấp phép

Trong chương này bạn sẽ

- Xem xét những khái niệm về quản lý xác thực,
- Khám phá những phương pháp xác thực khác nhau,
- Xem xét những lược đồ kiểm soát truy cập khác nhau.

Xác thực và cấp phép là những yếu tố quan trọng để kiểm soát ai đã truy cập vào các hệ thống và tài nguyên máy tính. Các nguyên tắc kiểm soát truy cập và xác thực đúng đắn áp dụng cho cả truy cập nội bộ và truy cập từ xa. Các yêu cầu đối với truy cập từ xa nghiêm ngặt hơn, tuy nhiên các nguyên tắc tương tự có thể được áp dụng cho truy cập trong nội bộ.

Các cơ chế kiểm soát truy cập hoạt động cùng với các tài khoản và chính sách tài khoản để xác định mức độ truy cập thích hợp cho người dùng trên các hệ thống. Chương này sẽ xem xét quản lý xác thực, các phương pháp xác thực và các lược đồ kiểm soát truy cập.

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 3.8 của kỳ thi CompTIA Security+: Đưa ra một kịch bản, triển khai các giải pháp xác thực và cấp phép.

## Quản lý Xác thực

Xác thực là một trong những yếu tố nền tảng của việc xác lập và duy trì tính bảo mật. Quản lý xác thực đạt được thông qua sự kết hợp các yếu tố phần cứng và phần mềm, bao gồm mật khẩu, khóa mật khẩu, mái vòm (vault), Mô-đun Nền tảng Đáng tin cậy (TPM) và các giải pháp mô-đun bảo mật phần cứng, cũng như là các phương pháp xác thực thay thế chặng hạn như các hệ thống dựa-trên-kiến-thức.

## Các Khóa Mật khẩu

Mật khẩu đại diện cho một bí mật giữa một người dùng và một hệ thống xác thực. Một trong những thách thức trong việc duy trì mật khẩu là có một hệ thống lưu giữ mật khẩu đối với người dùng, như là một bí mật, và thực hiện việc này một cách an toàn. Phương pháp thông thường bao gồm việc quản lý nhóm chứa các mật khẩu chung thông qua giải pháp quản lý mật khẩu, và giải pháp này sẽ mã hóa mật khẩu bằng một khóa. *Khóa mật khẩu* này đại diện cho đường dẫn truy cập vào mật khẩu và thay đổi vô số mật khẩu khác nhau, có thể là duy nhất cho mọi trang web hoặc mục đích sử dụng, thành một bí mật duy nhất được đại diện bởi khóa mật khẩu. Người dùng duy trì bí mật của khóa mật khẩu và trình quản lý mật khẩu quản lý các mật khẩu khác.

## Kho chứa Mật khẩu (Password vaults)

*Kho chứa mật khẩu* là các cơ chế phần mềm được thiết kế để quản lý vấn đề người dùng có nhiều mật khẩu cho vô số hệ thống khác nhau. Kho chứa cung cấp một phương tiện lưu trữ mật khẩu cho đến khi chúng được cần đến và nhiều chương trình quản lý mật khẩu có các chức năng bổ sung như tạo mật khẩu và xử lý mật khẩu thông qua trình duyệt. Các kho chứa thể hiện một điểm thắt bại duy nhất là nếu kẻ tấn công lấy được khóa mật khẩu hoặc mật khẩu chính, chúng sẽ có quyền truy cập vào tất cả mật khẩu khác của người dùng. Các biện pháp bảo vệ bằng mật mã sẽ khắc phục được điều này, nhưng nó cũng gây ra một vấn đề khác với

vault - phải làm gì khi người dùng mất mật khẩu chính của họ? Bất kỳ cơ chế khôi phục nào cũng sẽ gây ra rủi ro lớn cho hệ thống, vì vậy trong hầu hết các hệ thống, người dùng có trách nhiệm duy trì thông tin này ở một nơi khác như một bản sao lưu.

Một dạng khác của kho chứa mật khẩu là các hệ thống được tích hợp sẵn trong phần mềm và hệ điều hành (OS) để lưu giữ thông tin đăng nhập một cách an toàn. Ví dụ về những kho chứa dạng này là Chuỗi khóa (Keychain) trong macOS và iOS và Trình quản lý thông tin Xác thực (Credential Manager) trong Microsoft Windows. Việc sử dụng lưu trữ mật khẩu dựa-trên-trình-duyệt kém an toàn hơn nhiều, vì có rất nhiều tiện ích có thể lấy mật khẩu ra khỏi hầu hết chúng, khiến cho các giải pháp này trở nên kém an toàn hơn và trở thành mục tiêu rõ ràng cho những kẻ tấn công. Các giải pháp Keychain và Credential Manager dựa trên hệ điều hành mạnh mẽ hơn nhiều và có thể hạn chế rủi ro tổng thể.

## TPM

*Mô-đun Nền tảng Đáng tin cậy (Trusted Platform Module – TPM)* là một giải pháp phần cứng trên bo mạch chủ, một giải pháp hỗ trợ việc tạo ra và lưu trữ các khóa cũng như tạo ra các số ngẫu nhiên. Khi các khóa mã hóa được lưu trữ trong TPM, chúng là không thể truy cập được thông qua các kênh phần mềm và tách biệt về mặt vật lý với ổ cứng hoặc và vị trí dữ liệu được mã hóa khác. Điều này khiến cho TPM là một giải pháp an toàn hơn so với việc giữ các khóa trong bộ lưu trữ bình thường của máy tính.



## MÁCH NƯỚC CHO KỲ THI

Một TPM hoạt động như một bộ xử lý mã hóa an toàn. Nó là một giải pháp phần cứng hỗ trợ việc tạo ra và bảo vệ các khóa, bộ lưu trữ được mã hóa.

## HSM

Một *mô-đun bảo mật phần cứng* (*harward security module* – HSM) là một thiết bị được sử dụng để quản lý hoặc lưu trữ các khóa mã hóa. Nó cũng có thể hỗ trợ cho các hoạt động mật mã như mã hóa, băm hoặc áp dụng chữ ký điện tử. HSM thường là các thiết bị ngoại vi được kết nối qua cổng USB hoặc kết nối mạng. HSM có cơ chế bảo-vệ-chống-giả-mạo để ngăn chặn việc truy cập vật lý vào những bí mật mà chúng bảo vệ. Do được thiết kế chuyên dụng, chúng có thể mang lại những lợi thế đáng kể về hiệu suất so với các máy tính đa-năng khi nói đến các hoạt động mật mã. Khi một doanh nghiệp có các mức hoạt động mật mã đáng kể, HSM có thể mang lại tính hiệu quả về thông lượng.



## MÁCH NƯỚC CHO KỲ THI

Việc lưu giữ các khóa ở bất kỳ đâu trên một hệ thống được nối mạng là một công thức dẫn đến tổn thất. HSM được thiết kế để cho phép sử dụng các khóa mà không tiết lộ chúng cho một loạt các mối đe dọa dựa-trên-máy-vật-chủ.

## Xác thực dựa-trên-Kiến-thức

Xác thực dựa-trên-kiến-thức là một phương pháp trong đó danh tính của một người dùng được xác minh thông qua một tập hợp kiến thức chung. Đây là một phương pháp rất hữu ích để xác minh danh tính của một người dùng mà không cần phải lưu trữ trước bí mật. Phương pháp luận tiêu chuẩn liên quan đến xác thực là danh tính và bí mật chung đã từng được ghi lại trước đây trong hệ thống, tùy thuộc vào việc sử dụng sau đó được xác minh bằng cách thu hồi một phần từ phía người dùng và được tra cứu bởi hệ thống cứu. Tuy nhiên, điều gì sẽ xảy ra nếu người dùng chưa bao giờ truy cập trang web để thiết lập danh tính của họ? Có thể nói, làm thế nào để nó có thể được thiết lập một cách nhanh chóng? Xác thực dựa-trên-kiến-thức dựa trên một tập hợp kiến thức, mặc dù nó có thể có sẵn

cho rất nhiều người, nhưng từ một tập hợp thông tin khổng lồ đến nỗi việc thu hồi sẽ chỉ hoạt động cho chính người dùng.

Một ví dụ điển hình là khi truy cập một trang web, chẳng hạn như văn phòng tín dụng, để lấy thông tin về chính bạn. Trang web có một lượng lớn kiến thức liên quan đến bạn và nó có thể xem liệu bạn có thể xác định được một địa chỉ bạn đã từng sống hay không (trong danh sách bốn địa chỉ), chiếc xe bạn đã sở hữu (trong danh sách bốn chiếc xe), một chiếc ô tô hoặc số tiền thanh toán thẻ chấp, hoặc một tài khoản thẻ tín dụng. Trong một bài kiểm tra được tính thời gian, để loại bỏ các tra cứu mở rộng, người dùng được cung cấp một loạt các tùy chọn trắc-nghiệm. Nếu tất cả đều đúng, thì khả năng cao là họ chính là người mà họ đại diện cho chính mình. Lần cuối cùng tác giả trải qua một trong những bài kiểm tra này, phạm vi thời gian cho kiến thức được bao phủ là hơn 20 năm, khiến cho phạm vi kiến thức để lựa chọn thực sự lớn.

## Xác thực

Các giao thức *xác thực* là những phương pháp được tiêu chuẩn hóa được sử dụng để cung cấp các dịch vụ xác thực, và trong trường hợp các mạng không dây, những phương pháp [xác thực] này được cung cấp từ xa. Các mạng không dây có nhu cầu đối với các giao thức xác thực bảo mật. Những phần dưới đây để cập đến một số giao thức và phương pháp xác thực chính được sử dụng ngày nay.

## EAP

*Giao thức Xác thực Có thể mở rộng (EAP)* là một giao thức dành cho mạng không dây mở rộng trên các phương pháp xác thực được sử dụng bởi Giao thức Điểm-đến-Điểm (PPP). PPP là một giao thức thường được sử dụng để kết nối trực tiếp các thiết bị với nhau. EAP được thiết kế để hỗ trợ nhiều cơ chế xác thực, bao gồm mã thông báo, thẻ thông minh, chứng nhận, mật khẩu một-lần và xác thực mã hóa công khai. EAP đã được mở

rộng thành nhiều phiên bản, một vài trong số các phiên bản sẽ được đề cập trong các phần sau. EAP được định nghĩa trong RFC 2284 (đã lỗi thời bởi 3748).

PEAP, hay *EAP Được bảo vệ (Protected EAP)*, được phát triển để bảo vệ giao tiếp EAP bằng cách đóng gói nó với Bảo mật Lớp Truyền tải (TLS). Đây là một tiêu chuẩn mở do Cisco, Microsoft và RSA cùng phát triển. EAP được thiết kế với giả định rằng đây là một kênh giao tiếp an toàn. PEAP cung cấp sự bảo vệ đó như một phần của giao thức thông qua đường hầm TLS. PEAP được các nhà cung cấp hỗ trợ rộng rãi để sử dụng qua mạng không dây.

Wi-Fi Alliance đã thêm EAP-FAST vào danh sách bao gồm các giao thức được hỗ trợ dành cho WPA/WPA2 của mình vào năm 2010 và WPA3 vào năm 2018. *EAP-FAST (Xác thực Linh hoạt EAP qua Đường hầm Bảo mật – EAP Flexible Authentication via Secure Tunneling)* được mô tả trong RFC 4851 và được Cisco đề xuất thay thế cho LEAP, một phiên bản EAP của Cisco trước đây. Nó cung cấp một giao thức đường hầm hạng nhẹ để hỗ trợ cho xác thực. Đặc điểm phân biệt là việc chuyển thông tin xác thực truy cập được bảo vệ (Protected Access Credential - PAC) được sử dụng để thiết lập đường hầm TLS qua đó thông tin xác thực của khách hàng được xác minh. Wi-Fi Alliance cũng đã thêm EAP-TLS vào danh sách các giao thức được hỗ trợ dành cho cho WPA/WPA2 vào năm 2010 và WPA3 đã được thêm vào năm 2018. EAP-TLS là một tiêu chuẩn mở IETF (RFC 5216) sử dụng giao thức TLS để bảo mật quá trình xác thực. EAP-TLS dựa trên TLS, một nỗ lực chuẩn hóa cấu trúc SSL để chuyển thông tin đăng nhập. Đây vẫn được coi là một trong những triển khai an toàn nhất, chủ yếu vì các triển khai phổ biến chỉ sử dụng chứng chỉ phía máy khách. Điều này có nghĩa là kẻ tấn công cũng phải sở hữu khóa cho chứng chỉ phía máy khách để phá vỡ kênh TLS.

Wi-Fi Alliance cũng đã bổ sung EAP-TTLS vào danh sách được hỗ trợ của mình dành cho WPA/WPA2 vào năm 2010, WPA3 vào năm 2018. EAP-TTLS (từ viết tắt của giao thức TLS Đường hầm-EAP) là một biến thể của giao thức EAP-TLS. EAP-TTLS hoạt động theo cách thức giống như EAP-TLS, với máy chủ xác thực cho máy khách bằng một chứng chỉ, nhưng giao thức tạo đường hầm phía máy khách của xác thực, cho phép sử dụng các giao thức xác thực cũ nhu Giao thức Xác thực Mật khẩu (PAP), Giao thức Xác thực Bắt-tay-Thách thức (CHAP), MS-CHAP, MS-CHAP-V2. Trong EAP-TTLS, tiến trình xác thực được bảo vệ bởi đường hầm khỏi các cuộc tấn công người-trung-gian, và mặc dù các chứng chỉ phía-máy-khách có thể được sử dụng nhưng không nhất thiết phải có, điều này khiến cho việc thiết lập trở nên dễ dàng hơn so với EAP-TLS cho các máy khách không có chứng chỉ.



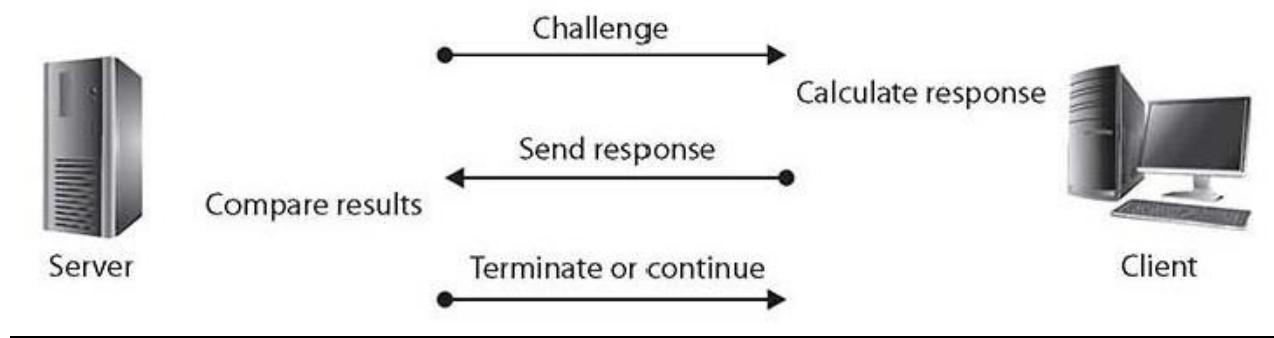
**LƯU Ý** WPA3 được phát hành bởi Wi-Fi Alliance vào năm 2018, và nó đã đặc biệt được thiết kế để giải quyết những điểm yếu trong WPA2, trong khi vẫn hỗ trợ cho các phương pháp khác. Theo thông số kỹ thuật WPA3, một trạm WPA3 sẽ thực hiện việc xác minh chứng chỉ máy chủ khi sử dụng các phương pháp EAP-TTLS, EAP-TLS, EAP-FEAPv0 hoặc EAP-FEAPv1 EAP.



**MÁCH NƯỚC CHO KỲ THI** Có hai thành phần then chốt liên quan đến EAP. Đầu tiên, nó chỉ là một khuôn khổ để bảo mật quá trình xác thực. Thứ hai, nó có thể hỗ trợ cho nhiều phương pháp khác và bản thân nó không phải là một phương pháp mã hóa thực tế.

## Giao thức Xác thực Bắt-tay-Thách-thức (CHAP)

*Giao thức Xác thực Bắt-tay-Thách-thức (CHAP)* được sử dụng để cung cấp sự xác thực qua một liên kết điểm-đến-điểm bằng cách sử dụng PPP. Trong giao thức này, xác thực sau khi liên kết đã được thiết lập là không bắt buộc. CHAP được thiết kế để cung cấp xác thực định kỳ thông qua việc sử dụng hệ thống thử thách/phản hồi đôi khi được mô tả như một kiểu bắt tay ba bước, như được minh họa trong Hình 24-1. Thủ thách ban đầu (một số được tạo ngẫu nhiên) được gửi cho máy khách. Máy khách sử dụng hàm băm một chiều để tính toán phản hồi nên là gì và sau đó gửi phản hồi này trở lại. Máy chủ so sánh phản hồi với những gì nó tính toán phản hồi phải như thế nào. Nếu chúng khớp, giao tiếp sẽ tiếp tục. Nếu hai giá trị không khớp thì kết nối sẽ bị ngắt. Cơ chế này dựa trên bí mật được chia sẻ giữa hai thực thể để có thể tính toán được các giá trị chính xác.



**Hình 24-1** Trình tự thách thức/phản hồi CHAP



**MÁCH NƯỚC CHO KỲ THI**  
năng:

CHAP sử dụng PPP, vốn hỗ trợ cho 3 chức

- Đóng gói các lược đồ dữ liệu qua các liên kết nối tiếp,

- Thiết lập, cấu hình và kiểm tra các liên kết bằng cách sử dụng LCP (Giao thức Kiểm soát Liên kết – Link Control Protocol),
- Thiết lập và cấu hình các giao thức mạng khác nhau bằng cách sử dụng NCP (Giao thức Kiểm soát Mạng – Network Control Protocol).

PPP hỗ trợ 2 giao thức xác thực:

- Giao thức Xác thực Mật khẩu (Password Authentication Protocol),
- Giao thức Xác thực Bắt-tay-Thách-thức.

### **Giao thức Xác thực Mật khẩu (PAP)**

Xác thực *Giao thức Xác thực Mật khẩu (PAP)* liên quan đến một quá trình bắt tay hai-chiều, trong đó tên người dùng và mật khẩu được gửi qua liên kết dưới dạng văn bản rõ ràng. Xác thực PAP không cung cấp bất kỳ sự bảo vệ nào để chống lại các cuộc tấn công phát lại và do thám tuyến đường. Giờ đây, PAP đã là một tiêu chuẩn không còn được sử dụng nữa.



### **MÁCH NƯỚC CHO KỲ THI**

PAP là một giao thức xác thực dạng văn bản rõ ràng và do đó là đối tượng của các cuộc tấn công đánh chặn. CHAP sử dụng giao thức bắt tay thử thách để bảo vệ kênh giao tiếp.

### **802.1X**

802.1X là một tiêu chuẩn để hỗ trợ cho các dịch vụ xác thực dựa-trên-cổng giữa một người dùng và một thiết bị xác thực, chẳng hạn như một bộ định tuyến biên. 802.1X thường được sử dụng trong các điểm truy cập không dây như một dịch vụ xác thực dựa-trên-cổng trước khi đi vào mạng không dây. 802.1X qua mạng không dây sử dụng 802.11i hoặc một giao thức dựa-trên-EAP, chẳng hạn như EAP-TLS hoặc PEAP-TLS.

## RADIUS

Dịch vụ *Người dùng Quay số Xác thực Từ xa (RADIUS)* là một giao thức được phát triển như một giao thức AAA. Nó đã được đệ trình lên IETF dưới dạng một loạt các RFC: RFC 2058 (đặc tả RADIUS), RFC 2059 (tiêu chuẩn tính toán RADIUS) và các RFC cập nhật 2865 – 2869 và 3579 hiện là các giao thức tiêu chuẩn. Nhóm Công tác IETF AAA đã đề xuất các phần mở rộng dành cho RADIUS (RFC 2882) và một giao thức thay thế được gọi là Đường kính (Diameter) (RFC 7075).

RADIUS được thiết kế như một giao thức không kết nối sử dụng Giao thức Sơ đồ dữ liệu Người dùng (UDP) làm giao thức cấp-độ-truyền-tải của nó. Các vấn đề về kiểu-kết-nối, chặng hạn như thời gian chờ, được xử lý bởi ứng dụng RADIUS thay vì lớp truyền tải. RADIUS sử dụng cổng UDP 1812 để xác thực và cấp phép và 1813 cho các chức năng tính toán.

RADIUS là một giao thức máy khách/máy chủ. Máy khách RADIUS thường là một máy chủ truy cập mạng (network access server - NAS). Máy chủ RADIUS là một tiến trình hoặc daemon chạy trên máy Linux hoặc Windows Server. Giao tiếp giữa máy khách RADIUS và máy chủ RADIUS được mã hóa bằng cách sử dụng bí mật chia sẻ được định cấu hình thủ công vào từng thực thể và không được chia sẻ qua kết nối. Do đó, giao tiếp giữa máy khách RADIUS (thường là NAS) và máy chủ RADIUS được bảo mật, nhưng giao tiếp giữa người dùng (thường là máy tính cá nhân) và máy khách RADIUS có thể bị xâm phạm. Đây là điều quan trọng cần phải được lưu ý là vì nếu máy của người dùng (máy tính cá nhân) không phải là máy khách RADIUS (NAS) thì giao tiếp giữa máy tính cá nhân và NAS thường không được mã hóa và được truyền dưới dạng [văb bản] rõ ràng.



**MÁCH NƯỚC CHO KỲ THI** Bằng cách sử dụng truyền tải UDP đến một máy chủ truy cập mạng tập trung, RADIUS cung cấp cho các hệ thống máy khách sự xác thực và kiểm soát truy cập trong phạm vi một mạng doanh nghiệp.

### **Đăng nhập Một lần (SSO)**

*Đăng nhập một-lần (SSO)* là một hình thức xác thực liên quan đến việc chuyển thông tin xác thực giữa các hệ thống. Khi ngày càng có nhiều hệ thống được kết hợp trong việc sử dụng hàng ngày, người dùng buộc phải có nhiều bộ thông tin đăng nhập. Người dùng có thể phải đăng nhập vào 3, 4, 5, hoặc thậm chí nhiều hệ thống hơn mỗi ngày chỉ để thực hiện công việc của mình. Đăng nhập một lần cho phép một người dùng chuyển thông tin đăng nhập của cô ấy để từ đó, việc đăng nhập vào một hệ thống sẽ giúp cô ấy đăng nhập vào tất cả các hệ thống. Điều này có ưu điểm là giảm bớt sự phức tạp khi đăng nhập đối với người dùng. Nó cũng có nhược điểm là khi kết hợp các hệ thống xác thực theo cách như vậy, nếu một thông tin đăng nhập bị xâm phạm, thì tất cả thông tin đăng nhập của người dùng sẽ bị xâm phạm.

### **Ngôn ngữ Đánh dấu Khẳng định Bảo mật (SAML)**

*Ngôn ngữ Đánh dấu Khẳng định Bảo mật (SAML)* là khả năng đăng nhập một lần được sử dụng cho các ứng dụng web để đảm bảo danh tính người dùng có thể được chia sẻ và được bảo vệ. Nó xác định các tiêu chuẩn dành cho việc trao đổi dữ liệu xác thực và ủy quyền giữa các miền bảo mật. Nó đang ngày càng trở nên quan trọng đối với các giải pháp dựa trên đám mây và với các ứng dụng Phần mềm như một Dịch vụ (SaaS) vì nó đảm bảo khả năng tương tác qua lại giữa các nhà cung cấp danh tính.

SAML là một giao thức dựa-trên-XML sử dụng mã thông báo bảo mật và khăng định để chuyển thông tin về một “người ủy nhiệm” (thường là một người dùng cuối) cho cơ quan SAML (“nhà cung cấp danh tính” hoặc IdP) và nhà cung cấp dịch vụ (SP). Người ủy nhiệm yêu cầu một dịch vụ từ SP, sau đó yêu cầu và nhận được xác nhận danh tính từ IdP. Sau đó, SP có thể cấp quyền truy cập hoặc thực hiện dịch vụ được yêu cầu cho người ủy nhiệm.

---



**MÁCH NƯỚC CHO KỲ THI** Bằng cách cho phép các nhà cung cấp danh tính chuyển thông tin đăng nhập cho các nhà cung cấp dịch vụ, SAML cho phép bạn đăng nhập và rất nhiều trang web khác nhau bằng cách chỉ sử dụng một bộ thông tin đăng nhập.

### **Hệ thống Kiểm soát Truy cập Bộ Kiểm soát Truy cập Thiết bị đầu cuối + (TACACS+)**

*Giao thức Hệ thống Kiểm soát Truy cập Bộ Kiểm soát Truy cập Thiết bị đầu cuối + (TACACS+)* là thế hệ hiện tại của họ TACACS. TACACS + có các quy trình tính toán và kiểm soát thuộc tính được mở rộng.

Một trong những khía cạnh thiết kế cơ bản là sự tách biệt của xác thực, cấp phép và tính toán trong giao thức này. Mặc dù có một dòng đơn giản của các giao thức này từ TACACS ban đầu, TACACS+ là một bản sửa đổi lớn và không tương thích ngược với các phiên bản trước của loạt giao thức họ TACACS.

TACACS + sử dụng TCP làm giao thức truyền tải của nó, thường hoạt động trên cổng TCP 49. Cổng này được sử dụng cho quá trình đăng nhập. Cả cổng UDP và TCP 49 đều được dành riêng cho giao thức máy chủ đăng nhập TACACS+.

TACACS+ là một giao thức máy khách/máy chủ, với máy khách thường là một máy chủ truy cập mạng (NAS) và máy chủ là một tiến trình daemon trên máy chủ UNIX, Linux hoặc Windows. Điều quan trọng cần phải lưu ý là vì nếu máy của người dùng (thường là máy tính cá nhân) không phải là máy khách (thường là NAS), thì thông tin liên lạc giữa máy tính cá nhân và NAS thường không được mã hóa và được truyền đi dưới dạng văn bản dạng rõ ràng. Thông tin liên lạc giữa máy khách TACACS+ và máy chủ TACACS+ được mã hóa bằng cách sử dụng một bí mật chia sẻ được định cấu hình thủ công cho từng thực thể và không được chia sẻ qua kết nối. Do đó, thông tin liên lạc giữa máy khách TACACS+ (thường là NAS) và máy chủ TACACS+ được bảo mật, nhưng thông tin liên lạc giữa người dùng (thường là máy tính cá nhân) và máy khách TACACS+ có thể bị ảnh hưởng.

---



**MÁCH NƯỚC CHO KỲ THI** TACACS+ là một giao thức sử dụng phương pháp tiếp cận mô hình máy khách/máy chủ và xử lý các dịch vụ xác thực, cấp phép và tính toán (AAA). Nó tương tự như RADIUS nhưng sử dụng TCP (cổng 49) làm phương pháp truyền tải.

## OAuth

*OAuth (Cấp phép Mở - Open Authorization)* là một giao thức mở cho phép cấp phép an toàn, dựa-trên-mã-thông-báo trên Internet từ các ứng dụng web, thiết bị di động và máy tính để bàn thông qua một phương pháp đơn giản và tiêu chuẩn. OAuth được sử dụng bởi các công ty như Google, Facebook, Microsoft và Twitter để cho phép người dùng chia sẻ thông tin về tài khoản của họ với các ứng dụng hoặc trang web của bên-thứ-ba. OAuth 1.0 được phát triển bởi một kỹ sư Twitter như một phần của việc triển khai Twitter OpenID. OAuth 2.0 (không tương thích ngược) đã thành

công với sự hỗ trợ từ hầu hết các nền tảng web lớn. Điểm mạnh chính của OAuth là nó có thể được trang web đối tác bên ngoài sử dụng để cho phép truy cập vào dữ liệu được bảo vệ mà không cần phải xác-thực-lại người dùng.

OAuth được tạo ra để loại bỏ nhu cầu của người dùng về việc chia sẻ mật khẩu của họ với các ứng dụng của bên-thứ-ba, thay vào đó là thay thế bằng một mã thông báo. OAuth 2.0 đã mở rộng điều này thành việc cung cấp các dịch vụ xác thực, vì vậy nó có thể loại bỏ nhu cầu đổi với OpenID.

### **OpenID**

*OpenID* là một lớp nhận dạng đơn giản nằm phía trên cùng của giao thức OAuth 2.0 vừa được thảo luận. OpenID cho phép các máy khách thuộc mọi loại, bao gồm các máy khách di động, JavaScript và dựa-trên-web, yêu cầu và nhận được thông tin về các phiên và người dùng cuối đã được xác thực. OpenID nhằm mục đích làm cho quá trình chứng minh bạn là ai trở nên dễ dàng hơn, là bước đầu tiên trong thang xác thực – cấp phép. Để thực hiện cấp phép, cần phải có quy trình thứ hai và OpenID thường được ghép nối với OAuth 2.0. OpenID đã được tạo ra để xác thực liên kết cho phép một bên-thứ-ba, chẳng hạn như Google hoặc Facebook, xác thực người dùng của bạn cho bạn, bằng cách sử dụng tài khoản mà người dùng thực sự đã có.



**MÁCH NƯỚC CHO KỲ THI** OpenID và Oauth thường được sử dụng cùng với nhau, nhưng có những mục đích khác nhau. OpenID được sử dụng để xác thực trong khi Oauth được sử dụng để cấp phép.

### **Kerberos**

Được phát triển như một phần của dự án Athena của MIT, *Kerberos* là một giao thức xác thực mạng được thiết kế cho môi trường máy

khách/máy chủ. Bản phát hành hiện tại tại thời điểm viết quyển sách này là Kerberos phiên bản 5, bản phát hành 1.18.5, được hỗ trợ bởi tất cả các hệ điều hành chính. Kerberos chuyển một cách an toàn một khóa đối xứng qua một mạng không bảo mật bằng cách sử dụng giao thức khóa đổi xứng Needham - Schroeder. Kerberos được xây dựng dựa trên ý tưởng về một bên-thứ-ba đáng tin cậy, được gọi là *trung tâm phân phối khóa (key distribution center - KDC)*, bao gồm hai phần tách biệt nhau về mặt logic: máy chủ xác thực (authentication server - AS) và máy chủ phân tích phiếu (ticket-granting server - TGS). Kerberos giao tiếp thông qua "phiếu (ticket)" dùng để chứng minh danh tính của người dùng.

Lấy tên gọi từ chú chó ba đầu trong thần thoại Hy Lạp, Kerberos được thiết kế để hoạt động trên Internet, một môi trường vốn dĩ không bảo mật. Kerberos sử dụng mã hóa mạnh mẽ để máy khách có thể chứng minh danh tính của mình với máy chủ và đến lượt mình, máy chủ có thể tự xác thực nó với máy khách. Môi trường Kerberos hoàn chỉnh được gọi là một lãnh địa Kerberos. Máy chủ Kerberos chứa các ID người dùng và mật khẩu đã được băm cho tất cả người dùng, những người sẽ có quyền đổi với các dịch vụ trong lãnh địa. Máy chủ Kerberos cũng có các khóa bí mật được chia sẻ với mọi máy chủ mà nó sẽ cấp phiếu truy cập.

Cơ sở để xác thực trong môi trường Kerberos là phiếu. Phiếu được sử dụng theo quy trình bao gồm hai bước với máy khách. Phiếu đầu tiên là phiếu cấp-phiếu (ticket-granting ticket - TGT) do AS cấp cho một máy khách đang có yêu cầu. Sau đó, máy khách có thể xuất trình phiếu này cho máy chủ Kerberos kèm theo yêu cầu một phiếu để truy cập một máy chủ cụ thể. Phiếu từ-máy-khách-đến-máy-chủ này được sử dụng để truy cập vào dịch vụ của máy chủ trong lĩnh vực này. Vì toàn bộ phiên có thể được mã hóa, do đó điều này sẽ loại bỏ việc truyền tải các mục vốn không bảo mật, chẳng hạn như mật khẩu có thể bị chặn lại trên mạng. Phiếu có

dẫu thời gian và có thời hạn sử dụng, vì vậy việc cố gắng sử dụng lại phiếu sẽ không thành công.

Các bước liên quan đến xác thực Kerberos bao gồm:

1. Người dùng trình ra thông tin đăng nhập và yêu cầu một phiếu từ Trung tâm Phân phối Khóa (KDS).
2. KDS xác minh thông tin đăng nhập và phát hành một TGT.
3. Người dùng trình ra một TGT và yêu cầu dịch vụ đối với KDS.
4. KDS xác minh việc cấp phép và phát hành một phiếu từ-máy-khách-đến-máy-chủ.
5. Người dùng trình ra một yêu cầu và một phiếu từ-máy-khách-đến-máy-chủ cho dịch vụ mong muốn.
6. Nếu phiếu từ-máy-khách-đến-máy-chủ hợp lệ, dịch vụ được cấp cho máy khách.

Để minh họa cách mà dịch vụ xác thực Kerberos hoạt động, bạn hãy nghĩ về giấy phép lái xe phổ biến. Bạn đã nhận được một giấy phép mà bạn có thể xuất trình cho các tổ chức khác để chứng minh rằng bạn là chính mình. Bởi vì các tổ chức khác tin tưởng vào tiểu bang mà giấy phép đã được cấp nên họ sẽ chấp nhận giấy phép của bạn như một bằng chứng về danh tính của bạn. Trạng thái mà giấy phép được cấp tương tự như lĩnh vực dịch vụ xác thực Kerberos và giấy phép này đóng vai trò như một phiếu máy-khách-máy-chủ. Đó là thực thể đáng tin cậy mà cả hai bên đều dựa vào để cung cấp thông tin nhận dạng hợp lệ. Tính tương tự này không phải là hoàn hảo, bởi vì tất cả chúng ta có thể đã nghe nói về những cá nhân lấy được bằng lái xe rởm, nhưng nó đóng vai trò minh họa cho ý tưởng cơ bản đằng sau Kerberos.



**MÁCH NƯỚC CHO KỲ THI** Kerberos là một dịch vụ xác thực của bên-thứ-ba sử dụng một loạt các phiếu như mã thông báo (token) để xác thực người dùng. Các bước liên quan được bảo vệ bằng cách sử dụng mật mã mạnh mẽ.

### Lược đồ Kiểm soát Truy cập

Thuật ngữ *kiểm soát truy cập* mô tả nhiều phương án bảo vệ. Nó đôi khi đề cập đến tất cả các tính năng bảo mật được sử dụng để ngăn chặn truy cập trái phép vào một hệ thống máy tính hoặc mạng. Theo nghĩa này, nó có thể bị nhầm lẫn với *xác thực*. Nói đúng hơn, *quyền truy cập* là khả năng của một chủ thể (chẳng hạn như một cá nhân hoặc một tiến trình đang chạy trên một hệ thống máy tính) tương tác với một đối tượng (chẳng hạn như một tập tin hoặc thiết bị phần cứng). Nói cách khác, xác thực liên quan đến việc xác minh danh tính của một chủ thể.

Để hiểu được sự khác biệt, hãy xem xét ví dụ về việc một cá nhân cố gắng đăng nhập vào hệ thống máy tính hoặc mạng. Xác thực là quá trình được sử dụng để xác nhận với hệ thống máy tính hoặc mạng rằng cá nhân đó [*cá nhân đang cố gắng đăng nhập*] là chính mình. Phương pháp phổ biến nhất để thực hiện việc này là thông qua việc sử dụng ID người dùng và mật khẩu. Sau khi cá nhân đã xác minh được danh tính của mình, các biện pháp kiểm soát truy cập quy định những gì cá nhân đó thực sự có thể thực hiện trên hệ thống - chỉ vì một người được cấp quyền truy cập vào hệ thống không có nghĩa là người đó phải có quyền truy cập vào tất cả những dữ liệu mà hệ thống đang chứa.

Hãy cùng xem xét một ví dụ khác. Khi bạn đến ngân hàng để rút tiền, nhân viên giao dịch tại quầy giao dịch sẽ xác minh rằng bạn thực sự chính là người mà bạn tuyên bố bằng cách yêu cầu bạn cung cấp một số mẫu

giấy tờ tùy thân có ảnh của bạn trên đó, chẳng hạn như bằng lái xe của bạn. Bạn cũng có thể phải cung cấp sổ tài khoản ngân hàng của mình. Sau khi nhân viên giao dịch đã xác minh được danh tính của bạn, bạn sẽ chứng minh được rằng bạn là khách hàng hợp lệ (được cấp phép) của ngân hàng này. Tuy nhiên, điều này không có nghĩa là bạn có khả năng xem tất cả thông tin mà ngân hàng đang bảo vệ - chẳng hạn như số dư tài khoản của hàng xóm của bạn. Nhân viên giao dịch sẽ kiểm soát những thông tin và số tiền mà bạn có thể truy cập và sẽ chỉ cấp cho bạn quyền truy cập vào thông tin mà bạn được phép xem. Trong ví dụ này, nhận dạng và số tài khoản ngân hàng của bạn đóng vai trò như là phương thức xác thực của bạn và nhân viên giao dịch đóng vai trò là cơ chế kiểm soát truy cập.

Trong các hệ thống máy tính và mạng, kiểm soát truy cập có thể được thực hiện theo một số cách. Ma trận kiểm soát truy cập cung cấp khuôn khổ đơn giản nhất để minh họa cho quy trình và được trình bày trong Bảng 24-1. Trong ma trận này, hệ thống đang theo dõi hai tiến trình, hai tập tin và một thiết bị phần cứng. Tiến trình 1 có thể đọc cả Tập tin 1 và Tập tin 2 nhưng chỉ có thể ghi vào Tập tin 1. Tiến trình 1 không thể truy cập Tiến trình 2, nhưng Tiến trình 2 có thể thực thi Tiến trình 1. Cả hai tiến trình đều có khả năng ghi vào máy in.

	Tiến trình 1	Tiến trình 2	Tập tin 1	Tập tin 2	Máy in
Tiến trình 1	Đọc, ghi, thực thi		Đọc, ghi	Đọc	Ghi
Tiến trình 2	Thực thi	Đọc, ghi, thực thi	Đọc, ghi	Đọc, ghi	Ghi

**Bảng 24-1** Ma trận Kiểm soát Truy cập

Mặc dù khá đơn giản để hiểu được nhưng ma trận kiểm soát truy cập ít khi được sử dụng trong các hệ thống máy tính bởi vì nó cực kỳ tốn kém về không gian lưu trữ và xử lý. Hãy tưởng tượng về kích thước của một ma trận kiểm soát truy cập cho một mạng lớn với hàng trăm người dùng và hàng nghìn tập tin. Những cơ chế thực tế về cách thức triển khai các biện pháp kiểm soát truy cập trong một hệ thống sẽ khác nhau, mặc dù danh sách kiểm soát truy cập (ACL) là rất phổ biến. ACL không gì khác hơn là một danh sách chứa các chủ thể có quyền truy cập vào một đối tượng cụ thể. Danh sách xác định không chỉ chủ thể mà còn xác định quyền truy cập cụ thể được cấp cho chủ thể đối với đối tượng. Các kiểu truy cập điển hình bao gồm đọc, ghi và thực thi, như được chỉ ra trong ma trận kiểm soát truy cập mẫu.

Bất kể cơ chế cụ thể nào được sử dụng để triển khai các biện pháp kiểm soát truy cập trong hệ thống máy tính hoặc mạng, các biện pháp kiểm soát đều phải dựa trên một *mô hình* truy cập cụ thể. Một số mô hình khác nhau được thảo luận trong tài liệu bảo mật và được liệt kê trong mục tiêu 3.8 của kỳ thi, bao gồm kiểm soát truy cập dựa-trên-thuộc-tính (attribute-based access control - ABAC), kiểm soát truy cập dựa-trên-vai-trò (role-based access control - RBAC), kiểm soát truy cập dựa-trên-quy-tắc (rule-based access control - cũng viết tắt là RBAC), kiểm soát truy cập bắt buộc (mandatory access control - MAC) , và kiểm soát truy cập tùy ý (discretionary access control - DAC).

### **Kiểm soát Truy cập Dựa-trên-Thuộc-tính (ABAC)**

*Kiểm soát truy cập dựa-trên-thuộc-tính (ABAC)* là một hình thức kiểm soát truy cập dựa trên các thuộc tính. Những thuộc tính này có thể khác nhau về hình thức, chẳng hạn như các thuộc tính người dùng, nguồn tài nguyên hoặc các thuộc tính của đối tượng và các thuộc tính của môi trường. Ví dụ, một bác sĩ có thể truy cập vào các hồ sơ y tế nhưng chỉ

của các bệnh nhân mà cô ấy đã được chỉ định, hoặc chỉ khi cô ấy đang trong ca trực. Sự khác biệt chính giữa ABAC và kiểm soát truy cập dựa-trên-vai-trò (sẽ được thảo luận tiếp theo) là khả năng bao gồm lý luận Boolean trong quyết định kiểm soát truy cập.



**MÁCH NƯỚC CHO KỲ THI** Quá trình cấp phép theo ABAC đánh giá các quy tắc và chính sách cụ thể so với các thuộc tính liên quan đến một chủ thể hoặc đối tượng. ABAC thường được sử dụng trong các doanh nghiệp lớn sử dụng một cấu trúc liên hợp. Nó có phần phức tạp và tốn kém hơn để triển khai so với các mô hình kiểm soát truy cập khác.

### **Kiểm soát Truy cập Dựa-trên-Vai-trò**

Các ACL có thể cồng kềnh và có thể mất thời gian để quản lý chúng một cách đúng đắn. Một cơ chế kiểm soát truy cập khác đang thu hút sự chú ý ngày càng tăng dần là *kiểm soát truy cập dựa-trên-vai-trò (RBAC)*. Trong lược đồ này, thay vì mỗi người dùng được chỉ định các quyền truy cập cụ thể cho các đối tượng được liên kết với hệ thống máy tính hoặc mạng, mỗi người dùng được chỉ định một tập hợp các vai trò mà họ có thể thực hiện. Các vai trò lần lượt được chỉ định các quyền truy cập cần thiết để thực hiện các tác vụ liên quan đến các vai trò đó. Do đó, người dùng sẽ được cấp quyền cho các đối tượng về các nhiệm vụ cụ thể mà họ phải thực hiện - không theo phân loại bảo mật liên quan đến các đối tượng riêng lẻ.

### **Kiểm soát Truy cập Dựa-trên-Quy-tắc**

Đầu tiên bạn có thể nhận thấy là sự mơ hồ đi kèm với phương pháp kiểm soát truy cập này cũng sử dụng từ viết tắt RBAC. *Kiểm soát truy cập dựa-trên-quy-tắc* cũng sử dụng các đối tượng như ACL để giúp xác định xem liệu có nên cấp quyền truy cập hay không. Trong trường hợp này,

một loạt các quy tắc được chứa trong ACL và việc xác định có cấp quyền truy cập hay không sẽ được thực hiện dựa trên các quy tắc này. Ví dụ về một quy tắc như vậy là quy tắc cho rằng không nhân viên nào có thể có quyền truy cập vào tập tin tiền lương sau giờ làm việc hoặc vào cuối tuần. Như với MAC (sẽ được thảo luận tiếp theo), người dùng không được phép thay đổi các quy tắc truy cập và quản trị viên sẽ được dựa vào để thực hiện việc này. Kiểm soát truy cập dựa-trên-quy-tắc thực sự có thể được sử dụng bổ sung hoặc như một phương pháp triển khai các phương pháp kiểm soát truy cập khác. Ví dụ, các phương pháp MAC có thể sử dụng phương pháp tiếp cận dựa-trên-quy-tắc để triển khai.



**MÁCH NƯỚC CHO KỲ THI** Để phân biệt rõ ràng giữa các biện pháp kiểm soát truy cập dựa-trên-vai-trò và dựa-trên-quy-tắc, ngay cả khi chúng sử dụng cùng một từ viết tắt. Tên gọi của từng biện pháp kiểm soát truy cập mô tả về những gì mà nó đòi hỏi và sẽ giúp bạn phân biệt được chúng.

### MAC

Một hệ thống ít được sử dụng hơn để hạn chế quyền truy cập là *kiểm soát truy cập bắt buộc* (*mandatory access control – MAC*). Hệ thống này, thường chỉ được sử dụng trong những môi trường mà trong đó các mức phân loại bảo mật khác nhau cùng tồn tại, hạn chế hơn nhiều về những gì người dùng được phép làm. Theo định nghĩa của "Orange Book", một tài liệu của Bộ Quốc phòng Hoa Kỳ (DoD) từng là tiêu chuẩn để mô tả những gì cấu thành nên một hệ thống máy tính đáng tin cậy, kiểm soát truy cập bắt buộc là "một phương tiện hạn chế quyền truy cập vào các đối tượng dựa trên độ nhạy cảm (như được thể hiện bằng một nhãn dán) của thông tin chứa trong các đối tượng và sự cấp phép chính thức (tức là cho phép sử dụng – clearance) cho các đối tượng truy cập thông tin

nhạy cảm như vậy". Trong trường hợp này, chủ sở hữu hoặc chủ thẻ không thể quyết định liệu quyền truy cập có được cấp cho chủ thẻ khác hay không, đó là công việc của hệ điều hành để đưa ra quyết định.



**MÁCH NƯỚC CHO KỲ THI** Phân loại thông tin phổ biến bao gồm Cao, Trung bình, Thấp, Mật, Riêng tư và Công khai (High, Medium, Low, Confidential, Private và Public).

Trong MAC, cơ chế bảo mật kiểm soát quyền truy cập vào tất cả các đối tượng, và các chủ thẻ riêng lẻ không thể thay đổi quyền truy cập đó. Điều then chốt ở đây là nhãn dán gắn liền với mọi chủ thẻ và đối tượng. Nhãn sẽ xác định mức độ phân loại cho đối tượng đó và mức độ mà theo đó chủ thẻ sẽ được hưởng. Hãy nghĩ đến các phân loại kiểu an ninh quân sự như Mật và Tối mật. Một tập tin đã được xác định là Tối mật (có nhãn dán cho biết rằng nó là Tối mật) chỉ có thể được xem bởi những cá nhân có quyền được xem thông tin Tối mật. Tùy thuộc vào cơ chế kiểm soát truy cập để đảm bảo rằng một cá nhân chỉ có quyền sử dụng thông tin Mật không bao giờ có quyền truy cập vào một tập tin đã được gắn nhãn là Tối mật. Tương tự, một người dùng đã bị xóa quyền truy cập Tối mật sẽ không được cơ chế kiểm soát truy cập cho phép thay đổi phân loại của tập tin đã được gắn nhãn là Tối mật thành Mật hoặc gửi tập tin Tối mật đó cho người dùng chỉ có quyền với thông tin Mật. Bạn có thể tìm hiểu thêm sự phức tạp của cơ chế như vậy khi bạn xem xét môi trường cửa sổ ngày nay. Cơ chế kiểm soát truy cập sẽ không cho phép người dùng cắt một phần của tài liệu Tối mật và dán nó vào cửa sổ chứa tài liệu chỉ có nhãn Mật. Chính sự tách biệt giữa các mức độ khác nhau của thông tin được phân loại dẫn đến việc kiểm soát này được gọi là *bảo mật đa cấp*.

Cuối cùng, chỉ vì một chủ thể có mức sử dụng thông tin thích hợp để xem được tài liệu không có nghĩa là cô ấy sẽ được phép thực hiện điều đó. Khái niệm về đặc quyền ít nhất (least privilege), đôi khi được gọi là “cần được biết (need to know)”, là một khái niệm DAC (sẽ được thảo luận tiếp theo dưới đây), cũng tồn tại trong các cơ chế MAC. Đặc quyền ít nhất có nghĩa là một người chỉ được cấp quyền truy cập vào thông tin mà cô ấy cần để hoàn thành công việc hoặc nhiệm vụ của mình.

### Kiểm soát Truy cập Tùy ý (DAC)

Cả kiểm soát truy cập tùy ý (*discretionary access control - DAC*) và kiểm soát truy cập bắt buộc đều là những thuật ngữ ban đầu được sử dụng bởi quân đội để mô tả hai phương pháp tiếp cận khác nhau để kiểm soát quyền truy cập của một cá nhân vào hệ thống. Theo “Orange Book”, DAC là “một phương tiện hạn chế quyền truy cập vào các đối tượng dựa trên danh tính của các chủ thể và/hoặc nhóm mà chúng thuộc về. Các biện pháp kiểm soát là tùy ý theo nghĩa là một chủ thể có quyền truy cập nhất định có thể chuyển quyền đó (có thể là gián tiếp) cho bất kỳ chủ thể nào đó khác”. Mặc dù điều này có vẻ gây nhầm lẫn khi “chính-phủ-nói”, nhưng nguyên tắc này khá đơn giản. Trong các hệ thống sử dụng DAC, chủ sở hữu của một đối tượng có thể quyết định chủ thể nào khác có thể có quyền truy cập vào đối tượng và quyền truy cập cụ thể nào mà họ [các chủ thể khác] có thể có. Một phương pháp phổ biến để thực hiện điều này là các bit về quyền được sử dụng trong các hệ thống dựa trên Linux. Chủ sở hữu tập tin có thể chỉ định những quyền nào (đọc/ghi/thực thi) các thành viên trong cùng một nhóm có thể có và những quyền mà tất cả những người khác có thể có. ACL cũng là một cơ chế phổ biến được sử dụng để triển khai DAC.



**MÁCH NƯỚC CHO KỲ THI** Nếu bạn đang cố gắng để ghi nhớ sự khác biệt giữa MAC và DAC thì chỉ cần nhớ rằng MAC tương ứng với các nhãn dán bảo mật đa cấp chẳng hạn như Tuyệt mật và Mật, trong khi DAC sử dụng các ACL.

### **Truy cập Có điều kiện**

*Truy cập có điều kiện* là một lược đồ kiểm soát truy cập trong đó những điều kiện cụ thể được kiểm tra trước khi quyền truy cập được cấp. Một điều kiện có thể là vị trí của người dùng khi truy cập vào các nguồn tài nguyên: nếu vị trí là cục bộ - quyền truy cập sẽ được cấp, nếu vị trí là từ xa – quyền truy cập bị từ chối. Danh sách các điều kiện có thể rất rộng và tuân theo hình thức phổ quát sau:

**Nếu {điều kiện} thì {hành động}**

Một số ví dụ bao gồm:

- **Nếu** {máy khách sử dụng xác thực kiểu kẽ thừa} **thì** {chặn quyền truy cập}
- **Nếu** {thiết bị không tuân thủ} **thì** {chặn quyền truy cập}
- **Nếu** {người dùng là quản trị viên} **thì** {kích hoạt xác thực đa yếu tố}

Truy cập có điều kiện có thể rất hữu ích khi một thực thể có một loạt các hệ thống khác nhau với những nhu cầu truy cập khác nhau.

### **Quản lý Truy cập có Đặc quyền**

Tài khoản có đặc quyền là bất kỳ tài khoản nào có quyền truy cập nhiều-hơn-người-dùng-bình-thường. Các tài khoản có đặc quyền thường là tài khoản cấp root hoặc cấp quản trị viên và đại diện cho rủi ro ở chỗ chúng không bị giới hạn về thẩm quyền của mình. Các tài khoản này đòi hỏi sự

giám sát theo-thời-gian-thực thường xuyên, nếu có thể, và luôn phải được giám sát khi vận hành từ xa. Các quản trị viên có thể cần phải thực hiện các tác vụ thông qua một phiên làm việc từ xa trong một số tình huống nhất định, nhưng khi họ thực hiện điều này, trước tiên họ cần xác định mục đích và được phê duyệt.

*Quản lý quyền truy cập có đặc quyền* là sự kết hợp của các chính sách, thủ tục và công nghệ để kiểm soát quyền truy cập và sử dụng các tài khoản nâng cao hoặc có đặc quyền. Điều này cho phép tổ chức ghi lại nhật ký và kiểm soát quyền truy cập có đặc quyền trên toàn bộ môi trường. Mục đích chính là hạn chế bề mặt tấn công mà các tài khoản này có và giảm thiểu khả năng bị phơi nhiễm dựa trên nhu cầu và điều kiện vận hành hiện tại.

### **Quyền hạn trên Hệ thống Tập tin**

Các tập tin cần phải được bảo mật trên hệ thống để ngăn chặn việc truy cập và thay đổi trái phép. Bảo mật hệ thống tập tin là tập hợp các cơ chế và quy trình được sử dụng để đảm bảo chức năng quan trọng này. Việc sử dụng một sự kết nối các cơ chế lưu trữ tập tin, cùng với danh sách kiểm soát truy cập và mô hình kiểm soát truy cập, mang lại một phương tiện để có thể thực hiện điều này. Bạn cần một hệ thống tập tin có khả năng hỗ trợ phân biệt quyền truy cập cấp-độ-người-dùng - một cái gì đó NTFS làm được nhưng FAT32 thì không. Tiếp theo, bạn cần có một mô hình kiểm soát truy cập đang hoạt động - MAC, DAC, ABAC, hoặc mô hình khác, như đã mô tả trước đây trong chương này. Sau đó, bạn cần một hệ thống để áp dụng các quyền của người dùng đối với tập tin, vốn có thể được xử lý bởi Hệ điều hành, mặc dù việc quản lý và duy trì điều này có thể là một thách thức.

Nếu có nhiều người dùng cùng chia sẻ một hệ thống máy tính, quản trị viên hệ thống có thể cần phải kiểm soát ai được phép làm những gì khi

xem, sử dụng hoặc thay đổi những tài nguyên hệ thống. Mặc dù các hệ điều hành khác nhau trong cách chúng triển khai các loại kiểm soát này nhưng hầu hết các hệ điều hành đều sử dụng các khái niệm về thẩm quyền và quyền hạn (permission và rights) để kiểm soát và bảo vệ quyền truy cập vào tài nguyên. *Thẩm quyền (permission)* kiểm soát những gì người dùng được phép thực hiện với các đối tượng trên hệ thống và *quyền hạn (rights)* xác định các hành động mà người dùng có thể thực hiện trên chính bản thân hệ thống. Hãy cùng xem xét cách mà hệ điều hành Windows triển khai khái niệm này.

Hệ điều hành Windows sử dụng các khái niệm về thẩm quyền và quyền hạn để kiểm soát quyền truy cập vào tập tin, thư mục và tài nguyên thông tin. Khi sử dụng hệ thống tập tin NTFS, quản trị viên có thể cấp quyền cho người dùng và các nhóm để thực hiện các tác vụ nhất định khi chúng liên quan đến tập tin, thư mục và khóa Registry. Những thể loại cơ bản của thẩm quyền NTFS như sau:



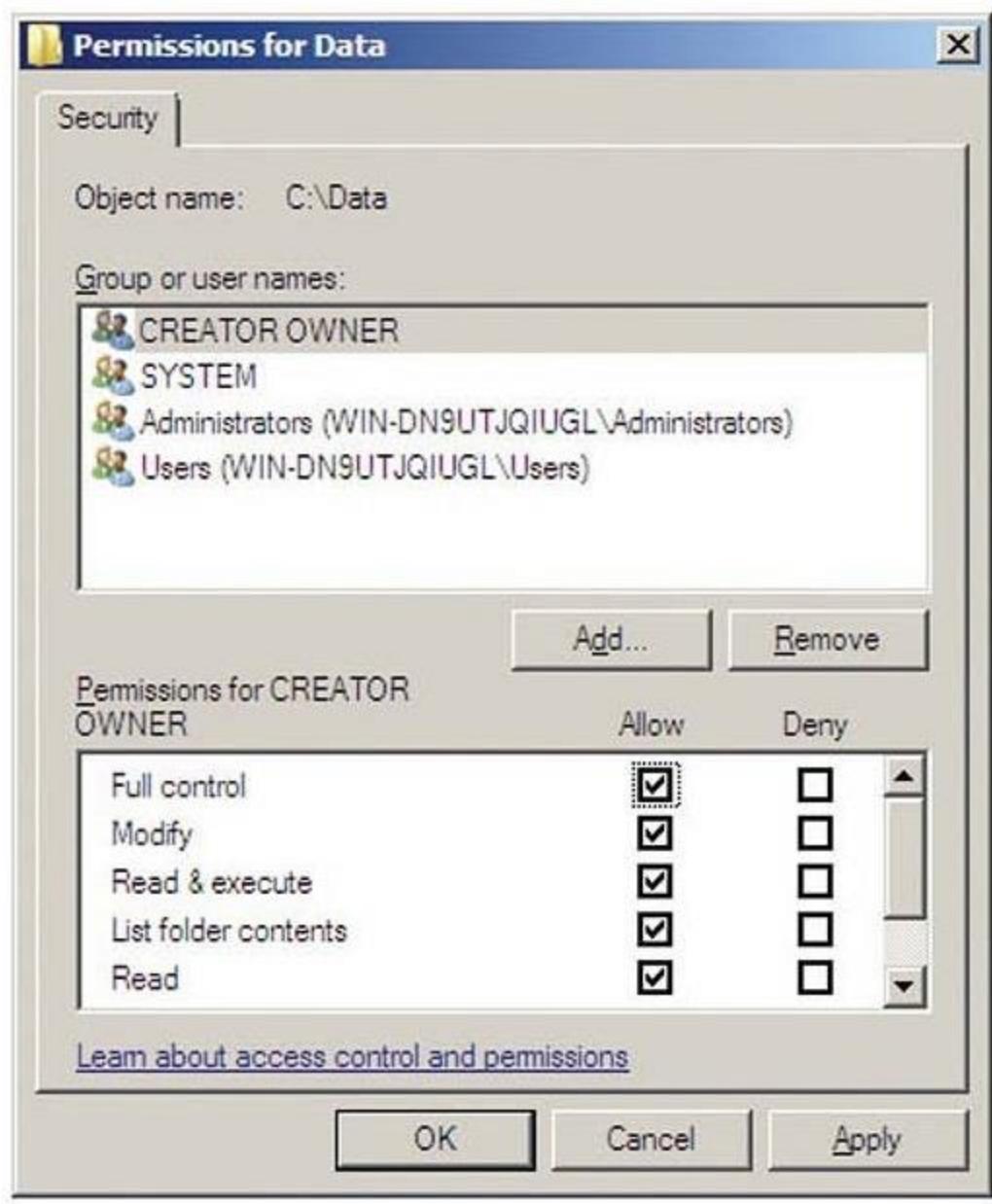
**MÁCH NƯỚC CHO KỲ THI** Thẩm quyền có thể được áp dụng cho một người dùng hoặc một nhóm cụ thể để kiểm soát khả năng của người dùng hoặc nhóm đó trong việc xem, sửa đổi, truy cập, sử dụng hoặc xóa nguồn tài nguyên như các thư mục và tập tin.

- **Toàn quyền (Full Control)** Một người dùng/nhóm có thể thay đổi thẩm quyền trên thư mục/tập tin, nắm quyền sở hữu nếu một ai đó khác đang sở hữu thư mục, tập tin, xóa các thư mục con và các tập tin, và thực hiện những hành động được chấp thuận bởi tất cả những quyền NTFS khác trên thư mục.
- **Sửa đổi (Modify)** Một người dùng/nhóm có thể xem và sửa đổi các tập tin/thư mục và những thuộc tính của chúng, có thể xóa và thêm

các tập tin/thư mục, và có thể xóa các thuộc tính khỏi hoặc bổ sung thêm thuộc tính cho một tập tin/thư mục.

- **Đọc và Thực thi (Read & Execute)** Một người dùng/nhóm có thể xem tập tin/thư mục và có thể thực thi các tập lệnh kịch bản và các tập tin có thể thực thi được, nhưng họ không thể thực hiện bất kỳ thay đổi nào (các tập tin/thư mục là chỉ-đọc).
- **Liệt kê Nội dung Thư mục (List Folder Content)** Một người dùng/nhóm có thể chỉ liệt kê được những gì nằm trong một thư mục (chỉ áp dụng cho các thư mục [*nghĩa là không áp dụng cho các tập tin – người dịch*]).
- **Đọc (Read)** Một người dùng/nhóm có thể xem được nội dung của tập tin/thư mục và các thuộc tính của tập tin/thư mục.
- **Ghi (Write)** Một người dùng/nhóm có thể ghi vào tập tin/thư mục.

Hình 24-2 minh họa cho các quyền trên một thư mục được gọi là Dữ liệu từ một hệ thống Máy chủ Windows. Nửa phần bên trên của cửa sổ Quyền là những người dùng và nhóm có quyền đối với thư mục này. Nửa phần dưới của cửa sổ là quyền được chỉ định cho người dùng hoặc nhóm đang được đánh dấu.



**Hình 24-2** Các quyền đối với thư mục Dữ liệu

Trong hệ điều hành UNIX, quyền đối với tập tin được cấu thành từ 3 phần khác nhau:

- **Quyền Chủ sở hữu (đọc, ghi, và thực thi)** Chủ sở hữu của tập tin.

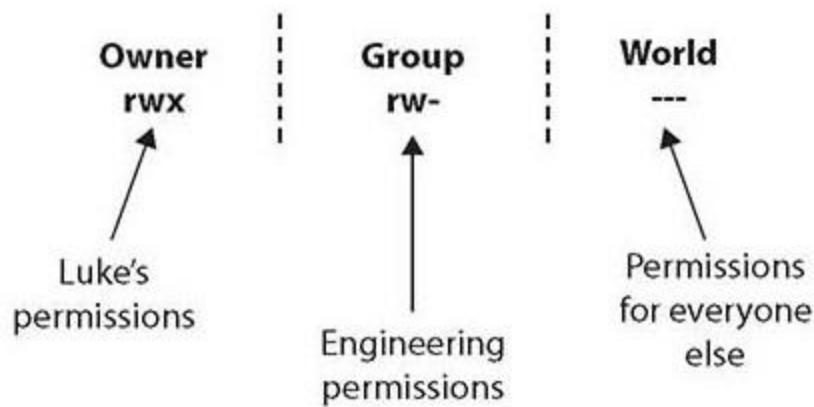
- **Quyền Nhóm (đọc, ghi và thực thi)** Nhóm mà chủ sở hữu của tập tin đang thuộc về.
- **Quyền Tất cả (đọc, ghi và thực thi)** Bất kỳ ai khác không phải là chủ sở hữu và không thuộc về nhóm mà chủ sở hữu của tập tin đang thuộc về.



**MÁCH NƯỚC CHO KỸ THI** Kiểm soát truy cập tùy ý giới hạn quyền truy cập dựa trên danh tính của người dùng hoặc quyền của thành viên của nhóm.

Ví dụ, giả sử một tập tin có tên là *dữ liệu bí mật (secretdata)* đã được tạo bởi chủ sở hữu của tập tin, Luke, người thuộc về nhóm Kỹ thuật. Quyền của chủ sở hữu đối với tập tin sẽ phản ánh quyền truy cập của Luke đối với tập tin (với tư cách là chủ sở hữu). Các quyền của nhóm sẽ phản ánh quyền truy cập được cấp cho bất kỳ ai là thành viên của nhóm Kỹ thuật. Các quyền tất cả sẽ đại diện cho quyền truy cập được cấp cho bất kỳ ai không phải là Luke và không thuộc nhóm Kỹ thuật.

Trong Linux, quyền của tập tin thường được hiển thị dưới dạng một chuỗi chín ký tự, với ba ký tự đầu tiên đại diện cho quyền của chủ sở hữu, ba ký tự thứ hai đại diện cho quyền của nhóm và ba ký tự cuối đại diện cho quyền của mọi người khác (nghĩa là cho tất cả những người khác). Khái niệm này được minh họa trong Hình 24-3.



**Hình 24-3** Quyền tùy ý đổi với tập tin trong môi trường UNIX

Giả sử rằng tập tin dữ liệu bí mật (secretdata) được sở hữu bởi Luke với quyền nhóm của Kỹ thuật (bởi vì Luke là một thành viên của nhóm Kỹ thuật), và quyền trên tập tin đó là rwx, rw-, và ---, như được minh họa trong Hình 24-3. Điều này có nghĩa là:

- Luke có thể đọc, ghi và thực thi tập tin (rwx).
  - Các thành viên của nhóm Kỹ thuật có thể đọc và ghi tập tin nhưng không được thực thi nó (rw-).
  - Những người khác không có quyền truy cập tập tin và không thể đọc, ghi hay thực thi nó (---).

Hãy nhớ rằng, theo mô hình DAC, chủ sở hữu của tập tin, Luke, có thể thay đổi những quyền đối với tập tin bất cứ khi nào anh ta muốn.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với cách triển khai các giải pháp xác thực và cấp phép. Chương này được mở đầu bằng việc kiểm tra quản lý xác thực, bao gồm khóa mật khẩu, kho chứa mật khẩu, giải pháp TPM và HSM và xác thực dựa-trên-kiến-thức.

Phần tiếp theo đề cập đến các dạng giải pháp xác thực, bắt đầu với các giao thức EAP, CHAP và PAP. Tiếp theo là IEEE 802.1X, RADIUS và các giải pháp đăng nhập một-lần. Mô tả về Ngôn ngữ Đánh dấu Khẳng định Bảo mật (SAML) là mục tiếp theo được đề cập, sau đó là phần thảo luận về Bộ Kiểm soát Truy cập Thiết bị đầu cuối/Hệ thống Kiểm soát Truy cập Plus (TACACS+). Các phương pháp của OAuth và OpenID đã được thảo luận tiếp theo và phần này khép lại bằng một cuộc thảo luận về Kerberos.

Phần cuối cùng của chương này đề cập đến các lược đồ kiểm soát truy cập. Nó mở đầu bằng một cuộc thảo luận về kiểm soát truy cập dựa-trên-thuộc-tính (ABAC), kiểm soát truy cập dựa-trên-vai-trò (RBAC), kiểm soát truy cập dựa-trên-quy-tắc (cũng viết tắt là RBAC), kiểm soát truy cập bắt buộc (MAC) và kiểm soát truy cập tùy ý (DAC). Phần này đã khép lại với một cuộc thảo luận về kiểm soát truy cập có điều kiện, quản lý quyền truy cập có đặc quyền và quyền đối với hệ thống tập tin.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

- 1.** Tổ chức của bạn cần một hệ thống để giới hạn quyền truy cập vào các tập tin dựa trên độ nhạy cảm của thông tin trong những tập tin đó. Bạn có thể đề xuất những hệ thống kiểm soát truy cập nào dưới đây?
  - A.** Kiểm soát truy cập tùy ý
  - B.** Kiểm soát truy cập bắt buộc
  - C.** Kiểm soát truy cập bí mật
  - D.** Kiểm soát truy cập dựa-trên-tập-tin.
- 2.** Điều nào dưới đây mô tả sự khác biệt chính giữa hệ thống tập tin NTFS và FAT32?
  - A.** NTFS hỗ trợ phân biệt quyền truy cập ở cấp-degree-user-used.
  - B.** FAT32 hỗ trợ phân biệt truy cập cấp-degree-group.
  - C.** FAT32 mã hóa nguyên bản các tập tin và thư mục.
  - D.** NTFS ghi lại tất cả các truy cập tập tin bằng cách sử dụng mã thông báo an toàn.
- 3.** Tổ chức của bạn đã phát triển quá lớn để hỗ trợ việc chỉ định quyền cho từng người dùng. Trong tổ chức của bạn, bạn có các nhóm lớn người dùng đang thực hiện các nhiệm vụ giống nhau và cần cùng kiểu và cấp độ truy cập vào các tập tin giống nhau. Thay vì chỉ định các quyền riêng lẻ, tổ chức của bạn có thể muốn xem xét sử dụng phương pháp kiểm soát truy cập nào sau đây?
  - A.** Kiểm soát truy cập dựa-trên-nhóm
  - B.** Kiểm soát truy cập dựa-trên-ca-làm-việc
  - C.** Kiểm soát truy cập dựa-trên-vai-trò

- D. Kiểm soát truy cập dựa-trên-tập-tin.**
- 4.** Máy chủ cấp phát phiếu (ticket) là yếu tố quan trọng trong mô hình xác thực nào sau đây?
- A. 802.1X**  
**B. RADIUS**  
**C. TACACS +**  
**D. Kerberos.**
- 5.** Tiêu chuẩn nào sau đây là một tiêu chuẩn mở sử dụng mã thông báo và xác nhận bảo mật và cho phép bạn truy cập nhiều trang web bằng một bộ thông tin xác thực?
- A. PAP**  
**B. CHAP**  
**C. SSO**  
**D. SAML.**
- 6.** Giao thức nào được sử dụng cho RADIUS?
- A. UDP**  
**B. NetBIOS**  
**C. TCP**  
**D. Độc quyền**
- 7.** Các tài khoản có quyền truy cập nhiều hơn "bình thường" của người dùng được gọi là gì?
- A. Tài khoản có đặc quyền**  
**B. Tài khoản hệ thống**  
**C. Tài khoản siêu người dùng**  
**D. Tài khoản kiểm toán.**
- 8.** Bạn phải triển khai một giải pháp OpenID. Mỗi quan hệ điển hình với các hệ thống hiện có là gì?
- A. OpenID được sử dụng để xác thực, OAuth được sử dụng để cấp phép.**

- B.** OpenID được sử dụng để cấp phép, OAuth được sử dụng để xác thực.
- C.** OpenID không tương thích với OAuth.
- D.** OpenID chỉ hoạt động với Kerberos.
- 9.** Bạn muốn tạo ra một lược đồ kiểm soát truy cập cho phép Giám đốc tài chính truy cập dữ liệu tài chính từ máy của mình, nhưng không phải từ máy tính trong khu vực lõi tân của sảnh. Mô hình kiểm soát truy cập nào phù hợp nhất cho việc này?
- A.** Kiểm soát truy cập dựa-trên-vai-trò
- B.** Kiểm soát truy cập có điều kiện
- C.** Kiểm soát truy cập bắt buộc
- D.** Kiểm soát truy cập tùy ý.
- 10.** Bạn cần thiết kế một hệ thống xác thực nơi những người dùng chưa từng kết nối với hệ thống có thể được xác định và xác thực trong một quy trình duy nhất. Giải pháp nào dưới đây là tốt nhất?
- A.** RADIUS
- B.** Xác thực dựa-trên-kho-chứa-mật-khẩu
- C.** Xác thực dựa-trên-TPM
- D.** Xác thực dựa-trên-kiến-thức.

## Đáp án

1. **B.** Kiểm soát truy cập bắt buộc (MAC) là một hệ thống được sử dụng trong các môi trường có các mức độ phân loại bảo mật khác nhau. Quyền truy cập vào các đối tượng (chẳng hạn như tập tin) dựa trên mức độ nhạy cảm của thông tin được chứa trong các đối tượng đó và sự cấp phép của người dùng để truy cập thông tin với mức độ nhạy cảm đó.
2. **A.** NTFS hỗ trợ phân biệt quyền truy cập ở cấp-độ-người-dùng và cho phép bạn gán quyền của người dùng cho các tập tin và thư mục.
3. **C.** Tổ chức của bạn có thể xem xét kiểm soát truy cập dựa-trên-vai-trò. Trong kiểm soát truy cập dựa-trên-vai-trò, thay vì mỗi người dùng được chỉ định các quyền truy cập cụ thể cho các đối tượng được liên kết với hệ thống máy tính hoặc mạng, mỗi người dùng được chỉ định một tập hợp các vai trò mà họ có thể thực hiện. Các vai trò lần lượt được chỉ định các quyền truy cập cần thiết để thực hiện các tác vụ liên quan đến các vai trò đó. Do đó, người dùng sẽ được cấp quyền đối với các đối tượng về các nhiệm vụ cụ thể mà họ phải thực hiện - không theo phân loại bảo mật liên quan đến các đối tượng riêng lẻ.
4. **D.** Kerberos sử dụng máy chủ cấp phát phiếu để quản lý việc phát hành phiếu cấp các quyền khác nhau trên hệ thống.
5. **D.** SAML là một giao thức dựa trên XML sử dụng mã thông báo bảo mật và xác nhận để chuyển thông tin về "người được ủy nhiệm" (thường là người dùng đầu cuối) cho cơ quan SAML ("nhà cung cấp danh tính" hoặc IdP) và nhà cung cấp dịch vụ (SP). Nói một cách đơn giản hơn, bằng cách cho phép nhà cung cấp danh tính chuyển thông tin đăng nhập cho nhà cung cấp dịch vụ, SAML

cho phép bạn có thể đăng nhập vào nhiều trang web khác nhau bằng cách sử dụng cùng một bộ thông tin xác thực.

6. **A.** RADIUS đã được Cơ quan quản lý Số được Chỉ định trên Internet (IANA) chỉ định chính thức cổng UDP 1812 để xác thực RADIUS và cổng 1813 cho tính toán RADIUS. Tuy nhiên, trước đây, các cổng 1645 (xác thực) và 1646 (tính toán) được sử dụng một cách không chính thức và trở thành các cổng mặc định được chỉ định bởi rất nhiều triển khai máy khách/máy chủ RADIUS tại thời điểm đó. Truyền thống sử dụng 1645 và 1646 để tương thích ngược vẫn còn tiếp tục cho đến ngày nay. Vì lý do này, nhiều triển khai máy chủ RADIUS giám sát cả hai bộ cổng UDP cho các yêu cầu RADIUS. Máy chủ RADIUS của Microsoft mặc định là 1812 và 1813, nhưng các thiết bị của Cisco mặc định là cổng 1645 và 1646 truyền thống.
7. **A.** Tài khoản có đặc quyền là bất kỳ tài khoản nào có quyền truy cập nhiều-hơn-người-dùng-bình-thường. Các tài khoản có đặc quyền thường là tài khoản cấp root hoặc cấp quản trị viên và thể hiện rủi ro ở chỗ quyền hạn của chúng là không bị giới hạn.
8. **A.** Thông thường OpenID được sử dụng để xác thực và OAuth được sử dụng để cấp phép.
9. **B.** Các mô hình kiểm soát truy cập có điều kiện hỗ trợ cho các lược đồ kiểm soát truy cập khác nhau dựa trên các điều kiện cụ thể ngoài tài khoản người dùng.
10. **D.** Các lược đồ xác thực dựa-trên-kiến-thức cho phép xác thực những người dùng chưa thiết lập danh tính của họ trước đó thông qua phương pháp xác thực và nhận dạng được kết hợp.

## Chương 25 Cơ sở hạ tầng Khóa Công khai

---

### Cơ sở hạ tầng Khóa Công khai

Trong chương này bạn sẽ

- Tìm hiểu về những thành phần khác nhau của một hệ thống PKI,
  - Tìm hiểu về những ý tưởng để triển khai một hệ thống PKI,
  - Tìm hiểu về cách các chứng nhận được sử dụng như một phần của một giải pháp bảo mật như thế nào,
  - Triển khai các thành phần cơ sở hạ tầng khóa công khai.
- 

Một *cơ sở hạ tầng khóa công khai (PKI)* cung cấp mọi thành phần cần thiết cho các kiểu người dùng và thực thể khác nhau để có thể giao tiếp một cách an toàn và theo cách có thể dự đoán được. Một PKI được tạo thành từ phần cứng, các ứng dụng, chính sách, dịch vụ, giao diện lập trình, thuật toán mật mã, giao thức, người dùng và tiện ích. Các thành phần này hoạt động cùng nhau để hỗ trợ giao tiếp để quản lý các khóa bất đối xứng tạo điều kiện thuận lợi cho việc sử dụng mật mã khóa công khai cho chữ ký kỹ thuật số, mã hóa dữ liệu và tính toàn vẹn. Mặc dù rất nhiều ứng dụng và giao thức khác nhau có thể cung cấp chức năng cùng loại nhưng việc xây dựng và triển khai PKI sẽ giúp thiết lập mức độ tin cậy.

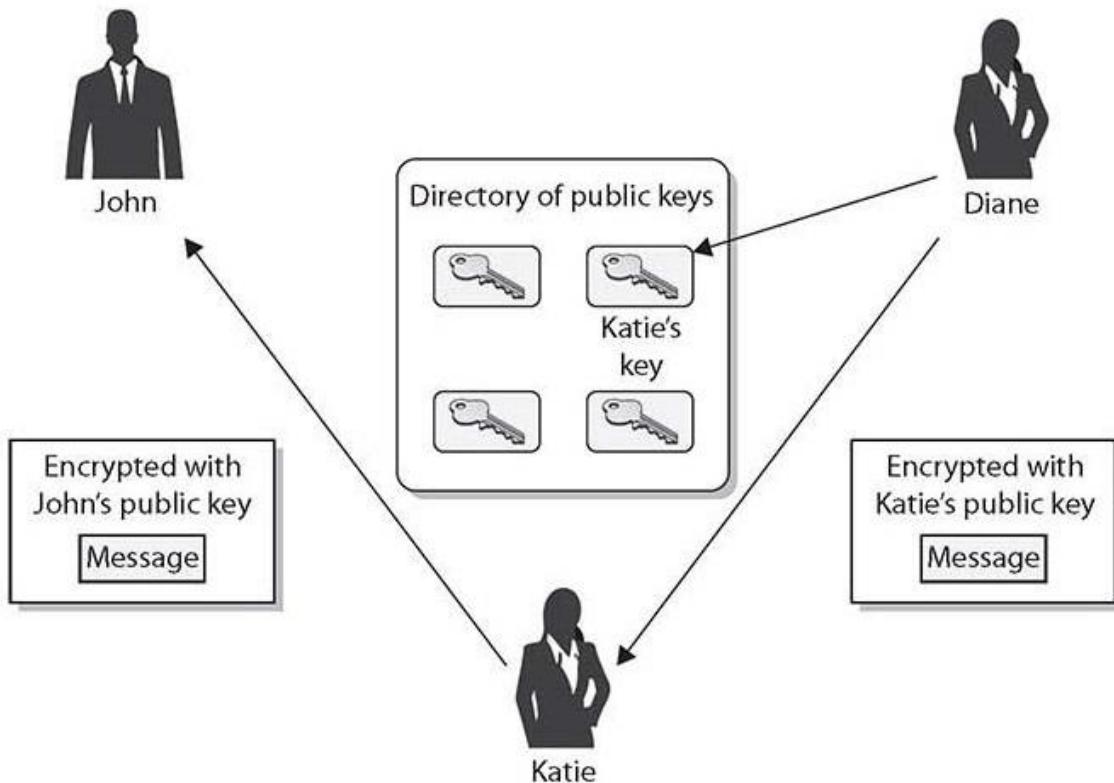
**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 3.9 của kỳ thi CompTIA Security+: Đưa ra một kịch bản, triển khai cơ sở hạ tầng khóa công khai.

Mục tiêu này là một ứng cử viên rất tốt cho các câu hỏi dựa-trên-hiệu-suất, có nghĩa là bạn nên dự kiến các câu hỏi trong đó bạn phải áp dụng kiến thức của mình về chủ đề cho một tình huống. Đáp án tốt nhất cho một câu hỏi sẽ phụ thuộc vào các chi tiết cụ thể trong tình huống trước câu hỏi chứ không chỉ câu hỏi. Các câu hỏi cũng có thể liên quan đến các nhiệm vụ khác ngoài việc chỉ chọn đáp án tốt nhất từ danh sách. Thay vào đó, bạn có thể được hướng dẫn để sắp xếp các mục trên sơ đồ, sắp xếp các tùy chọn theo thứ tự xếp hạng, khớp hai cột của các mục hoặc thực hiện một tác vụ tương tự.

## Cơ sở hạ tầng Khóa Công khai (PKI)

Một PKI được cấu thành từ một số thành phần, tất cả đều hoạt động cùng nhau để xử lý việc phân phối và quản lý các khóa trong hệ thống mật mã khóa công khai. Các khóa được thực hiện thông qua một cấu trúc kỹ thuật số được gọi là *chứng nhận*. Các thành phần khác, chẳng hạn như cơ quan cấp chứng nhận và cơ quan đăng ký tồn tại để quản lý các chứng nhận. Hoạt động cùng nhau, các thành phần này cho phép sử dụng liền mạch mật mã khóa công khai giữa các hệ thống.

Ví dụ: nếu John và Diane muốn giao tiếp một cách an toàn, John có thể tạo ra cặp khóa công khai/riêng tư của riêng mình và gửi khóa công khai của mình cho Diane hoặc anh ta có thể đặt khóa công khai của mình trong một danh bạ [directoy] (thư mục [folder]) khả dụng cho tất cả mọi người. Nếu Diane nhận được khóa công khai của John, cho dù từ anh ta hoặc từ một danh bạ công khai, làm thế nào cô ấy biết nó thực sự đến từ John? Có thể một cá nhân khác đang giả danh John và đã thay thế khóa công khai của John bằng khóa của chính cô ấy, như được minh họa trong Hình 25-1. Nếu điều này xảy ra, Diane sẽ tin rằng chỉ John mới có thể đọc được các tin nhắn của cô và các thư trả lời thực sự là từ anh ta. Tuy nhiên, cô ấy thực sự sẽ giao tiếp với Katie. Những gì cần thiết là một cách thức để xác minh danh tính của một cá nhân, để đảm bảo rằng khóa công khai của một người được ràng buộc với danh tính của họ và do đó đảm bảo rằng kịch bản trước đó (và những kịch bản khác) không thể diễn ra.



### Tấn công Người-Trung-gian

1. Katie thay thế khóa công khai của John bằng khóa của cô ấy trong danh bạ có thể truy cập công khai.
2. Diane trích xuất những gì cô ấy nghĩ là đó là khóa của John, nhưng trong thực tế lại là khóa của Katie,
3. Katie giờ đây đã có thể đọc được thông điệp từ Diane đang được mã hóa và gửi cho John.
4. Sau khi Katie giải mã và đọc thông điệp của Diane, cô ta lại mã hóa bằng khóa công khai của John và gửi nó cho anh ấy để anh ấy không nhận ra.

**Hình 25-1** Khi không có PKI, các cá nhân có thể giả mạo danh tính của những người khác, một cuộc tấn công người-trung-gian.

Trong các môi trường PKI, các thực thể được gọi là cơ quan đăng ký (RAs) và cơ quan chứng nhận (CAs) cung cấp các dịch vụ tương tự như những dịch vụ của Cục Xe Cơ giới Hoa Kỳ (Department of Motor Vehicles - DMV). Khi John đi đăng ký giấy phép lái xe, anh ta phải chứng minh danh tính của mình với DMV bằng cách cung cấp hộ chiếu, giấy khai sinh hoặc các tài liệu nhận dạng khác. Nếu DMV hài lòng với bằng chứng mà John cung cấp (và John vượt qua được bài kiểm tra lái xe), DMV sẽ tạo ra bằng lái xe để John có thể sử dụng để chứng minh danh tính của mình. Bất cứ khi nào John cần phải xác định danh tính của mình, anh ấy có thể xuất trình bằng lái xe của mình. Mặc dù nhiều người có thể không tin tưởng John xác định sự thật về bản thân anh ấy nhưng họ tin tưởng vào bên-thứ-ba, DMV.

Trong bối cảnh PKI, mặc dù một số biến thể tồn tại trong các sản phẩm cụ thể nhưng RA sẽ yêu cầu bằng chứng nhận dạng từ cá nhân đang yêu cầu một chứng nhận và sẽ xác thực thông tin này. Sau đó RA sẽ thông báo cho CA để tạo chứng nhận, chứng nhận này tương tự như bằng lái xe. CA sẽ ký số vào chứng nhận bằng khóa riêng của nó. Việc sử dụng khóa riêng tư đảm bảo với người nhận rằng chứng chỉ đến từ CA. Khi Diane nhận được chứng nhận của John và xác minh rằng nó thực sự được ký điện tử bởi một CA mà cô ấy tin tưởng, cô ấy sẽ tin rằng chứng chỉ đó thực sự là của John - không phải vì cô ấy tin tưởng John, mà bởi vì cô ấy tin tưởng tổ chức đang xác minh danh tính của John ( CA).

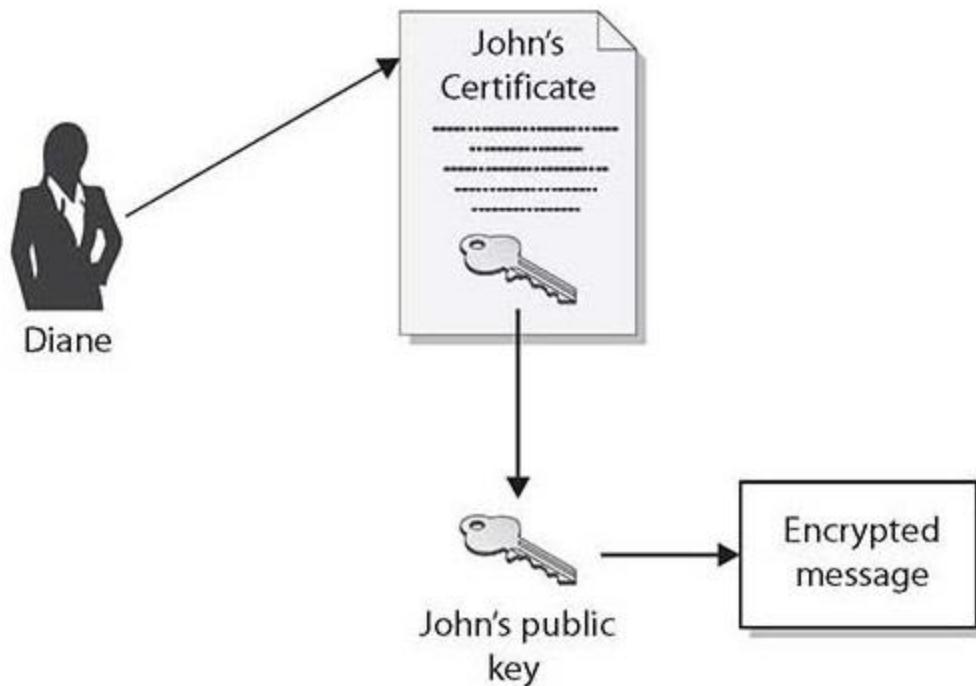


**MÁCH NƯỚC CHO KỲ THI** Một cơ quan đăng ký (RA) xác minh các yêu cầu chứng nhận kỹ thuật số và chuyển chúng cho một cơ quan cấp

chứng nhận (CA). CA là một tổ chức đáng tin cậy xác thực và cấp các chứng nhận kỹ thuật số.

Đây thường được gọi là *mô hình tin cậy bên-thứ-ba*. Các khóa công khai là những thành phần của các chứng nhận kỹ thuật số, vì vậy, khi Diane xác minh chữ ký kỹ thuật số của CA, điều này sẽ xác minh rằng chứng nhận đó thực sự là của John's và khóa công khai mà chứng chỉ đang chứa cũng là của John. Đây là cách mà danh tính của John được liên kết với khóa công khai của anh ấy.

Quá trình này cho phép John xác thực bản thân với Diane và những người khác. Bằng cách sử dụng chứng nhận của bên-thứ-ba, John có thể giao tiếp với cô ấy, sử dụng mã hóa khóa công khai mà không cần giao tiếp trước hoặc có mối quan hệ từ trước. Khi Diane bị thuyết phục về tính hợp pháp của khóa công khai của John, cô ấy có thể sử dụng nó để mã hóa và giải mã các thông điệp giữa mình và John, như được minh họa trong Hình 25-2.



1. Diane xác minh chứng nhận
2. Diane trích xuất khóa công khai của John
3. Diane sử dụng khóa công khai của John cho mục đích mã hóa.

**Hình 25-2** Các khóa công khai là những thành phần của các chứng nhận kỹ thuật số

### Quản lý Khóa

Một loạt các ứng dụng và giao thức có thể tạo ra các cặp khóa công khai/khóa riêng tư và cung cấp chức năng tương tự như những gì PKI cung cấp, nhưng không có bên thứ ba đáng tin cậy nào khả dụng cho cả hai bên giao tiếp. Để mỗi bên chọn giao tiếp theo cách này mà không cần bên thứ ba xác nhận danh tính của người kia, cả hai phải chọn tin tưởng lẫn nhau và tin vào kênh giao tiếp mà họ đang sử dụng. Trong nhiều tình huống, việc tin tưởng một cách tùy tiện vào một cá nhân mà bạn không biết là không thực tế và rất nguy hiểm, và đây là lúc các thành phần của

PKI phải được đặt đúng vị trí - để cung cấp mức độ tin cậy cần thiết mà bạn không thể cung cấp hoặc chọn không cung cấp bởi chính mình.

“Cơ sở hạ tầng” trong “cơ sở hạ tầng khóa công khai” thực sự có nghĩa là gì? Một cơ sở hạ tầng cung cấp một nền tảng bền vững để những thứ khác có thể được xây dựng trên đó. Vì vậy, một cơ sở hạ tầng hoạt động ở cấp thấp để cung cấp một môi trường đồng nhất và có thể dự đoán được để cho phép những công nghệ khác ở cấp-độ-cao-hơn hoạt động cùng nhau thông qua các điểm truy cập thống nhất. Môi trường mà cơ sở hạ tầng cung cấp cho phép các ứng dụng cấp-cao-hơn này giao tiếp với nhau và cung cấp cho chúng các công cụ cơ bản để thực hiện các nhiệm vụ của chúng.



**MÁCH NƯỚC CHO KỲ THI** Hãy đảm bảo rằng bạn hiểu về vai trò của PKI trong việc quản lý các chứng nhận và sự tin cậy liên quan đến các khóa công khai.

### Quản lý Khóa

Toàn bộ mục đích của PKI là cung cấp cấu trúc và các thành phần cần thiết cho một tổ chức để quản lý các khóa mật mã cần được chia sẻ giữa các thực thể. Một khóa kỹ thuật số chỉ là một con số kỹ thuật số, chỉ đơn giản là dữ liệu. Các phần tử siêu dữ liệu về khóa - ai đã tạo ra chúng, chúng được sử dụng để làm gì, chúng có giá trị trong bao lâu và một loạt các câu hỏi khác - cần được lưu trữ cùng với khóa. Do đó, việc phát minh ra chứng nhận, là một tập tin văn bản đơn giản chứa thông tin quan trọng về khóa [*câu này hơi thiếu ý – người dịch*]. Ngoài siêu dữ liệu này, các yếu tố quan trọng khác xoay quanh việc quản lý khóa bao gồm các chính sách về bảo vệ khóa, lưu trữ, giao kèo khóa và khôi phục khóa. Các khóa mật mã rất quan trọng và trọng yếu đối với các giải pháp mật mã đang

hoạt động trong một doanh nghiệp. Một số khóa cần phải được chia sẻ để có hiệu quả, những khóa khác lại cần được giữ kín. Quản lý khóa là tập hợp các hoạt động mà một tổ chức phải thực hiện để đảm bảo rằng các khóa hỗ trợ mật mã phù hợp và không gây ra các vấn đề về bảo mật.



**LƯU Ý** Tính bảo mật liên quan đến việc sử dụng mật mã khóa công khai xoay quanh tính bảo mật của khóa công khai. Không khước từ phụ thuộc vào nguyên tắc rằng khóa riêng tư chỉ có thể được truy cập bởi người giữ khóa. Nếu một người khác có quyền truy cập vào khóa riêng tư, họ có thể mạo danh người giữ khóa hợp lệ.

### **Cơ quan cấp Chứng nhận (CA)**

Như đã được mô tả trước đây, *cơ quan cấp chứng nhận (CA)* là cơ quan đáng tin cậy xác nhận danh tính của các cá nhân và tạo ra các tài liệu điện tử chỉ ra rằng các cá nhân là chính họ. Tài liệu điện tử này được gọi là *chứng nhận kỹ thuật số* và nó thiết lập mối liên kết giữa danh tính của chủ thẻ và một khóa công khai. Khóa riêng tư được ghép nối với khóa công khai trong chứng nhận được lưu trữ một cách riêng biệt.

Tuy nhiên, CA còn nhiều hơn một phần của phần mềm, nó thực sự được tạo thành từ phần mềm, phần cứng, các thủ tục, chính sách và những người liên quan đến việc xác thực danh tính của các cá nhân và tạo ra các chứng nhận. Điều này có nghĩa rằng nếu một trong những thành phần này bị xâm phạm, nó có thể sẽ ảnh hưởng tiêu cực đến CA tổng thể và có thể đe dọa tính toàn vẹn của các chứng nhận mà nó tạo ra.

Mọi CA nên có một tuyên bố về thực hành chứng nhận (certification practices statement - CPS) nêu rõ cách thức xác minh danh tính, các bước mà CA tuân theo để tạo ra, duy trì và truyền tải các chứng chỉ, và lý do

tại sao CA có thể được tin tưởng để hoàn thành trách nhiệm của mình. Nó mô tả cách các khóa được bảo mật, dữ liệu nào được đặt trong chứng chỉ kỹ thuật số và cách xử lý việc thu hồi [chứng chỉ]. Nếu một công ty sẽ sử dụng và phụ thuộc vào một CA công cộng, các nhân viên bảo mật, quản trị viên và bộ phận pháp lý của công ty nên xem xét toàn bộ CPS của CA để đảm bảo rằng nó sẽ đáp ứng đúng nhu cầu của công ty và để đảm bảo rằng mức độ bảo mật được CA tuyên bố là đủ cao cho việc sử dụng và môi trường của chúng. Một khía cạnh quan trọng của PKI là sự tin cậy giữa người dùng và CA, do đó, CPS nên được xem xét và được hiểu rõ để đảm bảo rằng mức độ tin cậy này được đảm bảo.

Máy chủ chứng nhận là dịch vụ thực tế cấp chứng nhận dựa trên dữ liệu được cung cấp trong quá trình đăng ký ban đầu. Máy chủ xây dựng và điền vào chứng nhận kỹ thuật số những thông tin cần thiết và kết hợp khóa công khai của người dùng với chứng nhận kết quả. Sau đó, chứng nhận được ký kỹ thuật số bằng khóa riêng tư của CA.

### **CA Trung gian**

Các *CA trung gian* hoạt động để chuyển sự tin cậy giữa các CA khác nhau. Những CA này cũng được gọi là một CA cấp dưới bởi vì chúng là cấp dưới của CA mà chúng tham chiếu. Con đường tin cậy được đi lên từ CA cấp dưới đến CA cấp-cao-hơn, về bản chất, CA cấp dưới đang sử dụng CA cấp-cao-hơn như là một điểm tham chiếu.

### **Cơ quan Đăng ký (RA)**

Một *cơ quan đăng ký (RA)* là thành phần PKI chấp nhận một yêu cầu chứng nhận kỹ thuật số và thực hiện các bước cần thiết để đăng ký và xác thực người đang yêu cầu chứng nhận. Các yêu cầu xác thực sẽ khác nhau tùy thuộc vào loại chứng nhận được yêu cầu. Hầu hết các CA đều cung cấp một loạt các lớp chứng nhận với độ tin cậy ngày càng gia tăng theo từng lớp.

Mỗi lớp chứng nhận cao hơn có thể thực hiện nhiều tác vụ quan trọng và mạnh mẽ hơn loại chứng nhận lớp bên dưới. Đây là lý do tại sao các lớp khác nhau sẽ có các yêu cầu khác nhau về bằng chứng nhận dạng. Nếu bạn muốn nhận chứng nhận Hạng 1, bạn có thể chỉ được yêu cầu cung cấp tên, địa chỉ email và địa chỉ thực của bạn. Đối với chứng nhận Hạng 2, bạn có thể cần cung cấp cho RA nhiều dữ liệu hơn, chẳng hạn như bằng lái xe, hộ chiếu và thông tin công ty có thể xác minh được. Để có được chứng nhận Lớp 3, bạn sẽ được yêu cầu cung cấp thêm thông tin và rất có thể bạn sẽ phải đến văn phòng của RA để gặp mặt trực-tiếp. Mỗi CA sẽ phác thảo các lớp chứng nhận mà nó cung cấp và các yêu cầu nhận dạng phải được đáp ứng để có được mỗi loại chứng chỉ.

### **Danh sách Thu hồi Chứng nhận (CRL)**

CA cung cấp khả năng bảo vệ chống lại các chứng nhận xấu bằng cách duy trì một *danh sách thu hồi chứng chỉ (CRL)*, một danh sách bao gồm các số sê-ri của những chứng nhận đã bị thu hồi. CRL cũng chứa một tuyên bố cho biết lý do tại sao các chứng nhận riêng lẻ bị thu hồi và ngày diễn ra việc thu hồi. Danh sách này thường chứa tất cả các chứng nhận đã bị thu hồi trong vòng đời của CA. Các chứng nhận đã hết hạn sẽ khác với chứng chỉ đã bị thu hồi. Nếu một chứng nhận đã hết hạn, điều đó có nghĩa là chứng nhận đó đã đến ngày hiệu lực cuối cùng.

CA là thực thể chịu trách nhiệm về trạng thái của các chứng nhận mà nó tạo ra, nó cần được thông báo về việc thu hồi và nó phải cung cấp thông tin này cho những người khác. CA chịu trách nhiệm duy trì CRL và đăng nó trong một thư mục có sẵn công khai.



### **MÁCH NƯỚC CHO KỲ THI**

Danh sách thu hồi chứng nhận là một mục thiết yếu để đảm bảo rằng một chứng nhận vẫn còn hiệu lực. CA đăng

các CRL trong các danh bạ công khai để cho phép việc kiểm tra được tự động hóa về các chứng nhận so với danh sách trước khi chứng nhận được sử dụng bởi một máy khách. Một người dùng không bao giờ nên tin tưởng vào một chứng nhận đã không được kiểm tra so với một CRL thích hợp.

Điều gì sẽ xảy ra nếu Stacy muốn trả thù Joe vì điều gì đó và cô ấy cố gắng thu hồi chứng nhận của Joe? Nếu cô ấy thành công, việc Joe tham gia PKI sẽ có thể bị ảnh hưởng một cách tiêu cực vì những người khác sẽ không còn tin tưởng vào khóa công khai của anh ấy. Mặc dù chúng ta có thể nghĩ rằng Joe xứng đáng với điều này, nhưng chúng ta cần có một số hệ thống để đảm bảo mọi người không thể tự ý thu hồi chứng nhận của người khác, cho dù là để trả thù hay vì mục đích xấu.

Khi yêu cầu thu hồi [chứng nhận] được đệ trình, cá nhân gửi yêu cầu cũng phải được xác thực. Nếu không, điều này có thể cho phép một kẻ tấn công từ-chối-dịch-vụ, trong đó một ai đó đã thu hồi chứng nhận của người khác. Quá trình xác thực có thể liên quan đến mật khẩu đã-thỏa-thuận được tạo trong quá trình đăng ký, nhưng quá trình xác thực không chỉ được dựa trên việc cá nhân chứng minh rằng anh ta có khóa cá nhân tương ứng, vì nó có thể đã bị đánh cắp và CA sẽ xác thực cho một kẻ mạo danh.

Tính toàn vẹn của CRL cần phải được bảo vệ để đảm bảo rằng những kẻ tấn công không thể sửa đổi dữ liệu liên quan đến một chứng nhận đã bị thu hồi từ danh sách. Nếu điều này được phép xảy ra, bất kỳ ai lấy cắp được một khóa riêng tư chỉ có thể xóa khóa đó khỏi CRL và tiếp tục sử dụng khóa riêng một cách gian lận. Tính toàn vẹn của danh sách cũng cần phải được bảo vệ để đảm bảo rằng dữ liệu không có thật sẽ không được thêm vào đó. Nếu không, bất kỳ ai cũng có thể thêm chứng nhận của người khác vào danh sách và thu hồi chứng nhận của người đó một

cách hiệu quả. Thực thể duy nhất có thể sửa đổi bất kỳ thông tin nào trên CRL là CA.

Cơ chế được sử dụng để bảo vệ tính toàn vẹn của một CRL là một *chữ ký kỹ thuật số*. Dịch vụ thu hồi của CA tạo ra một chữ ký kỹ thuật số cho CRL. Để xác minh một chứng nhận, người dùng truy cập vào danh bạ nơi CRL đã được đăng, tải danh sách về, và xác thực chữ ký kỹ thuật số của CA để đảm bảo rằng cơ quan có thẩm quyền thích hợp đã ký vào danh sách và để đảm bảo rằng danh sách đã không bị sửa đổi theo cách trái phép. Sau đó, người dùng xem qua danh sách để xác định xem số sê-ri của chứng nhận mà anh ta đang cố gắng xác thực có được liệt kê hay không. Nếu số sê-ri nằm trong danh sách, khóa riêng tư sẽ không còn đáng tin cậy nữa và khóa công khai cũng sẽ không nên được sử dụng nữa.

Một mối quan tâm là làm thế nào để cập nhật CRL - tần suất nó được cập nhật và nó có thực sự phản ánh *mọi* chứng nhận hiện đang bị thu hồi không? Tần suất thực tế mà theo đó danh sách được cập nhật sẽ phụ thuộc vào CA và CPS của nó. Điều quan trọng là danh sách được cập nhật một cách kịp thời để bất kỳ ai sử dụng danh sách đều có được thông tin mới nhất. Các tập tin CRL có thể được yêu cầu bởi những cá nhân cần xác minh và xác thực chứng nhận mới nhận được hoặc các tập tin có thể được định kỳ đẩy xuống (gửi) cho tất cả người dùng đang tham gia vào một PKI cụ thể. Điều này có nghĩa là CRL có thể được kéo (tải xuống) bởi người dùng cá nhân khi cần thiết hoặc được đẩy xuống cho tất cả người dùng trong PKI theo một khoảng thời gian định sẵn.

Tập tin CRL thực tế có thể phát triển một cách đáng kể và việc truyền tập tin này và yêu cầu phần mềm khách PKI trên mỗi máy trạm để lưu và duy trì nó có thể sử dụng khá nhiều tài nguyên, do đó, CRL càng nhỏ càng tốt. Trước tiên cũng có thể đẩy CRL đầy đủ xuống và sau lần tải

đầu tiên đó, các CRL sau đó được đẩy xuống người dùng là CRL delta, nghĩa là chúng chỉ chứa các thay đổi đối với CRL gốc hoặc cơ sở. Điều này có thể làm giảm đáng kể lượng băng thông tiêu thụ khi cập nhật CRLs.

Trong các triển khai khi mà CRL không được đẩy xuống các hệ thống riêng lẻ, phần mềm PKI của người dùng cần phải biết nơi để tìm kiếm CRL đã được đăng liên quan đến chứng nhận mà nó đang cỗ gắng xác thực. Chứng nhận có thể có phần mở rộng trả người dùng đang xác thực đến điểm phân phối CRL cần thiết. Quản trị viên mạng thiết lập các điểm phân phối và một hoặc nhiều điểm có thể tồn tại cho một PKI cụ thể. Điểm phân phối giữ một hoặc nhiều danh sách chứa các số sê-ri của chứng nhận đã bị thu hồi và phần mềm PKI của người dùng quét (các) danh sách để tìm số sê-ri của chứng nhận mà người dùng đang cỗ gắng xác thực. Nếu số sê-ri không hiện diện [trong (các) danh sách], người dùng yên tâm rằng nó vẫn chưa bị thu hồi. Phương pháp tiếp cận này giúp hướng người dùng đến đúng tài nguyên và cũng làm giảm lượng thông tin cần được quét khi kiểm tra rằng chứng nhận chưa bị thu hồi.

Một tùy chọn cuối cùng để kiểm tra CRL đã được phân phối là một dịch vụ trực tuyến. Khi một người dùng máy khách cần xác thực chứng nhận và đảm bảo rằng chứng nhận đó chưa bị thu hồi, anh ta có thể giao tiếp với một dịch vụ trực tuyến sẽ truy vấn các CRL cần thiết đang sẵn có trong môi trường. Dịch vụ này có thể truy vấn các danh sách cho máy khách thay vì đẩy toàn bộ CRL xuống từng hệ thống. Vì vậy, nếu Alice nhận được chứng nhận từ Bob, cô ấy có thể liên hệ với một dịch vụ trực tuyến và gửi cho nó số sê-ri được liệt kê trong chứng nhận mà Bob đã gửi. Dịch vụ trực tuyến sẽ truy vấn CRLs cần thiết và trả lời Alice bằng cách cho biết số sê-ri đó có được liệt kê là đã bị thu hồi hay không.

## Các Thuộc tính của Chứng nhận

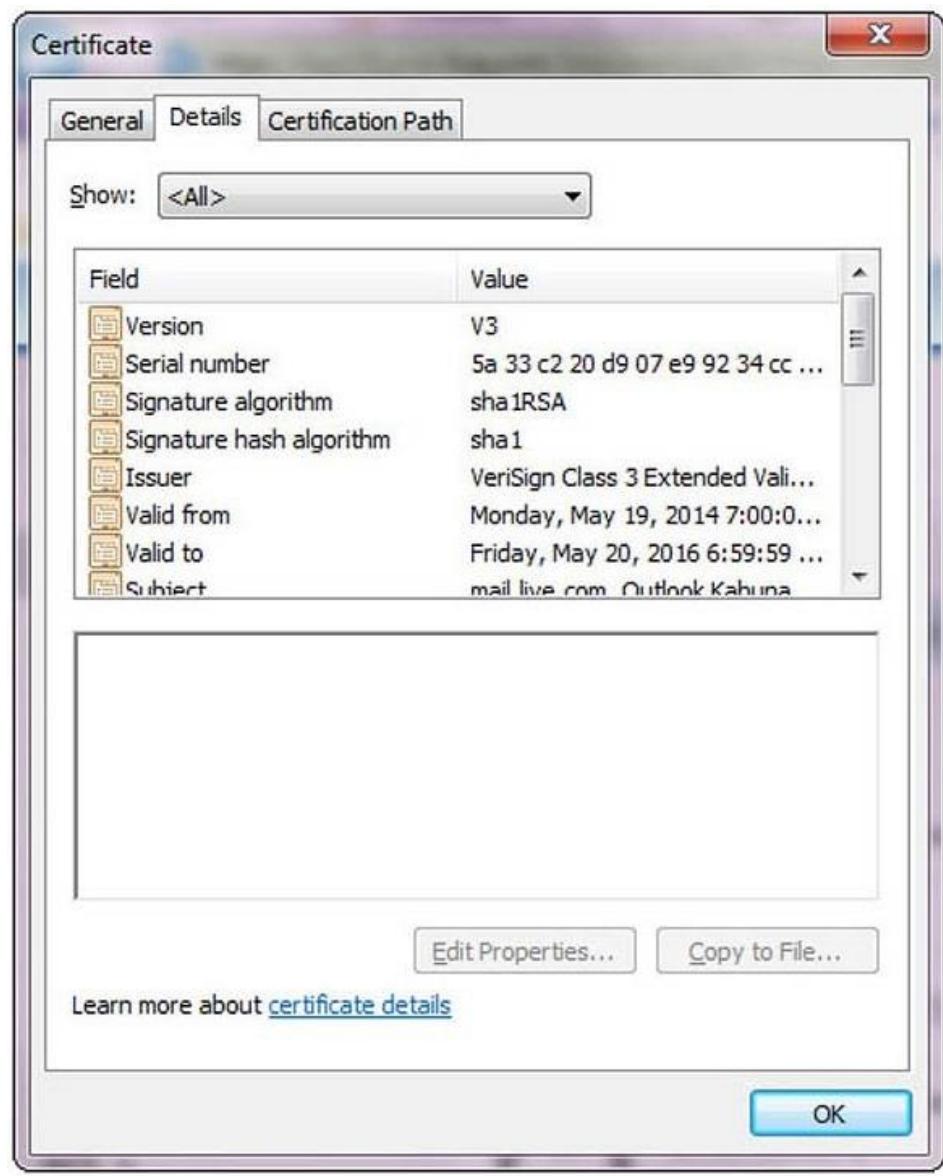
Một chứng nhận kỹ thuật số liên kết danh tính của một cá nhân với một khóa công khai và nó chứa tất cả thông tin mà người nhận cần để đảm bảo chắc chắn về danh tính của chủ sở hữu khóa công khai. Các chứng nhận được tạo ra và định dạng dựa trên tiêu chuẩn X.509, tiêu chuẩn này xác định các trường cần thiết của một chứng nhận và các giá trị khả thi có thể được chèn vào các trường. Phiên bản mới nhất của X.509 là v3 và các trường mà nó chứa được mô tả trong Bảng 25-1.

Tên Trường	Mô tả Trường
Phiên bản Chứng nhận	Phiên bản X509 được sử dụng cho chứng nhận này Phiên bản 1 = 0 Phiên bản 2 = 1 Phiên bản 3 = 2
Số sê-ri	Một số nguyên lớn hơn hoặc bằng 0 được chỉ định bởi người phát hành chứng nhận và phải là duy nhất đối với chứng nhận.
Chữ ký Thuật toán Các tham số (tùy chọn)	Mã định danh thuật toán cho thuật toán được sử dụng bởi CA để ký vào chứng nhận. Các Tham số là tùy chọn được sử dụng để cung cấp các tham số thuật toán mật mã được sử dụng trong việc tạo ra chữ ký.
Người phát hành	Xác định thực thể đã ký và phát hành chứng nhận. Đây phải là một Tên Phân biệt trong sơ đồ phân cấp cấu trúc của CA.
Hiệu lực Không có hiệu lực trước thời điểm Không có hiệu lực sau thời điểm	Định một khoảng thời gian mà theo đó, chứng nhận vẫn có hiệu lực, sử dụng một thời điểm "không có hiệu lực trước khi" và một thời điểm "không có hiệu lực sau khi" (đã được nêu cụ thể trong UTC hay trong một thời gian tổng quát).

Chủ thể	Tên Phân biệt của chủ sở hữu chứng nhận. Tên gọi này có thể chứa Tên Phổ biến và các phần tử khác, chứng hạn như: Tổ chức, Vị trí, Bang, Quốc gia, CN=*.google.com, O = Google LLC, L = Mountain View, S = California, C = US.
Thông tin Khóa Công khai của Chủ thể	Một mã định danh thuật toán mã hóa tiếp theo là một chuỗi-bit dành cho khóa công khai.
ID Duy nhất của Nhà phát hành	Tùy chọn dành cho phiên bản 2 và 3. Đây là một mã định danh chuỗi-bit dành cho CA đã phát hành chứng nhận.
ID Duy nhất của Chủ thể	Tùy chọn dành cho phiên bản 2 và 3. Đây là một mã định danh chuỗi-bit dành cho chủ thể của đã phát hành chứng nhận.
Phần mở rộng  Mã Mở rộng  Phần mở rộng Quan trọng  Giá trị	Tùy chọn dành cho phiên bản 2 và 3. Khu vực Mở rộng bao gồm một chuỗi các trường mở rộng có chứa một mã định danh phần mở rộng, một trường Boolean chỉ ra rằng liệu phần mở rộng có quan trọng không, và một chuỗi octet trình bày giá trị của phần mở rộng. Các phần mở rộng có thể được xác định trong các tiêu chuẩn hoặc được định nghĩa và đăng ký bởi tổ chức hoặc cộng đồng.
Thuật toán Dấu ấn chỉ  Thuật toán  Tham số (tùy chọn)	Xác định thuật toán được sử dụng bởi CA để ký vào chứng nhận. Trường này phải khớp với thuật toán đã được xác định trong trường Thuật toán Chữ ký.
Dấu ấn Chỉ	Chữ ký là một giá trị băm chuỗi-bit có được khi CA ký vào chứng nhận. Chữ ký chứng nhận cho nội dung của chứng nhận, ràng buộc khóa công khai với chủ sở hữu.

**Bảng 25-1** Các trường Chứng nhận X.509

Hình 25-3 minh họa cho giá trị thực tế của các trường chứng nhận khác nhau đối với một chứng nhận cụ thể. Phiên bản của chứng nhận này là v3 (X.509 v3) và số sê-ri cũng được liệt kê – con số này là duy nhất đối với từng chứng nhận được tạo ra bởi một CA cụ thể. CA sử dụng thuật toán băm SHA-1 để tạo ra giá trị đồng hóa thông điệp và sau đó ký vào nó bằng cách sử dụng khóa riêng tư của CA sử dụng thuật toán RSA.



**Hình 25-3** Các trường trong một chứng nhận kỹ thuật số

## Giao thức Trạng thái Chứng nhận Trực tuyến (OCSP)

Một trong những giao thức được sử dụng cho các dịch vụ thu hồi [chứng nhận] trực tuyến là *Giao thức Trạng thái Chứng nhận Trực tuyến (Online Certificate Status Protocol - OCSP)*, một giao thức yêu cầu và phản hồi lấy số sê-ri của chứng nhận đang được xác thực và xem xét các CRL cho máy khách. Giao thức có một dịch vụ phản hồi để báo cáo trạng thái của chứng nhận trả lại cho máy khách, cho biết liệu nó [chứng nhận] đã bị thu hồi, có hợp lệ hay không hay trạng thái của nó là không xác định. Giao thức và dịch vụ này giúp máy khách tìm kiếm, tải xuống và xử lý các danh sách phù hợp.



## MÁCH NƯỚC CHO KỲ THI

Kiểm tra sự thu hồi chứng nhận được thực hiện bằng cách kiểm tra CRL hoặc sử dụng OSCP để xem liệu một chứng nhận đã bị thu hồi hay chưa.

## Yêu cầu Ký Chứng nhận (CSR)

Một *yêu cầu ký chứng nhận (certificate signing request – CSR)* là một yêu cầu thực tế cho một CA có chứa khoá công khai và những thông tin cần thiết để tạo ra chứng nhận. CSR chứa mọi thông tin nhận dạng được liên kết với khóa bằng quy trình tạo-chứng-nhận.

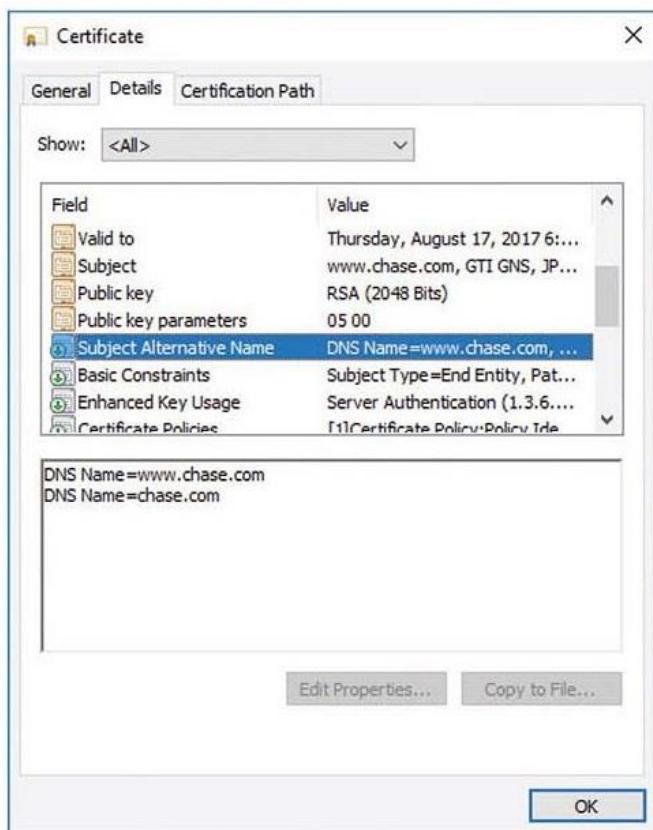
## CN

Trường *Tên Chung (Common Name - CN)* được thể hiện trong trường Chủ thể của chứng chỉ và là tên miền đủ điều kiện (fully qualified domain name - FQDN) để chứng chỉ hợp lệ. Phần trình bày chung trong dòng chủ thể của chứng chỉ có thể chứa Tên Chung và các thành phần khác, chẳng hạn như Tổ chức, Vị trí, Tiểu bang và Quốc gia: CN = \* .google.com, O = Google LLC, L = Mountain View, S = California, C = Hoa Kỳ. O là tổ chức, L là địa điểm, S là tiểu bang và C là quốc gia.

Tên phân biệt (distinguished name - DN) là một thuật ngữ mô tả thông tin nhận dạng trong một chứng nhận và là một phần của chính chứng nhận đó. Chứng nhận chứa thông tin DN cho cả chủ sở hữu hoặc người yêu cầu chứng nhận (được gọi là Chủ thể DN) và CA cấp chứng chỉ (được gọi là DN của người cấp).

### **Tên Thay thế Chủ thể (SAN)**

Tên thay thế chủ đề (subject alternative name - SAN) là một trường (phần mở rộng) trong chứng nhận có một số mục đích sử dụng. Trong các chứng nhận dành cho máy, nó có thể đại diện cho FQDN của máy. Đối với người dùng, nó có thể là tên chính của người dùng (user principal name - UPN) hoặc trong trường hợp chứng chỉ SSL, nó có thể chỉ ra nhiều miền mà chứng chỉ hợp lệ qua các miền đó. Hình 25-4 cho thấy nhiều miền được bao hàm bởi chứng chỉ trong hộp bên dưới các chi tiết trường. SAN là một phần mở rộng được sử dụng ở một mức độ đáng kể, vì nó đã trở thành một phương pháp tiêu chuẩn được sử dụng trong rất nhiều trường hợp.



**Hình 25-4** Tên Thay thế Chủ thẻ



### LƯU Ý

Các chứng nhận SAN cho phép bạn bảo mật một miền chính và sau đó bổ sung thêm các miền phụ vào trường Tên Thay thế Chủ thẻ của chứng nhận. Ví dụ, bạn có thể bảo mật tất cả những miền nay chỉ với một chứng nhận SAN duy nhất:

- [www.example.com](http://www.example.com)
- [email.exapamle.com](http://email.exapamle.com)
- [intranet.example.com](http://intranet.example.com)
- [www.example.net](http://www.example.net)

Thông tin thêm về Tên Thay thế Chủ thể và các chứng nhận sẽ được trình bày trong các phần sau.

### **Thời hạn**

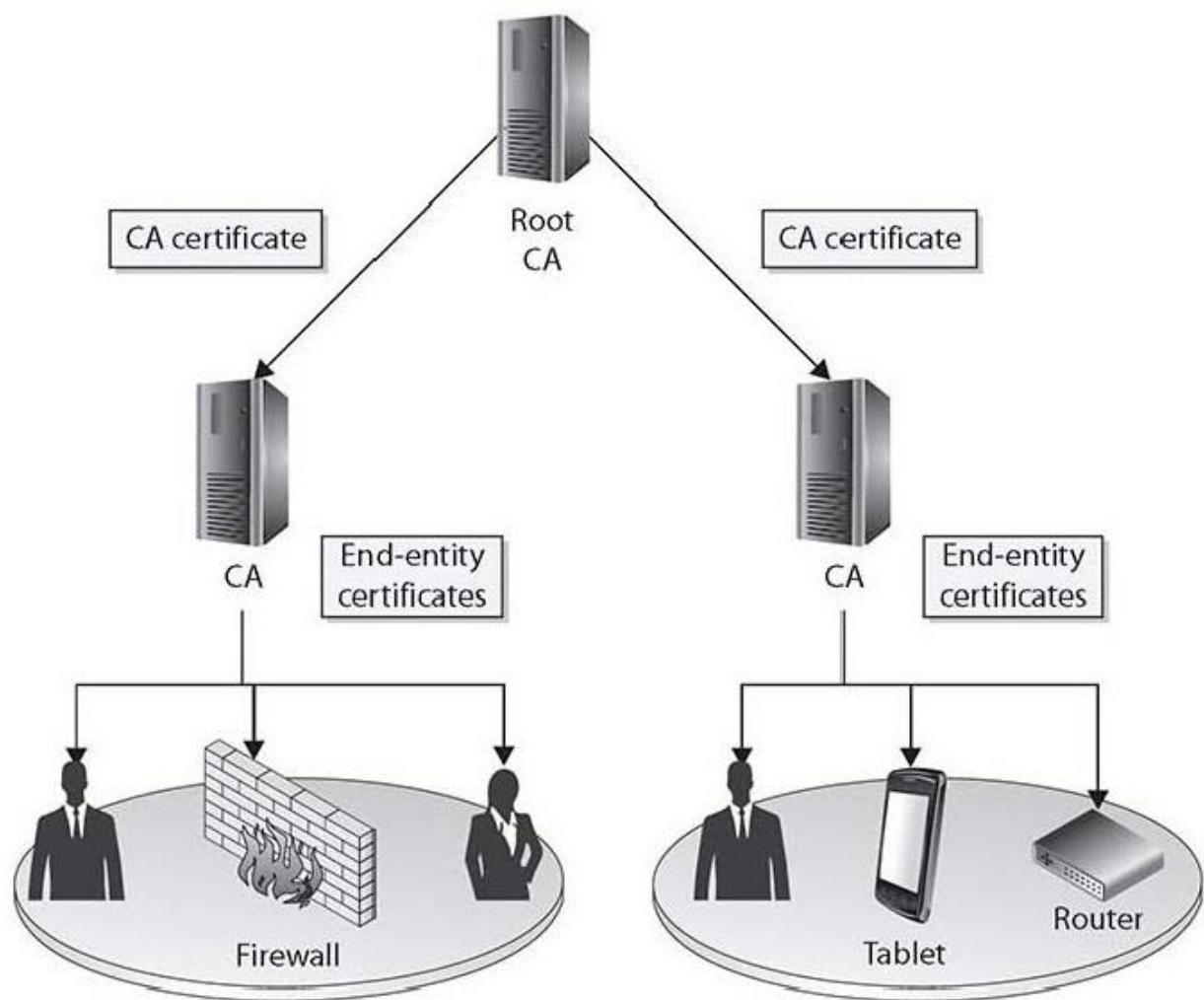
Bản thân một chứng nhận có thời gian tồn tại có thể khác với thời gian tồn tại của cặp khóa. Thời gian tồn tại của chứng nhận được xác định theo ngày hiệu lực được chèn vào chứng nhận kỹ thuật số. Đây là những ngày bắt đầu và ngày kết thúc cho biết khoảng thời gian mà chứng chỉ có hiệu lực. Không thể sử dụng chứng chỉ trước ngày bắt đầu và sau khi đã đến ngày kết thúc, chứng nhận sẽ hết hạn và cần phải cấp lại chứng nhận mới. Xem xét Hình 25-3 ở phần trước trong chương, bạn có thể nói gì về tình trạng của chứng chỉ này?

### **Các kiểu Chứng nhận**

Có 4 kiểu chứng nhận được sử dụng:

- Các chứng nhận thực-thể-đầu-cuối,
- Các chứng nhận CA,
- Các chứng nhận chứng-nhận-chéo,
- Các chứng nhận chính sách.

Các *chứng nhận thực-thể-đầu-cuối* được cấp bởi một CA cho một chủ thể cụ thể, chẳng hạn như Joyce, phòng Kế toán, hoặc một tường lửa, như được minh họa trong Hình 25-5. Một chứng nhận thực-thể-đầu-cuối là một tài liệu nhận dạng được cung cấp bởi các triển khai PKI.



**Hình 25-5** Các chứng nhận thực-thể-đầu-cuối và chứng nhận CA

Một *chứng nhận CA* có thể được tự-ký (self-signed), trong trường hợp một CA độc lập hoặc CA gốc (root), hoặc nó có thể được cấp bởi một CA cấp trên trong một mô hình phân cấp. Trong mô hình được minh họa trong Hình 25-5, CA cấp trên cấp quyền và cho phép CA cấp dưới chấp thuận các yêu cầu chứng nhận và tự tạo ra các chứng nhận riêng lẻ. Đây có thể là điều cần thiết khi một công ty cần có nhiều CA nội bộ và các bộ phận khác nhau trong tổ chức cần có CA riêng phục vụ các thực-thể-đầu-cuối cụ thể (người dùng, các thiết bị mạng và ứng dụng) trong các bộ phận của họ. Trong những tình huống này, một đại diện từ mỗi bộ phận

yêu cầu CA đăng ký với CA đáng tin cậy hơn và yêu cầu một chứng nhận CA.

Chứng nhận chứng-nhận-chéo, hoặc chứng-nhận-chéo, được sử dụng khi các CA độc lập thiết lập mối quan hệ tin cậy ngang-hàng. Nói một cách đơn giản, chúng là một cơ chế mà qua đó một CA có thể cấp chứng chỉ cho phép người dùng của nó tin tưởng một CA khác.

Trong các CA tinh vi được sử dụng cho các ứng dụng bảo-mật-cao, một cơ chế là cần thiết để cung cấp thông tin chính sách được kiểm soát tập trung cho các máy khách PKI. Điều này thường được thực hiện bằng cách đặt thông tin chính sách vào trong một *chứng chỉ chính sách*.

### Các Chứng nhận Wildcard

Chứng nhận có thể được cấp cho một thực thể chẵng hạn như example.com. Nhưng điều gì sẽ xảy ra nếu có nhiều thực thể khác trong example.com cần chứng nhận? Sẽ có hai sự lựa chọn: (1) cấp chứng nhận riêng biệt cho từng địa chỉ cụ thể hoặc (2) sử dụng chứng nhận ký tự đại diện (wildcard). Chứng nhận ký tự đại diện hoạt động một cách chính xác đúng như người ta mong đợi. Chứng chỉ được cấp cho \*.example.com sẽ hợp lệ cho one.example.com cũng như two.example.com.

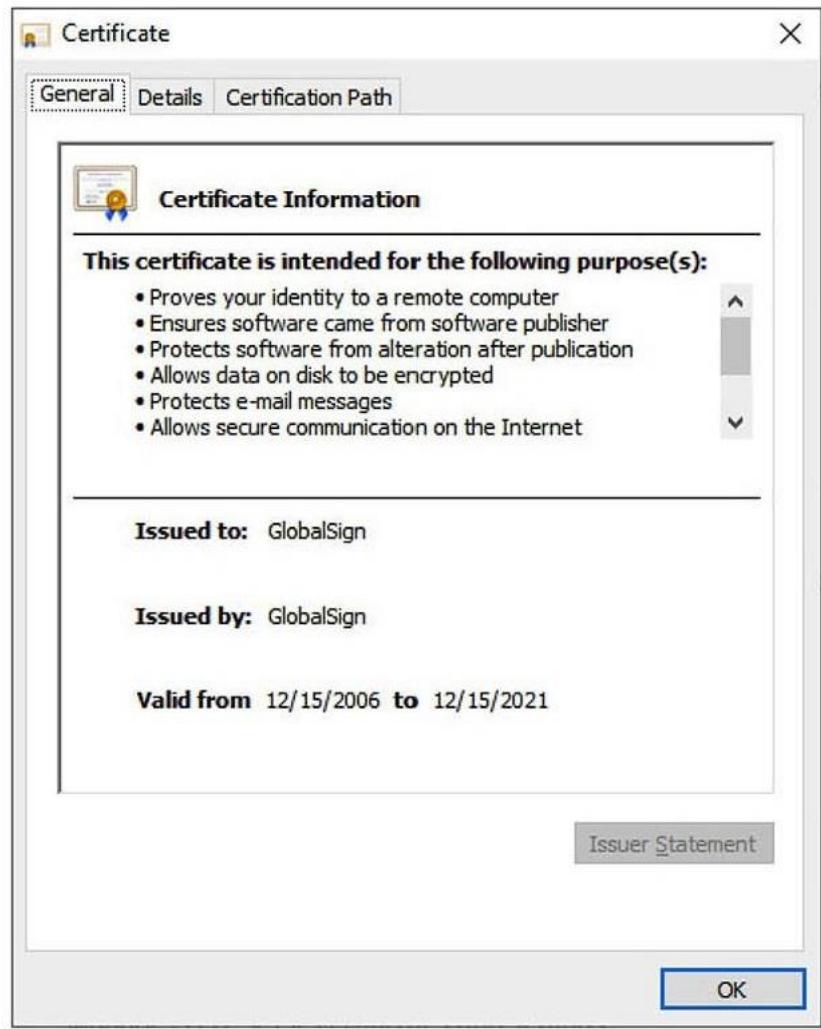


**MÁCH NƯỚC CHO KỲ THI** Các chứng nhận ký tự đại diện bao gồm một dấu hoa thị và khoảng trắng trước tên miền. Các chứng nhận SSL thường mở rộng mã hóa cho các tên miền phụ thông qua việc sử dụng ký tự thay thế.

### Tên Thay thế Chủ thể (SAN)

Như đã được đề cập trước đây trong chương, *Tên Thay thế Chủ thể* (*Subject Alternative Name – SAN*) là một trường (mở rộng) trong một

chứng nhận có nhiều cách sử dụng. Trong những chứng nhận dành cho các máy, nó có thể đại diện cho tên miền đầy đủ điều kiện (FQDN) của máy, đối với người dùng, nó có thể là tên chính của người dùng (user principal name – UPN). Trong trường hợp một chứng nhận SSL, nó có thể chỉ ra nhiều miền mà chứng nhận có hiệu lực. Hình 25-6 cho thấy hai miền được bao hàm bởi chứng nhận trong hộp bên dưới chi tiết Trường. SAN là một phần mở rộng được sử dụng ở một mức độ đáng kể vì nó đã trở thành một phương pháp tiêu chuẩn được sử dụng trong nhiều trường hợp khác nhau.



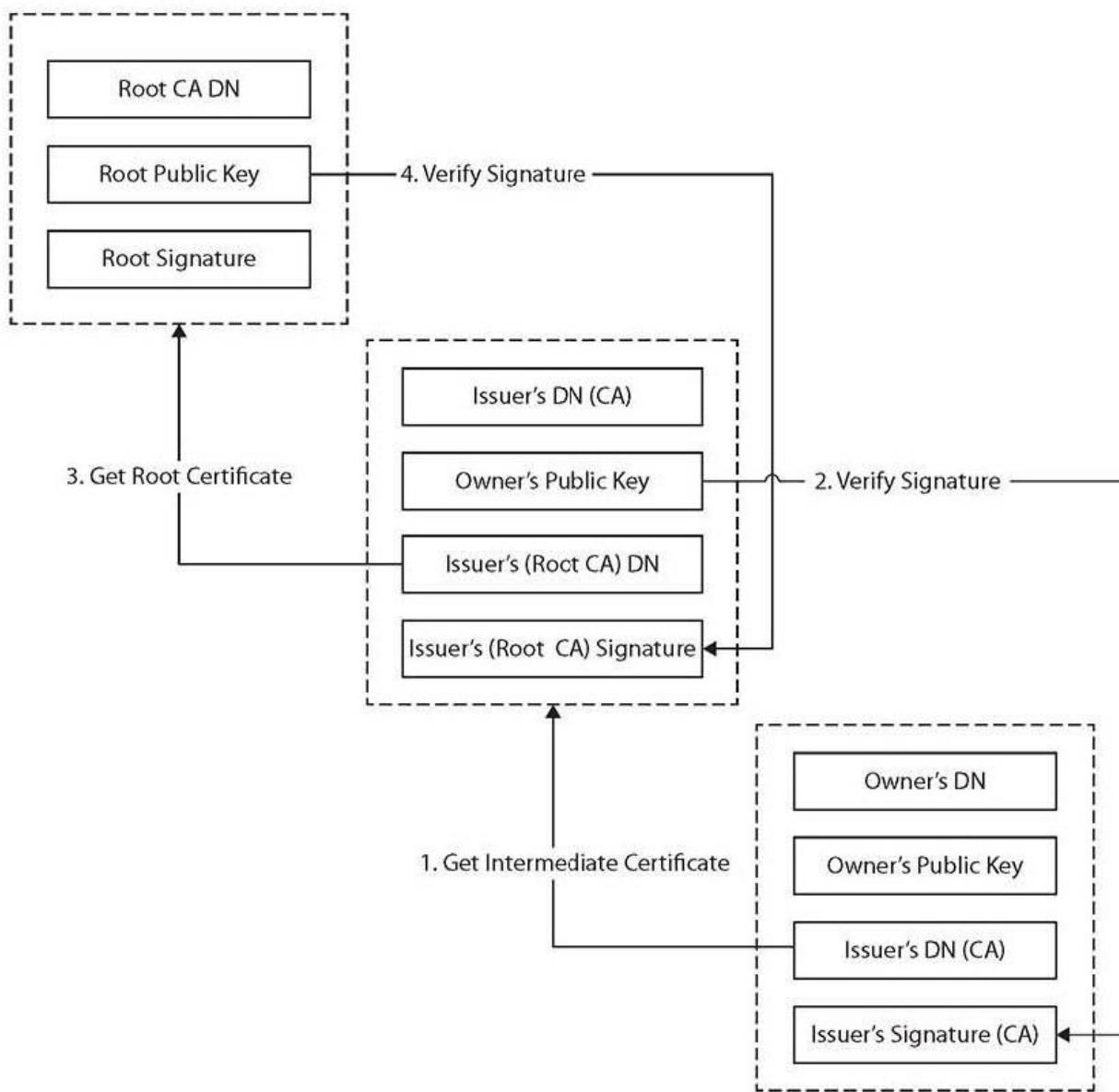
**Hình 25-6** Chứng nhận Ký Mã (Code Signing Certificate)

## Các Chứng nhận Ký-Mã-phần-mềm

Các chứng nhận có thể được chỉ định cho những mục đích cụ thể, chẳng hạn như để ký mã. Điều này cho phép sự linh hoạt trong việc quản lý chứng nhận đối với các chức năng cụ thể và giảm rủi ro trong trường hợp bị xâm phạm. Chứng nhận ký-mã được chỉ định như vậy trong chính bản thân chứng nhận và ứng dụng sử dụng chứng chỉ tuân theo giới hạn chính sách này để đảm bảo sử dụng chứng nhận thích hợp.

## Các Chứng nhận Tự-Ký

Các chứng nhận được ký bởi CA cấp-cao hơn, cung cấp nguồn gốc của sự tin cậy (root of trust). Như với tất cả các chuỗi, sẽ có một nút cuối cùng của sự tin cậy: nút gốc. Không phải mọi chứng nhận đều phải có cùng một nút gốc. Một công ty có thể tạo ra chuỗi chứng nhận của riêng mình để sử dụng bên trong công ty và do đó nó tạo ra nút gốc của riêng mình. "Chứng nhận gốc" do công-ty-tạo-ra này là một ví dụ về chứng nhận CA, đã được đề cập trước đó và phải được *tự-ký*, vì không có nút tin cậy "cao hơn" nào khác. Điều gì ngăn cản một người ký chứng chỉ của chính họ? Chuỗi tin cậy sẽ bắt đầu và kết thúc với chứng nhận và người dùng sẽ phải đối mặt với tình huống tiến thoái lưỡng nan về việc có nên tin tưởng chứng nhận hay không bởi vì cuối cùng, tất cả những gì một chứng nhận thực hiện là trình bày chi tiết chuỗi tin cậy cho một thực thể nào đó kết thúc sự tin cậy của người dùng. Tự-ký được hiển thị cho chứng nhận gốc trong Hình 25-7 (chứng nhận phía trên bên trái).



**Hình 25-7 Chuỗi Chứng nhận**

### Máy móc/Máy tính

Chứng nhận ràng buộc danh tính với các khóa và cung cấp một phương tiện xác thực, đôi khi là điều cần thiết cho máy tính. Active Directory Domain Services (AD DS) có thể theo dõi các máy trong hệ thống thông qua các máy tự nhận dạng bằng *chứng nhận máy*, còn được gọi là *chứng nhận máy tính*. Khi một người dùng đăng nhập, hệ thống có thể sử dụng

chứng nhận máy, nhận dạng máy hoặc chứng nhận người dùng, xác định người dùng – bất kỳ tùy chọn nào thích hợp cho hoạt động được mong muốn. Đây là một ví dụ về chứng nhận thực-thể-đầu-cuối.

## Email

Các chứng nhận kỹ thuật số có thể được sử dụng với các hệ thống email cho những mục như chữ ký kỹ thuật số liên kết với email. Cũng giống như các chức năng chuyên biệt khác, chẳng hạn việc như ký mã có chứng nhận của riêng mình, một *chứng nhận email* riêng biệt thường được sử dụng để nhận dạng liên quan đến e-mail. Đây là một ví dụ về chứng nhận thực-thể-đầu-cuối.

## Người dùng

Các *chứng nhận người dùng* là đúng như tên gọi – các chứng nhận xác định một người dùng. Chúng là một ví dụ về chứng nhận thực-thể-đầu-cuối.



## LƯU Ý

Các chứng nhận người dùng được sử dụng bởi người dùng cho các hệ thống tập tin được mã hóa (encrypted file system), email, và xác thực máy khách, trong khi các chứng nhận máy tính giúp các máy tính được xác thực trên hệ thống mạng.

## Root

Chứng nhận gốc là chứng nhận hình thành nền cơ sở tin cậy ban đầu trong chuỗi tin cậy. Mọi chứng nhận được ký bởi CA cấp chúng và các CA có thể được liên kết với nhau trong một cấu trúc đáng tin cậy. Đi theo chuỗi, một người đi lên cây tin cậy cho đến khi họ tìm thấy chứng nhận tự-ký, cho biết đó là chứng nhận gốc. Điều xác định một hệ thống có tin cậy vào chứng nhận gốc hay không chính là việc chứng nhận gốc có nằm trong kho lưu trữ chứng nhận đáng tin cậy của hệ thống hay không. Các

nha cung cấp khác nhau, chẳng hạn như Microsoft và Apple, đều có các chương trình chứng nhận gốc đáng tin cậy để xác định theo chính sách của công ty những CA nào mà họ sẽ gắn nhãn là đáng tin cậy. Chứng nhận gốc, vì chúng tạo thành mỏ neo tin cậy cho các chứng nhận khác, là ví dụ về chứng nhận CA, như đã được giải thích trước đó.

### Xác thực Miền

*Xác thực miền* là một phương tiện xác thực có độ-tin-cậy-thấp dựa trên việc người nộp đơn chứng minh quyền kiểm soát miền DNS. Xác thực tên miền thường được sử dụng cho TLS và có ưu điểm là nó có thể được tự động hóa thông qua kiểm tra so với một bản ghi DNS. Chứng nhận dựa-trên-xác-thực-miền, thường là miễn phí, cung cấp rất ít sự đảm bảo rằng danh tính không bị giả mạo vì người đăng ký không cần phải tương tác một cách trực tiếp với tổ chức phát hành. Xác thực miền có quy mô tốt và có thể được tự động hóa với ít hoặc không có tương tác thực sự giữa người đăng ký và CA, nhưng đổi lại, nó mang lại rất ít sự đảm bảo. Xác thực miền được chỉ định khác nhau trong các trình duyệt khác nhau, chủ yếu để tách nó khỏi các chứng nhận xác thực mở rộng, được mô tả tiếp theo.

### Xác thực Mở rộng

Các chứng nhận *xác thực mở rộng* (*extended validation - EV*) được sử dụng cho các trang web HTTPS và các phần mềm để mang lại mức độ đảm bảo cao về danh tính của người khởi tạo. Các chứng nhận EV sử dụng các phương pháp tương tự như mã hóa để bảo vệ tính toàn vẹn của chứng nhận cũng như các chứng nhận tổ chức và miền đã được xác thực. Sự khác biệt trong đảm bảo đến từ các quy trình đã được sử dụng bởi CA để xác thực danh tính pháp lý của một thực thể trước khi ban hành. Vì thông tin bổ sung được sử dụng trong quá trình xác thực, chứng nhận EV hiển

thị danh tính và những thông tin pháp lý khác như một phần của chứng nhận. Chứng nhận EV hỗ trợ đa miền nhưng không hỗ trợ ký tự đại diện.

Để hỗ trợ người dùng trong việc xác định chứng nhận EV và nâng cao độ tin cậy, một số manh mối trực quan bổ sung được cung cấp cho người dùng khi sử dụng EV. Khi được triển khai trong một trình duyệt, danh tính pháp lý được hiển thị, ngoài URL và một biểu tượng khóa, và trong hầu hết các trường hợp, toàn bộ thanh URL có màu xanh lục. Tất cả các nhà cung cấp trình duyệt lớn đều cung cấp sự hỗ trợ này và bởi vì thông tin được bao gồm trong chính chứng nhận, chức năng này là máy chủ web bất khả tri.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhận biết được các kiểu chứng nhận khác nhau được thảo luận trong phần này và chúng được sử dụng cho mục đích gì.

### **Định dạng Chứng nhận**

Chứng nhận kỹ thuật số được định nghĩa trong *RFC 5280: Chứng nhận Cơ sở hạ tầng Khóa công Khai Internet X.509 và Hồ sơ Danh sách Thu hồi Chứng nhận (CRL)*. RFC này mô tả chi tiết định dạng chứng nhận kỹ thuật số X.509 v3. Có rất nhiều cách để mã hóa thông tin trong chứng nhận trước khi trình bày dưới dạng tập tin và các phương pháp khác nhau dẫn đến các phần mở rộng tập tin khác nhau. Các phần mở rộng phổ biến bao gồm .der, .pem, .crt, .cer, .pfx, .p12 và .p7b. Mặc dù tất cả chúng đều có thể chứa thông tin về chứng nhận nhưng chúng không thể hoán đổi trực tiếp cho nhau. Mặc dù trong một số trường hợp nhất định, một số dữ liệu có thể được hoán đổi cho nhau, nhưng thực tiễn tốt nhất là xác định cách chứng nhận của bạn được mã hóa và sau đó dán nhãn một cách chính xác.

## KEY

Một tập tin *KEY*, được ký hiệu bằng phần mở rộng tập tin là .key có thể được sử dụng cho cả khóa PKCS#8 công khai và riêng tư. Các khóa có thể được mã hóa dưới dạng DER nhị phân hoặc ASCII PEM.

## Các Quy tắc Mã hóa Phân biệt (DER)

Các *quy tắc mã hóa phân biệt* (*Distinguished Encoding Rules - DER*) là một trong những quy tắc mã hóa Trừu tượng Cú pháp Một (Abstract Syntax Notation One - ASN.1) có thể được sử dụng để mã hóa bất kỳ đối tượng dữ liệu nào thành một tập tin nhị phân. Đối với chứng nhận, dữ liệu được liên kết với chứng nhận, một loạt các cặp tên-giá trị, cần được chuyển đổi sang một định dạng nhất quán để ký kỹ thuật số. DER đưa ra một cơ chế nhất quán dành cho nhiệm vụ này. Tập tin DER (phần mở rộng là .der) chứa dữ liệu nhị phân và có thể được sử dụng cho một chứng chỉ duy nhất.

## Thư được Tăng-cường-Quyền-riêng-tư

*Thư được Tăng-cường-Quyền-riêng-tư* (*Privacy-Enhanced Mail - PEM*) là định dạng phổ biến nhất được sử dụng bởi cơ quan cấp chứng nhận khi cấp chứng nhận. PEM đến từ RFC 1422 và là tập tin ASCII được mã-hóa-Base64 bắt đầu bằng “----- BEGIN CERTIFICATE -----”, tiếp theo là dữ liệu Base64 và kết thúc bằng “----- END CERTIFICATE-----”. Tập tin PEM hỗ trợ nhiều chứng nhận kỹ thuật số, bao gồm một chuỗi chứng nhận. Một tập tin PEM có thể chứa nhiều mục nhập, lần lượt, và có thể bao gồm cả khóa công khai và khóa riêng tư. Tuy nhiên, hầu hết các nền tảng, chẳng hạn như các máy chủ web, đều kỳ vọng các chứng chỉ và khóa riêng tư nằm trong các tập tin riêng biệt.

Định dạng PEM cho dữ liệu chứng nhận được sử dụng trong nhiều loại tập tin, bao gồm các tập tin .pem, .cer, .crt và .key.



**MÁCH NƯỚC CHO KỲ THI** Nếu bạn cần chuyển nhiều chứng nhận, hoặc một chuỗi chứng nhận, hãy sử dụng PEM để mã hóa. Mã hóa PEM có thể mang nhiều chứng nhận, trong khi DER chỉ có thể mang một chứng nhận duy nhất.

### **Trao đổi Thông tin Cá nhân (PFX)**

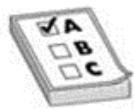
Tập tin PKCS#12 là một định dạng tập tin di động có phần mở rộng là .pfx. Đây là một định dạng nhị phân để lưu trữ chứng nhận máy chủ, chứng nhận trung gian và khóa cá nhân trong một tập tin. Tập tin *Trao đổi Thông tin Cá nhân (Personal Information Exchange - PFX)* thường được sử dụng trên các máy Windows để nhập và xuất các chứng nhận và khóa cá nhân.

### **CER**

Phần mở rộng tập tin .cer được sử dụng để biểu thị một dạng thay thế, từ Microsoft, của tập tin CRT. Phần mở rộng .cer/.crt được sử dụng cho các chứng nhận và có thể được mã hóa dưới dạng DER nhị phân hoặc ASCII PEM. Các phần mở rộng .cer và .crt gần như đồng nghĩa. Phần mở rộng .cer thường được kết hợp với hệ thống Microsoft Windows, trong khi .crt được liên kết với hệ thống UNIX.



**LƯU Ý** Thời điểm mà duy nhất .crt và .cer có thể được hoán đổi cho nhau một cách an toàn là khi loại mã hóa có thể giống hệt nhau (ví dụ: CRT được-mã-hóa-PEM giống với CER được-mã-hóa-PEM).



**MÁCH NƯỚC CHO KỲ THI** Phần mở rộng tập tin .crt là một định dạng tập tin chứng nhận SSL được sử dụng bởi các máy chủ web để giúp xác minh danh tính và bảo mật của trang đang được đề cập.

## P12

*P12* là một phần mở rộng tập tin thay thế cho một định dạng tập tin PKCS#12, một định dạng nhị phân dành cho việc lưu trữ chứng nhận máy chủ, các chứng nhận trung gian, và khóa riêng tư trong một tập tin đã được mã hóa. Những tập tin này thường có một phần mở rộng như .pfx hoặc .p12. Chúng thường được sử dụng trên các máy Windows để nhập và xuất các chứng nhận và các khóa riêng tư.

## P7B

Định dạng *PKCS#7* hoặc *P7B* được lưu trữ ở định dạng Base64 ASCII và có phần mở rộng tập tin là .p7b hoặc .p7c. Một tập tin P7B bắt đầu bằng “----- BEGIN PKCS7 -----” và chỉ chứa các chứng nhận và chuỗi chứng nhận (CA trung gian) chứ không phải khóa cá nhân. Các nền tảng phổ biến nhất hỗ trợ tập tin P7B là Microsoft Windows và Java Tomcat.

## Các Khái niệm

Hệ thống PKI bao gồm các mục đã được thảo luận trong phần đầu tiên, cũng như các phương pháp sử dụng các mục đó để đạt được chức năng mong muốn. Khi bạn đang sử dụng một giải pháp dựa-trên-PKI, điều quan trọng là phải hiểu rằng tính bảo mật của giải pháp phụ thuộc vào cách các phần tử được sử dụng cũng như cách thức chúng được xây dựng như thế nào. Phần này mô tả một số yếu tố mang tính vận hành quan trọng, chẳng hạn như chốt (pinning), ghim (stapling) và chuỗi chứng chỉ, và xem xét các mô hình tin cậy khác nhau.

## CA Trực tuyến so với Ngoại tuyến

Máy chủ chứng nhận phải trực tuyến để cung cấp dịch vụ chứng nhận, vậy tại sao ai đó lại có một máy chủ ngoại tuyến? Nguyên nhân chủ yếu là vì vẫn đề bảo mật. Nếu một tổ chức phát hành chứng nhận nhất định chỉ được sử dụng cho các chức năng định kỳ - ví dụ: ký các chứng nhận cụ thể hiếm khi được cấp lại hoặc được ký - thì việc giữ máy chủ ngoại tuyến trừ khi cần thiết sẽ cung cấp mức độ bảo mật đáng kể cho quá trình ký. Các yêu cầu CA khác, chẳng hạn như CRL và các yêu cầu xác thực, có thể được chuyển đến cơ quan xác thực đã được phê duyệt bởi CA.

## Stapling

Ghim (*stapling*) là quá trình kết hợp các mục liên quan để giảm bớt các bước giao tiếp. Một ví dụ là khi ai đó yêu cầu một chứng nhận, việc ghim sẽ gửi cả chứng nhận và thông tin người trả lời OCSP trong cùng một yêu cầu để tránh các lần tìm nạp bổ sung mà máy khách sẽ phải thực hiện trong quá trình xác thực đường dẫn.



## MÁCH NƯỚC CHO KỲ THI

Ghim chứng nhận được coi là một cách thức hiệu quả hơn để xử lý quá trình xác minh chứng nhận. Nó giảm thiểu gánh nặng cho CA.

## Chốt (Pinning)

Khi một chứng nhận được cung cấp cho một máy chủ, dù là xác định máy chủ hoặc cung cấp khóa công khai, thông tin này có thể được lưu trong một hành động được gọi là *chốt*, là quá trình liên kết máy chủ với một chứng nhận X.509 hoặc khóa công khai đã được cung cấp trước đó. Điều này có thể quan trọng đối với các ứng dụng di động di chuyển giữa các mạng một cách thường xuyên và có nhiều khả năng được liên kết với các

mạng thù địch nơi có mức độ tin cậy thấp và nguy cơ dữ liệu độc hại cao. Chốt hỗ trợ bảo mật thông qua việc tránh sử dụng DNS và các rủi ro cõi hữu của nó khi ở trên các mạng-bảo-mật-kém.

Quá trình sử dụng lại chứng nhận hoặc khóa công khai được gọi là *tính liên tục của khóa*. Điều này cung cấp sự bảo vệ khỏi một kẻ tấn công, giả sử rằng kẻ tấn công đã không ở vị trí để tấn công vào lần chốt ban đầu. Nếu kẻ tấn công có thể chặn và phá hoại liên lạc ban đầu thì việc chốt sẽ bảo toàn cuộc tấn công. Bạn nên chốt bất kỳ lúc nào bạn muốn tương đối chắc chắn về danh tính của máy chủ từ xa, dựa vào bảo mật mạng gia đình của bạn và bạn có khả năng sẽ hoạt động sau này trong một môi trường thù địch. Nếu bạn chọn chốt, bạn sẽ có hai tùy chọn: chốt chứng nhận hoặc chốt khóa công khai.



## MÁCH NƯỚC CHO KỲ THI

Việc chốt chứng nhận là quá trình liên kết một máy chủ với khóa công khai hoặc chứng nhận X.509 dự kiến của nó.

### Mô hình Tin cậy

Một *mô hình tin cậy* là một cấu trúc bao gồm các hệ thống, nhân sự, ứng dụng, giao thức, công nghệ và chính sách hoạt động cùng nhau để cung cấp một mức độ bảo vệ nhất định. Tất cả các thành phần này có thể hoạt động cùng nhau một cách liền mạch trong phạm vi cùng một miền tin cậy vì chúng đã được các thành phần khác trong miền biết đến và được tin cậy ở một mức độ nào đó. Các miền tin cậy khác nhau thường được quản lý bởi các nhóm quản trị viên khác nhau, có các chính sách bảo mật khác nhau và hạn chế người ngoài truy cập có đặc quyền.

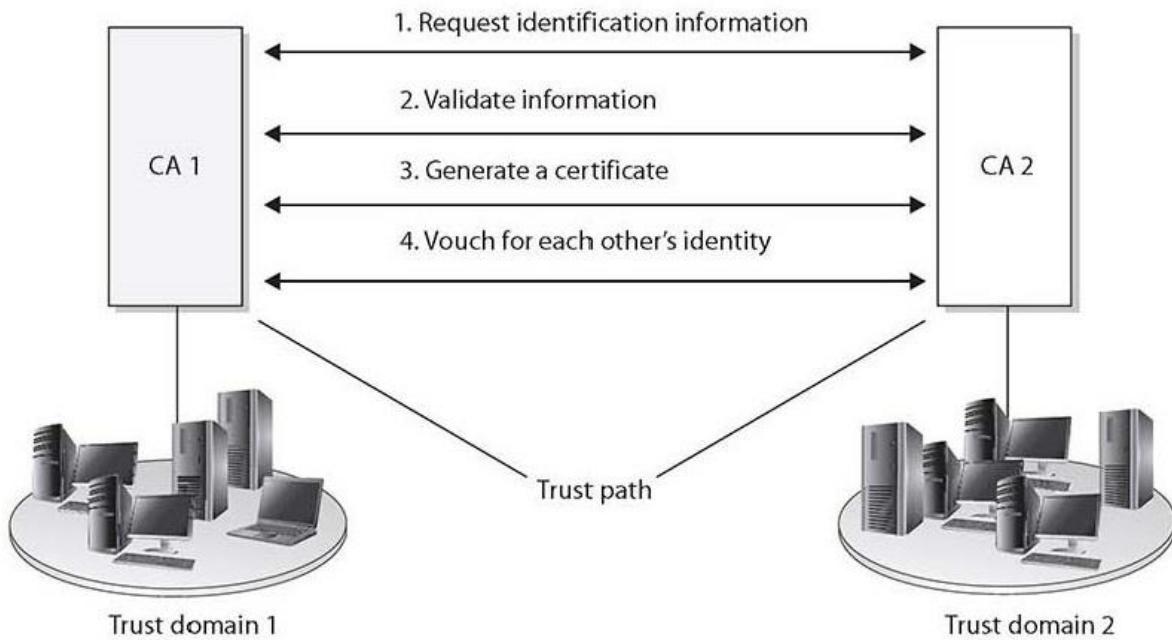
Hầu hết các miền tin cậy (cho dù là các công ty hay phòng ban riêng lẻ) thường không phải là những hòn đảo tách rời khỏi thế giới - chúng cần giao tiếp với các miền khác, ít-đáng-tin-cậy-hơn. Bí quyết ở đây là tìm ra rằng hai miền khác nhau nên tin cậy nhau đến mức nào, cũng như cách thức triển khai và định cấu hình cơ sở hạ tầng sẽ cho phép hai miền này giao tiếp theo cách không cho phép xâm phạm hoặc vi phạm bảo mật. Điều này có thể nói sẽ dễ hơn làm.

Một ví dụ về sự tin cậy đã được xem xét trước đó trong chương là bằng lái xe được cấp bởi DMV. Ví dụ, giả sử Bob đang mua một chiếc đèn từ Carol và anh ấy muốn thanh toán bằng séc. Vì Carol không biết Bob nên cô không biết mình có thể tin tưởng anh ta hay tin tưởng nhiều vào tấm séc của anh ta hay không. Nhưng nếu Bob cho Carol xem giấy phép lái xe của anh ấy, cô ấy có thể so sánh tên [trên bằng lái xe] với những gì xuất hiện trên séc và cô ấy có thể chọn chấp nhận. Mở neo tin cậy (bên-thứ-ba đáng tin cậy đã được thỏa thuận) trong trường hợp này là DMV, vì cả Carol và Bob đều tin tưởng nó hơn là tin tưởng lẫn nhau. Vì Bob phải cung cấp tài liệu để chứng minh danh tính của mình cho DMV nên tổ chức đó tin cậy anh ta đủ để tạo ra giấy phép và Carol tin tưởng DMV, vì vậy cô quyết định tin tưởng vào séc của Bob.

Hãy cùng xem xét một ví dụ khác về mở neo tin cậy. Nếu Joe và Stacy cần giao tiếp qua email và muốn sử dụng mã hóa và chữ ký điện tử, họ sẽ không chỉ tin tưởng riêng vào chứng nhận của nhau. Nhưng khi mỗi người nhận được chứng nhận của người kia và thấy rằng cả hai đều đã được ký điện tử bởi một tổ chức mà cả hai đều tin tưởng – CA - thì họ sẽ có mức độ tin cậy sâu hơn vào nhau. Mở neo tin cậy ở đây là CA. Điều này khá dễ dàng, nhưng khi chúng ta cần thiết lập mở neo tin cậy giữa các CA và môi trường PKI khác nhau, nó sẽ phức tạp hơn một chút.

Khi hai công ty cần giao tiếp bằng cách sử dụng PKI riêng của họ hoặc nếu hai bộ phận trong cùng một công ty sử dụng các CA khác nhau thì hai miền tin cậy tách biệt sẽ liên quan. Người dùng và các thiết bị từ các miền tin cậy khác nhau này sẽ cần giao tiếp với nhau và họ cũng sẽ cần trao đổi chứng chỉ và khóa công khai. Điều này có nghĩa là các mỏ neo tin cậy cần phải được xác định và một kênh giao tiếp phải được xây dựng và duy trì.

Một mối quan hệ tin cậy phải được thiết lập giữa hai cơ quan phát hành [chứng nhận] (CA). Điều này xảy ra khi một hoặc cả hai CA cấp chứng nhận cho khóa công khai của CA khác, như được minh họa trong Hình 25-8. Điều này có nghĩa là mỗi CA đăng ký một chứng nhận và khóa công khai từ CA khác. Mỗi CA sẽ xác thực thông tin nhận dạng của CA khác và tạo ra một chứng nhận có chứa khóa công khai để CA đó sử dụng. Điều này thiết lập nên một lộ tuyến tin cậy giữa hai thực thể mà sau đó có thể được sử dụng khi người dùng cần xác minh chứng nhận của người dùng khác nằm trong các miền tin cậy khác nhau. Lộ tuyến tin cậy có thể là một chiều hoặc hai chiều, do đó hoặc hai CA tin tưởng lẫn nhau (hai chiều) hoặc chỉ một CA tin tưởng vào CA còn lại (một chiều).



**Hình 25-8** Một mối quan hệ đáng tin cậy có thể được xây dựng giữa hai miền tin cậy để thiết lập một kênh giao tiếp.

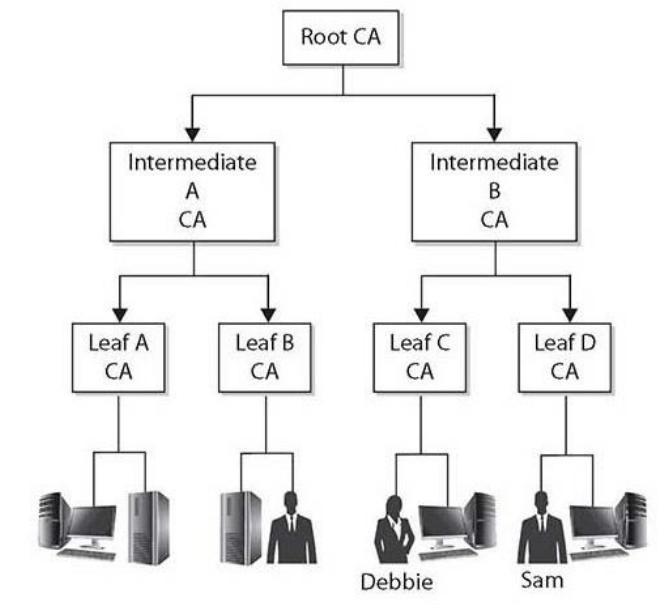
Như được minh họa trong Hình 25-8, mọi người dùng và thiết bị trong miền tin cậy 1 tin tưởng vào cơ quan cấp chứng nhận (CA 1) của riêng họ, vốn là mỏ neo tin cậy của họ. Mọi người dùng và thiết bị trong miền tin cậy 2 có mỏ neo tin cậy của riêng mình, CA 2. Hai CA đã trao đổi các chứng nhận và tin cậy lẫn nhau, nhưng chúng không có chung một mỏ neo tin cậy giữa chúng.

Các mô hình tin cậy mô tả và phác thảo nên mối quan hệ tin cậy giữa các CA khác nhau và các môi trường khác nhau, sẽ chỉ ra nơi mà các lô tuyến tin cậy tồn tại. Các mô hình và lô tuyến tin cậy cần phải được suy nghĩ trước khi triển khai để hạn chế và kiểm soát quyền truy cập một cách thích hợp và để đảm bảo rằng số lượng lô tuyến tin cậy được sử dụng là càng ít càng tốt. Một vài mô hình tin cậy khác nhau có thể được sử dụng:

phân cấp có cấu trúc, ngang-hàng, và các mô hình lai ghép được thảo luận trong các phần tiếp theo.

### **Mô hình Tin cậy Phân cấp có cấu trúc**

Kiểu mô hình tin cậy đầu tiên mà chúng ta sẽ xem xét là một cấu trúc phân cấp cơ bản có chứa một CA gốc, một CA trung gian và các CA nút, và các thực-thể-đầu-cuối. Hình dạng của mô hình này là một cây đảo ngược, như được minh họa trong Hình 25-9. CA gốc là mỏ neo tin cậy cuối cùng cho tất cả mọi thực thể khác trong cơ sở hạ tầng này và nó tạo ra các chứng nhận cho các CA trung gian, từ đó tạo ra các chứng nhận cho các CA nút và các CA nút tạo ra các chứng nhận cho các thực-thể-đầu-cuối.



**Hình 25-9** Mô hình tin cậy phân cấp có cấu trúc phác họa nên các lô tuyến tin cậy

Như đã được giới thiệu trước đó trong chương, các CA trung gian có chức năng truyền tải sự tin cậy giữa các CA khác nhau. Các CA này được gọi là CA cấp dưới, vì chúng là cấp dưới của CA mà chúng tham chiếu đến.

Lộ tuyển tin cậy được đi lên từ CA cấp dưới đến CA cấp trên, và về bản chất, CA cấp dưới đang sử dụng CA cấp cao-hơn làm tham chiếu.

Như trong Hình 25-9, không có sự tin cậy hai chiều nào tồn tại – tất cả chúng đều là sự tin cậy một chiều, như được chỉ ra bởi các mũi tên một chiều. Vì không thực thể nào khác có thể xác nhận và tạo ra chứng nhận cho CA gốc nên nó tạo ra một chứng nhận tự-ký. Điều này có nghĩa là tổ chức phát hành chứng nhận và các trường chủ thể giữ cùng một thông tin, và cả hai đều đại diện cho CA gốc và khóa công khai của CA gốc sẽ được sử dụng để xác minh chứng nhận này khi đến thời điểm đó. Chứng nhận CA gốc và khóa công khai này được phân phối cho tất cả các thực thể trong mô hình tin cậy này.

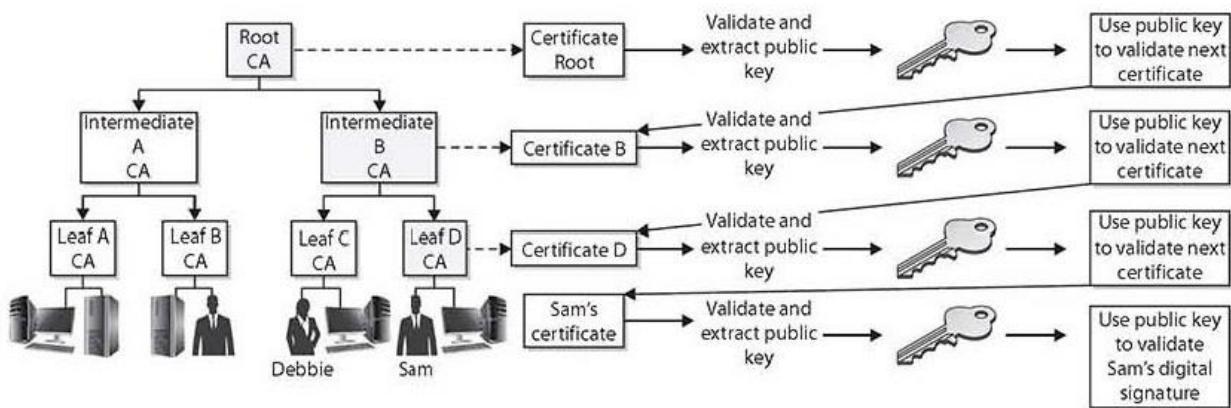
**Đi theo Đường dẫn Chứng nhận** Khi người dùng trong một miền tin cậy cần giao tiếp với một người dùng khác trong một miền tin cậy khác, một người dùng sẽ cần xác thực chứng nhận của người kia. Điều này nghe có vẻ khá đơn giản, nhưng nó thực sự có nghĩa là mỗi chứng nhận cho mỗi CA, cho đến một mỏ neo đáng tin cậy được chia sẻ cũng phải được xác thực. Nếu Debbie cần xác thực chứng nhận của Sam, như được minh họa trong Hình 25-9, cô ấy thực sự cũng cần xác thực chứng chỉ Nút CA D và CA Trung gian B, cũng giống như Sam.

Vì vậy, trong Hình 25-9, chúng ta có một người dùng - Sam, người ký điện tử vào một thông điệp và gửi nó cùng chứng nhận của anh ta tới Debbie. Debbie cần xác thực chứng nhận này trước khi cô ấy có thể tin tưởng vào chữ ký kỹ thuật số của Sam. Được bao gồm trong chứng nhận của Sam là một trường tổ chức phát hành, cho biết rằng chứng nhận được cấp bởi Nút CA D. Debbie phải lấy chứng nhận kỹ thuật số của Nút CA D và khóa công khai để xác thực chứng nhận của Sam. Hãy nhớ rằng Debbie xác thực chứng nhận bằng cách xác minh chữ ký số của nó. Chữ ký kỹ thuật số do tổ chức phát hành chứng nhận tạo ra bằng khóa riêng của

họ, vì vậy Debbie cần xác minh chữ ký bằng khóa công khai của tổ chức phát hành.

Debbie theo dõi chứng chỉ và khóa công khai của Nút CA D, nhưng giờ đây cô ấy cần xác minh chứng nhận của [nút] CA này, vì vậy cô ấy xem xét trường tổ chức phát hành, trường này cho biết rằng chứng nhận của Nút CA D đã được phát hành bởi CA Trung gian B. Đến lúc này thì Debbie cần nhận được chứng nhận và khóa công khai của CA Trung gian B.

Phần mềm máy khách của Debbie theo dõi điều này và phát hiện rằng nhà phát hành của CA Trung gian B là CA gốc, nhà phát hành mà cô đã có chứng nhận và khóa công khai. Vì vậy, phần mềm máy khách của Debbie phải đi theo *lộ tuyến chứng nhận*, nghĩa là nó phải tiếp tục theo dõi và thu thập chứng nhận cho đến khi có được chứng nhận tự-ký. Một chứng nhận tự-ký cho biết rằng nó đã được ký bởi CA gốc và phần mềm của Debbie đã được thiết lập cấu hình để tin cậy thực thể này như là mỏ neo tin cậy của cô ấy, vì vậy cô ấy có thể dừng lại ở đó. Hình 25-10 minh họa các bước mà phần mềm của Debbie phải thực hiện để có khả năng xác minh chứng nhận của Sam.



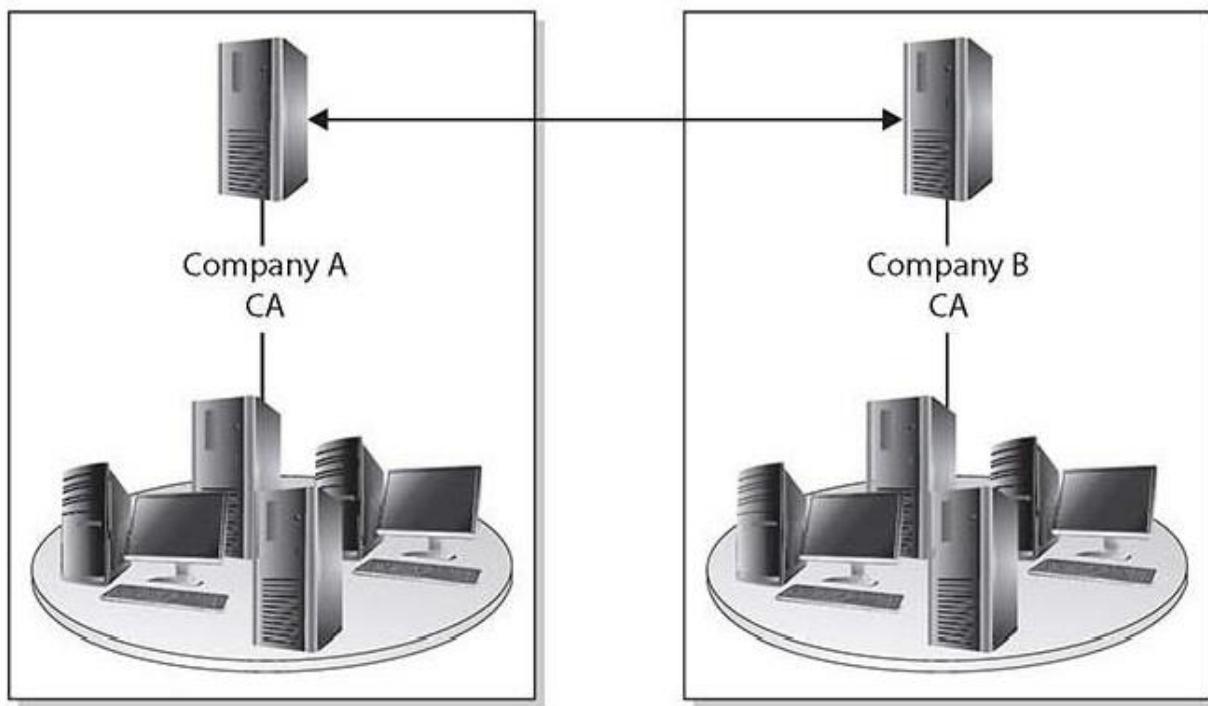
**Hình 25-10** Việc xác minh mỗi chứng nhận trong một lộ tuyến chứng nhận

Kiểu mô hình tin cậy đơn giản này hoạt động tốt trong một doanh nghiệp dễ dàng tuân theo sơ đồ tổ chức phân cấp, nhưng rất nhiều công ty không thể sử dụng kiểu mô hình tin cậy này vì các phòng ban hoặc văn phòng khác nhau yêu cầu các mỏ neo tin cậy của riêng họ. Những nhu cầu này có thể xuất phát từ nhu cầu kinh doanh trực tiếp hoặc từ các yếu tố chính trị giữa các tổ chức. Mô hình phân cấp này có thể không khả thi khi hai hoặc nhiều công ty cần giao tiếp với nhau. Không công ty nào sẽ để CA của bên kia trở thành CA gốc, bởi vì mỗi công ty không nhất thiết phải tin tưởng tổ chức kia đến mức độ đó. Trong những tình huống này, các CA sẽ cần phải làm việc trong một mối quan hệ ngang hàng thay vì trong mối quan hệ phân cấp.

### **Mô hình Tin cậy Ngang-hàng**

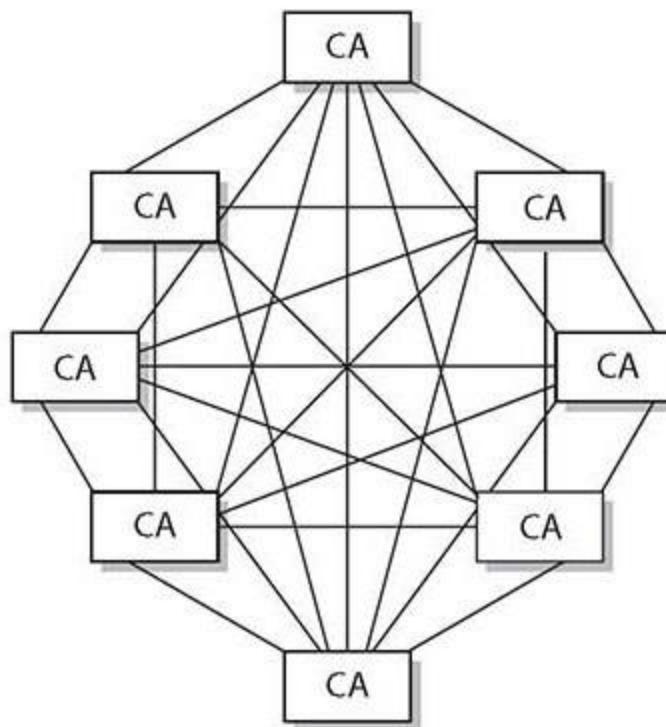
Trong một *mô hình tin cậy ngang hàng*, một CA không trực thuộc CA khác và không có mỏ neo đáng tin cậy nào được thiết lập giữa các CA được tham gia. Các thực-thể-đầu-cuối sẽ xem CA phát hành của họ như một mỏ neo đáng tin cậy của họ, nhưng các CA khác nhau sẽ không có một mỏ neo chung.

Hình 25-11 minh họa kiểu mô hình tin cậy này. Hai CA khác nhau sẽ chứng nhận khóa công khai cho nhau, và điều này tạo ra sự tin cậy hai chiều. Điều này được gọi là *chứng-nhận-chéo* vì các CA không nhận chứng nhận và khóa công khai của họ từ CA cấp trên, mà thay vào đó chúng đang tạo ra chứng nhận cho nhau.



**Hình 25-11** Sự chứng nhận chéo tạo ra một mô hình PKI ngang-hàng.

Một trong những nhược điểm chính của mô hình này là khả năng mở rộng quy mô. Mỗi CA phải chứng nhận mọi CA khác đang tham gia và một lô tuyển tin cây hai chiều phải được triển khai, như được thể hiện trong Hình 25-12. Nếu một CA gốc chứng nhận tất cả các CA trung gian thì khả năng mở rộng sẽ không còn là vấn đề nữa. Hình 25-12 đại diện cho một kiến trúc dạng lưới được kết nối đầy đủ, có nghĩa là mỗi CA được kết nối trực tiếp và có mối quan hệ tin cậy hai chiều với mọi CA khác. Như bạn có thể thấy trong hình minh họa này, sự phức tạp của thiết lập này có thể trở nên bị quá tải.

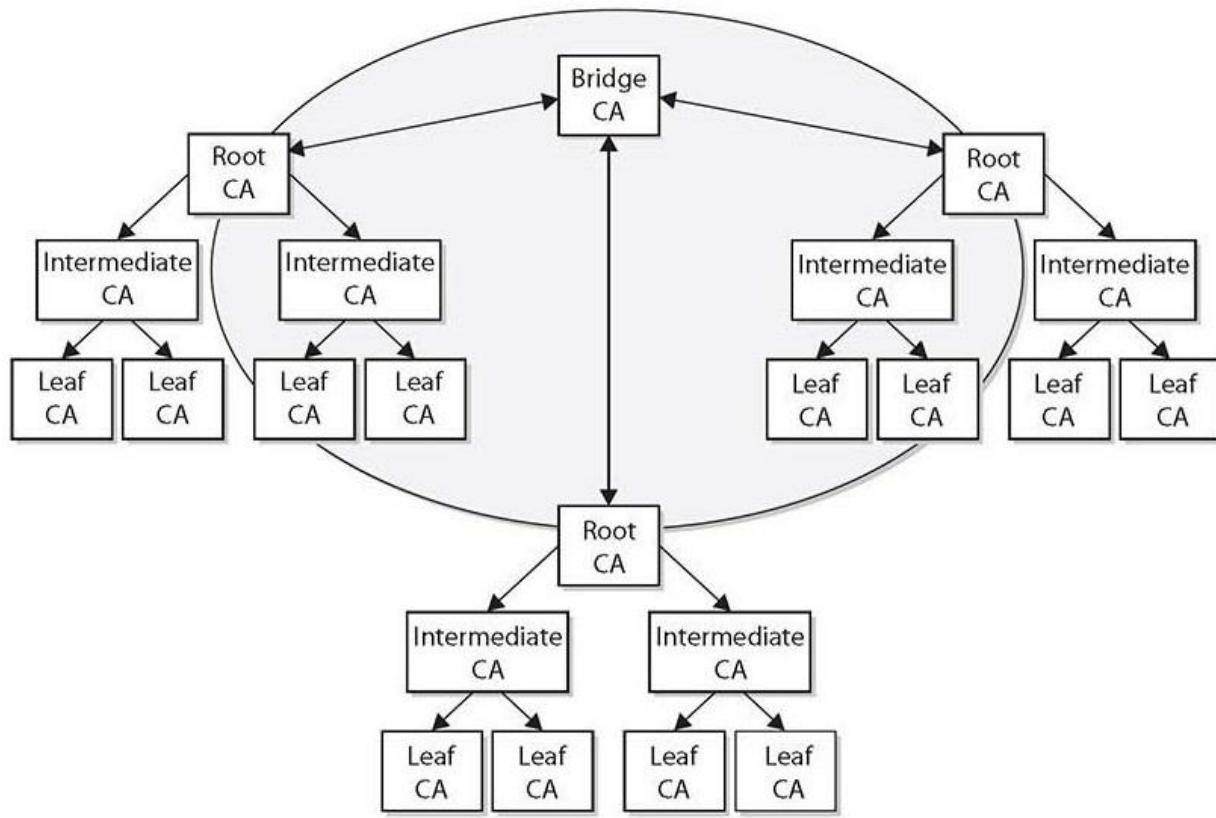


**Hình 25-12** Khả năng mở rộng quy mô là một nhược điểm trong các mô hình chứng nhận chéo.

Một công ty có thể rất phức tạp trong phạm vi bản thân nó, và khi phát sinh nhu cầu giao tiếp đúng cách với các đối tác, nhà cung cấp và khách hàng bên ngoài theo một cách được cấp phép và bảo mật thì sự phức tạp này có thể khiến việc bám sát mô hình tin cậy có cấu trúc phân cấp hoặc ngang hàng trở nên khó khăn, nếu không muốn nói là bất khả thi. Trong rất nhiều triển khai, các kiểu mô hình khác nhau phải được kết hợp để cung cấp các đường giao tiếp và mức độ tin cậy cần thiết. Trong *mô hình tin cậy lai ghép*, hai công ty có các mô hình phân cấp nội bộ của riêng họ và được kết nối thông qua mô hình ngang-hàng bằng cách sử dụng chứng-nhận-chéo.

Một tùy chọn khác trong cấu hình lai ghép này là triển khai một *CA cầu nối* (*bridge CA*). Hình 25-13 minh họa vai trò mà CA cầu nối có thể thực

hiện - nó chịu trách nhiệm cho việc phát hành các chứng-nhận-chéo cho tất cả các CA được kết nối và miễn tin cậy. Cầu nối CA không được coi là gốc hoặc mỏ neo tin cậy, mà chỉ đơn thuần là thực thể tạo và duy trì chứng-nhận-chéo cho các môi trường được kết nối.



**Hình 25-13** Một CA cầu nối có thể kiểm soát các thủ tục chứng-nhận-chéo



### MÁCH NƯỚC CHO KỲ THI

Có 3 mô hình tin cậy: có cấu trúc phân cấp, ngang-hàng, và lai ghép. Niềm tin có thứ bậc giống như một cái cây úp ngược. Ngang hàng là một loạt các tham chiếu bên và kết hợp là sự kết hợp của sự tin cậy theo cấu trúc phân cấp và ngang-hàng.

## Ký quỹ Khóa

Sự phát triển ấn tượng của việc sử dụng công nghệ mã hóa đã dẫn đến những phương pháp mới để xử lý khóa. *Ký quỹ khóa* là một hệ thống mà trong đó khoá cá nhân của bạn được giữ bởi cả bạn và bên thứ ba. Mã hóa rất giỏi trong việc che giấu bí mật và với công nghệ máy tính có giá cả phải chăng đối với tất cả mọi người, tội phạm và những kẻ ác ý khác đã bắt đầu sử dụng mã hóa để che giấu thông tin liên lạc và giao dịch kinh doanh khỏi sự theo dõi của các cơ quan thực thi pháp luật. Bởi vì họ không thể phá vỡ mã hóa nên các cơ quan chính phủ bắt đầu yêu cầu ký quỹ khóa. Ký quỹ khoá trong trường hợp này là một hệ thống mà khoá cá nhân của bạn được giữ bởi cả bạn và chính phủ. Điều này cho phép những người có lệnh của tòa án để truy xuất khóa riêng tư của bạn để có quyền truy cập vào bất kỳ thứ gì đã được mã hóa bằng khóa công khai của bạn. Dữ liệu về cơ bản được mã hóa bằng khóa của bạn và khóa của chính phủ, cho phép chính phủ truy cập vào dữ liệu bản rõ ràng của bạn.

Ký quỹ khóa cũng được sử dụng bởi các tập đoàn doanh nghiệp vì nó cung cấp một phương pháp lấy khóa trong trường hợp người giữ khóa không sẵn sàng. Ngoài ra, còn có một số các cơ chế khôi phục chính để thực hiện việc này, và các chính sách của công ty sẽ xác định cách thức phù hợp để bảo vệ các khóa trong toàn doanh nghiệp.

Ký quỹ khoá liên quan đến một cơ quan bên ngoài có thể có tác động tiêu cực đến tính bảo mật được cung cấp bởi mã hóa, vì chính phủ yêu cầu một hệ thống cơ sở hạ tầng khổng lồ và phức tạp để giữ mọi khóa được ký quỹ và tính bảo mật của những hệ thống đó kém hiệu quả hơn khi so với việc bạn ghi nhớ khóa. Tuy nhiên, có hai mặt đối với việc ký quỹ khóa. Nếu không có một cách thực tế để khôi phục khóa nếu hoặc khi nó bị mất hoặc người giữ khóa chết chẳng hạn, một số thông tin quan trọng

sẽ bị mất vĩnh viễn. Những vấn đề như vậy sẽ có ảnh hưởng đến thiết kế và bảo mật của công nghệ mã hóa trong tương lai gần.



**MÁCH NƯỚC CHO KỲ THI** Ký quỹ khóa có thể giải quyết rất nhiều vấn đề do không thể truy cập được vào khóa, và bản chất của mật mã khiến cho việc truy cập vào dữ liệu là điều bất khả nếu không có khóa.

### **Chuỗi Chứng nhận**

Các chứng nhận được sử dụng để truyền tải danh tính và cắp khóa công khai cho người dùng, nhưng điều này cũng sẽ đặt ra câu hỏi: tại sao lại tin tưởng vào chứng nhận? Câu trả lời nằm trong *chuỗi chứng nhận*, một chuỗi tin cậy từ chứng nhận này sang chứng nhận khác, dựa trên việc được ký bởi tổ chức phát hành, cho đến khi chuỗi kết thúc bằng chứng nhận mà người dùng tin tưởng. Điều này truyền sự tin cậy từ chứng nhận đáng tin cậy sang chứng nhận đang được sử dụng. Hãy xem xét Hình 25-7 ở phần trước của chương, chúng ta có thể xem danh sách các chứng nhận theo thứ tự từ chứng nhận được trình bày đến chứng nhận đáng tin cậy.

Các chứng nhận nằm giữa chứng nhận được trình bày và chứng nhận gốc được gọi là chứng nhận chuỗi hoặc chứng nhận trung gian. Chứng nhận trung gian là người ký/người phát hành của chứng nhận được trình bày, chỉ ra rằng nó tin cậy chứng nhận. Chứng nhận CA gốc là người ký/người phát hành chứng nhận trung gian, cho biết rằng nó tin cậy chứng nhận trung gian. Chuỗi các chứng nhận là một cách chuyển niềm tin xuống từ chứng nhận gốc đáng tin cậy. Chuỗi [chứng nhận] kết thúc bằng chứng nhận CA gốc, và chứng nhận này luôn được chính CA ký. Chữ ký của tất cả các chứng nhận trong chuỗi phải được xác minh với chứng nhận CA gốc.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các nguyên tắc của cơ sở hạ tầng khóa công khai. Chương này bắt đầu với mô tả về các thành phần của một hệ thống PKI, bao gồm tổ chức phát hành chứng nhận (CA), quản lý khóa, CA trung gian, cơ quan đăng ký (RA), danh sách thu hồi chứng nhận (CRL) và các thuộc tính của chứng nhận. Tiếp theo, các chủ đề Giao thức Trạng thái Chứng nhận Trực tuyến (OCSP), yêu cầu ký chứng nhận (CSR), CN, SAN và hết hạn đã được đề cập. Cuộc thảo luận được tiếp tục với các loại chứng nhận, bao gồm các chứng nhận ký tự đại diện, SAN, ký mã, tự-ký, máy móc/máy tính, email, người dùng, root, xác thực miễn và xác thực mở rộng. Chương tiếp tục với các định dạng chứng nhận, chẳng hạn như Quy tắc Mã hóa Phân biệt (DER), Thư được-Nâng-cao-Quyền-riêng-tư (PEM), Trao đổi Thông tin Cá nhân (PFX), CER, P12 và P7B. Chương này kết thúc bằng một cuộc thảo luận về các khái niệm PKI, bao gồm CA trực tuyến và ngoại tuyến, chốt, ghim, mô hình tin cậy, ký quỹ và chuỗi chứng chỉ.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Bạn được yêu cầu từ quản trị viên hệ thống cấp cao để làm mới chứng nhận SSL trên các máy chủ web. Quy trình là tạo ra một yêu cầu ký chứng nhận (CSR), gửi nó cho một bên thứ ba để được ký, và sau đó áp dụng thông tin được trả về cho CSR. Đây là ví dụ về điều gì?

  - A. Chốt
  - B. Cơ quan được vay
  - C. Mô hình tin cậy bên-thứ-ba
  - D. Ghim.
2. Tổ chức phát hành chứng chỉ bao gồm những tổ chức nào sau đây?

  - A. Phần cứng và phần mềm
  - B. Chính sách và thủ tục
  - C. Những người đang quản lý chứng chỉ
  - D. Tất cả những đáp án trên.
3. Người quản lý của bạn muốn bạn xem xét CPS của hệ thống PKI nội bộ của công ty về khả năng áp dụng và xác minh cũng như để đảm bảo rằng nó đáp ứng các nhu cầu hiện tại. Bạn có nhiều khả năng sẽ tập trung vào điều gì nhất?

  - A. Thu hồi
  - B. Mức độ tin cậy được cung cấp cho người dùng
  - C. Entropy của khóa
  - D. Cách thức các khóa được lưu trữ.
4. Bạn đang chuẩn bị một e-mail để gửi cho đồng nghiệp tại nơi làm việc, và vì thông tin trong thông điệp là nhạy cảm nên bạn quyết

định mã hóa nó. Khi bạn cố gắng áp dụng chứng nhận mà bạn có cho đồng nghiệp, mã hóa đã không thành công. Chứng nhận được liệt kê là vẫn còn hiệu lực trong một năm nữa và cơ quan cấp chứng nhận vẫn được tin cậy và đang hoạt động. Điều gì đã xảy ra với khóa của người dùng này?

- A.** Nó đã sử dụng thuật toán sai.
  - B.** Bạn đang truy vấn cơ quan cấp chứng nhận không chính xác.
  - C.** Chứng nhận đã bị thu hồi.
  - D.** Mô hình tin cậy bên-thứ-ba thất bại.
- 5.** Điều nào dưới đây là một yêu cầu đối với CRL?
- A.** Nó phải có địa chỉ e-mail của tất cả chủ sở hữu chứng chỉ.
  - B.** Nó phải chứa một danh sách mọi chứng chỉ đã hết hạn.
  - C.** Nó phải chứa thông tin về tất cả các miền phụ được bao hàm bởi CA.
  - D.** Nó phải được đăng vào một thư mục công cộng.
- 6.** OCSP thực hiện việc gì?
- A.** Nó xem xét CRL cho máy khách và cung cấp trạng thái về việc chứng nhận đang được xác thực.
  - B.** Nó phác thảo các chi tiết của cơ quan cấp chứng nhận, bao gồm cách thức xác minh danh tính, các bước mà CA tuân theo để tạo ra chứng nhận và lý do tại sao CA có thể được tin cậy.
  - C.** Nó cung cấp một bộ các giá trị được đính kèm vào chứng chỉ.
  - D.** Nó cung cấp mã hóa cho chữ ký kỹ thuật số.
- 7.** Tiêu chuẩn X.509 áp dụng cho trường hợp nào sau đây?
- A.** Các nhà cung cấp SSL
  - B.** Chứng nhận kỹ thuật số
  - C.** Danh sách thu hồi chứng nhận
  - D.** Cơ sở hạ tầng khóa công khai

- 8.** Bạn đang duyệt một trang web thì trình duyệt của bạn đưa ra cho bạn thông báo cảnh báo sau: “Đã xảy ra sự cố với chứng nhận bảo mật của trang web này”. Khi bạn kiểm tra chứng nhận, nó chỉ ra rằng CA gốc không đáng tin cậy. Điều gì có khả năng xảy ra nhất đã gây ra lỗi này?
- A.** Chứng nhận đã bị thu hồi.  
**B.** Chứng nhận không có đủ độ dài bit cho giao thức TLS.  
**C.** CSR của máy chủ không được ký bởi một CA đáng tin cậy.  
**D.** Chứng nhận đã hết hạn sử dụng.
- 9.** Bạn được CA cấp chứng nhận và gửi qua email, nhưng tập tin không có phần mở rộng. Email lưu ý rằng CA gốc, CA trung gian và chứng nhận của bạn đều được đính kèm trong tập tin. Chứng nhận của bạn có thể ở định dạng nào?
- A.** DER  
**B.** CER  
**C.** PEM  
**D.** PFX
- 10.** Tại sao chốt lại quan trọng hơn trên thiết bị di động?
- A.** Nó sử dụng mật mã đường cong elliptic.  
**B.** Nó sử dụng ít năng lượng hơn cho các yêu cầu chứng chỉ đã được chốt.  
**C.** Nó làm giảm việc sử dụng băng thông mạng bằng cách kết hợp nhiều yêu cầu CA thành một.  
**D.** Nó cho phép lưu vào bộ nhớ đệm một chứng nhận tốt đã biết khi chuyển vùng tới các mạng có độ tin cậy thấp.

## Đáp án

1. **C.** Đây là một ví dụ về mô hình tin cậy bên-thứ-ba. Mặc dù bạn đang tạo ra các khóa mã hóa trên máy chủ cục bộ nhưng bạn đang nhận được các khóa này được ký bởi một cơ quan bên-thứ-ba để từ đó bạn có thể giới thiệu bên-thứ-ba làm tác nhân đáng tin cậy để người dùng tin tưởng vào khóa của bạn.
2. **D.** Một tổ chức phát hành chứng nhận (CA) là phần cứng và phần mềm quản lý các bit chứng nhận thực tế, các chính sách và thủ tục xác định khi nào chứng nhận được cấp một cách đúng đắn và những người đưa ra và giám sát việc tuân thủ các chính sách.
3. **B.** Bạn có nhiều khả năng tập trung vào mức độ tin cậy mà CA cung cấp cho người dùng hệ thống, vì việc cung cấp độ tin cậy là mục đích chính của CA.
4. **C.** Chứng nhận có thể đã bị thu hồi hoặc bị xóa khỏi danh tính của người dùng đó và không còn hợp lệ bởi tổ chức phát hành chứng nhận.
5. **D.** Danh sách thu hồi chứng nhận (CRL) phải được đăng vào một thư mục công cộng để tất cả người dùng của hệ thống có thể truy vấn nó.
6. **A.** Giao thức Trạng thái Chứng chỉ Trực tuyến (OCSP) là một giao thức trực tuyến sẽ tìm kiếm số seri của chứng nhận trên CRL và cung cấp thông báo trạng thái về chứng nhận cho máy khách.
7. **B.** Tiêu chuẩn X.509 được sử dụng để xác định các thuộc tính của chứng nhận kỹ thuật số.
8. **C.** Trong trường hợp này, yêu cầu ký chứng chỉ (CSR) của máy chủ đã không được ký bởi CA được máy tính điểm cuối tin cậy, vì vậy không thể thiết lập được sự tin cậy bên-thứ-ba. Đây có thể là dấu hiệu của một cuộc tấn công, do đó, chứng nhận phải được

xác minh theo cách thủ công trước khi dữ liệu được cung cấp cho máy chủ web.

9. **C.** Vì chứng nhận bao gồm toàn bộ chuỗi chứng nhận, nên rất có khả năng nó được gửi cho bạn ở định dạng Thư được-Nâng-cao-Quyền-riêng-tư (PEM).
10. **D.** Chốt rất quan trọng trên các thiết bị di động vì chúng [các thiết bị di động] có nhiều khả năng được sử dụng trên nhiều mạng khác nhau, rất nhiều trong số đó có độ tin cậy thấp hơn nhiều so với mạng gia đình của chúng.

## Phần IV

### Vận hành và Ứng phó Sự cố

- Chương 26 Các Công cụ/Đánh giá Bảo mật của Tổ chức
- Chương 27 Các Chính sách, Quy trình và Thủ tục Ứng phó Sự cố
- Chương 28 Điều tra
- Chương 29 Các Kỹ thuật và Biện pháp kiểm soát Giảm nhẹ
- Chương 30 Điều tra pháp y Kỹ thuật số

## Chương 26 Các Công cụ/Đánh giá Bảo mật Tổ chức

### Các Công cụ/Đánh giá Bảo mật Tổ chức

Trong chương này bạn sẽ

- Tìm hiểu sử dụng các công cụ do thám và khám phá mạng,
- Tìm hiểu sử dụng các công cụ để thao túng tập tin,
- Khám phá các môi trường shell và tập lệnh kịch bản,
- Tìm hiểu cách sử dụng các công cụ bắt và phát lại gói tin,
- Tìm hiểu cách sử dụng các công cụ điều tra pháp y,
- Khám phá thế giới các công cụ để hoàn thành các nhiệm vụ có-liên-quan-đến-bảo-mật.

Năng lực thực hiện rất nhiều chức năng bảo mật liên quan đến việc sử dụng các công cụ. Số lượng, phạm vi và chi tiết của các công cụ được sử dụng trong ngành bảo mật có thể lấp đầy toàn bộ quyển sách này, nhưng một hiểu biết cơ bản về bộ công cụ cốt lõi là điều rất quan trọng. Chương này cố gắng cung cấp tiền đề này và mục tiêu Security+ đối với việc sử dụng công cụ.

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 4.1 của kỳ thi CompTIA Security+: Đưa ra một kịch bản, hãy sử dụng công cụ thích hợp để đánh giá tính bảo mật của tổ chức.



#### MÁCH NƯỚC CHO KỲ THI

Chương này chứa đầy các câu lệnh thực-hành cần phải được sử dụng để học tập. Con đường để tìm hiểu các lệnh

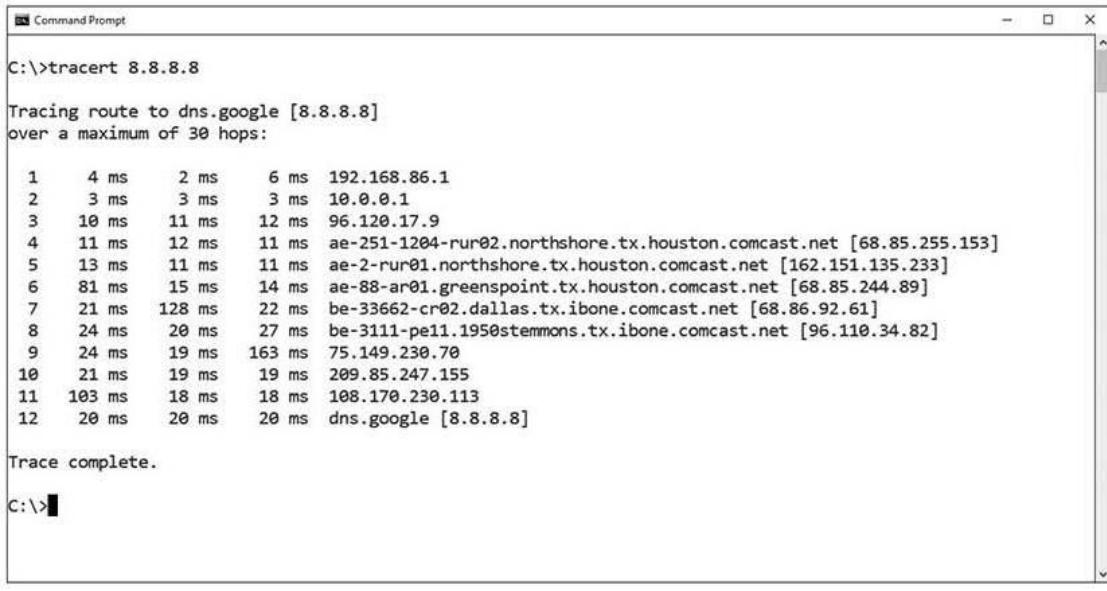
này chính là sử dụng chúng. Đây không phải là một chương để đọc-và-nhớ, mà là một chương vừa-học-vừa-làm. Các lệnh Linux có thể hơi rắc rối đối với một số người, vì vậy bạn nên thực hành. Chúng tôi khuyên bạn nên thực hành với các lệnh Linux được mô tả và truy cập các trang hướng dẫn Linux, là hướng dẫn tham khảo trực tuyến để biết các ví dụ về một loạt các lệnh Linux: <https://www.kernel.org/doc/manpages/>.

## Do thám và Khám phá Hệ thống Mạng

Mạng cũng giống như hầu hết các cơ sở hạ tầng - bạn không bao giờ xem xét hoặc quan tâm đến nó cho đến khi nó không hoạt động. Và khi bạn muốn xem xét, bạn phải làm điều đó như thế nào? Một loạt các công cụ có thể được sử dụng để cho phép bạn xem xét hoạt động bên trong của một mạng và chúng được đề cập trong các phần tiếp theo.

### tracert/traceroute

Lệnh *tracert* là một câu lệnh của Windows để theo dõi định tuyến mà các gói tin đi qua mạng. Câu lệnh tracert cung cấp một danh sách bao gồm các máy chủ, bộ chuyển mạch và bộ định tuyến theo thứ tự gói tin đi qua chúng, cung cấp dấu vết của định tuyến mạng từ nguồn đến đích. Vì tracert sử dụng Giao thức Thông điệp Kiểm soát Internet (ICMP) nên nếu ICMP bị chặn, tracert sẽ không cung cấp được thông tin. Trên các hệ thống Linux và macOS, lệnh có chức năng tương tự là traceroute. Hình 26-1 minh họa cho việc sử dụng lệnh tracert để theo dõi định tuyến từ hệ thống Windows trên mạng riêng đến máy chủ DNS của Google.



```
Command Prompt

C:\>tracert 8.8.8.8

Tracing route to dns.google [8.8.8.8]
over a maximum of 30 hops:

 1  4 ms   2 ms   6 ms  192.168.86.1
 2  3 ms   3 ms   3 ms  10.0.0.1
 3  10 ms  11 ms  12 ms  96.120.17.9
 4  11 ms  12 ms  11 ms  ae-251-1284-rur02.northshore.tx.houston.comcast.net [68.85.255.153]
 5  13 ms  11 ms  11 ms  ae-2-rur01.northshore.tx.houston.comcast.net [162.151.135.233]
 6  81 ms  15 ms  14 ms  ae-88-ar01.greenspoint.tx.houston.comcast.net [68.85.244.89]
 7  21 ms  128 ms 22 ms  be-33662-cr02.dallas.tx.ibone.comcast.net [68.86.92.61]
 8  24 ms  20 ms  27 ms  be-3111-pe11.1950stemmons.tx.ibone.comcast.net [96.110.34.82]
 9  24 ms  19 ms  163 ms  75.149.230.70
10  21 ms  19 ms  19 ms  209.85.247.155
11  103 ms 18 ms  18 ms  108.170.230.113
12  20 ms  20 ms  20 ms  dns.google [8.8.8.8]

Trace complete.

C:\>
```

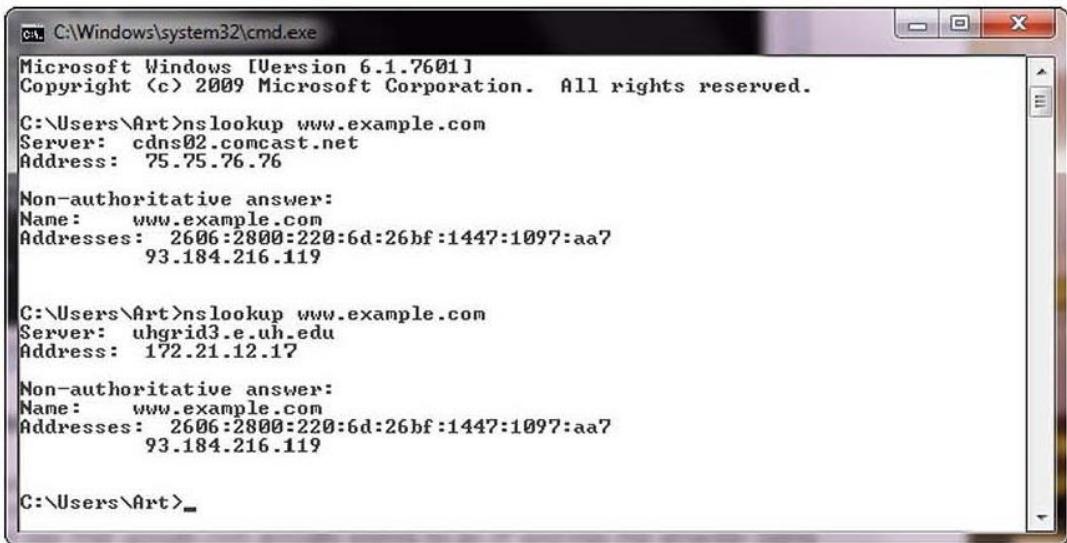
**Hình 26-1** Ví dụ về [câu lệnh] tracert



**MÁCH NƯỚC CHO KỲ THI** Các câu lệnh tracert và traceroute hiển thị tuyến đường mà một gói tin đi đến đích, ghi lại số lượng các bước đọc đường đi. Có những công cụ tuyệt vời để sử dụng để xem xét vị trí nơi một gói tin có thể bị treo trong quá trình truyền tải.

### **nslookup/dig**

Hệ thống Tên Miền (DNS) được sử dụng để chuyển đổi một tên miền con- người-có-thể-đọc-được thành một địa chỉ IP. Đây không phải là một hệ thống đơn lẻ mà là một hệ thống phân cấp bao gồm nhiều máy chủ DNS, từ các máy chủ gốc trên mạng chính của Internet cho đến các bản sao tại nhà cung cấp dịch vụ Internet (ISP), bộ định tuyến tại nhà và máy cục bộ của bạn, mỗi một trong số đó hình thành nên một bộ nhớ đệm DNS. Để kiểm tra truy vấn DNS cho một địa chỉ cụ thể, bạn có thể sử dụng câu lệnh *nslookup*. Hình 26-2 cho thấy một loạt các truy vấn DNS được thực thi trên máy Windows. Trong yêu cầu đầu tiên, máy chủ DNS là với ISP, trong khi ở yêu cầu thứ hai, máy chủ DNS là từ kết nối mạng riêng ảo (VPN). Giữa hai yêu cầu, các kết nối mạng đã được thay đổi, dẫn đến việc tra cứu DNS khác nhau.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright © 2009 Microsoft Corporation. All rights reserved.

C:\Users\Art>nslookup www.example.com
Server: cdns02.comcast.net
Address: 75.75.76.76

Non-authoritative answer:
Name: www.example.com
Addresses: 2606:2800:220:6d:26bf:1447:1097:aa7
93.184.216.119

C:\Users\Art>nslookup www.example.com
Server: uhgrid3.e.uh.edu
Address: 172.21.12.17

Non-authoritative answer:
Name: www.example.com
Addresses: 2606:2800:220:6d:26bf:1447:1097:aa7
93.184.216.119

C:\Users\Art>_
```

**Hình 26-2** nslookup của một truy vấn DNS

Đôi khi, nslookup sẽ trả về kết quả nonauthoritative, như được minh họa trong Hình 26-3. Điều này thường có nghĩa là kết quả từ một bộ nhớ đệm ngược lại với một máy chủ có câu trả lời có thẩm quyền (nghĩa là, được biết là hiện tại), chẳng hạn như một máy chủ DNS.



```
C:\Windows\system32\cmd.exe
C:\Users\Art>nslookup www.google.com
Server: uhgrid3.e.uh.edu
Address: 172.21.12.17

Non-authoritative answer:
Name: www.google.com
Addresses: 2607:f8b0:4001:c05::63
74.125.193.105
74.125.193.147
74.125.193.104
74.125.193.103
74.125.193.99
74.125.193.106

C:\Users\Art>_
```

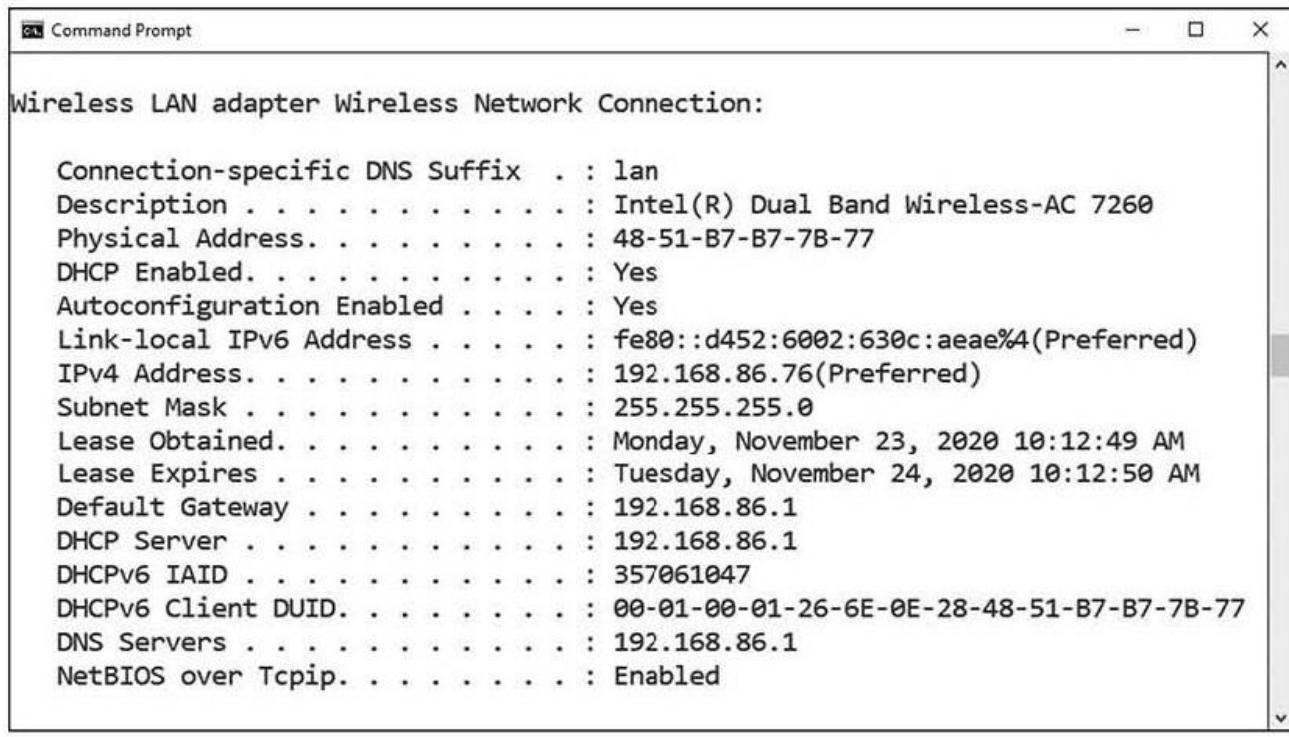
**Hình 26-3** Bộ nhớ đệm phản hồi một truy vấn DNS

Trong khi câu lệnh nslookup hoạt động trên các hệ thống Windows thì câu lệnh *dig*, là viết tắt của Người dò tìm Thông tin Miền (Domain Information Groper), hoạt động trên các hệ thống Linux. Một điểm khác biệt là câu lệnh dig được thiết kế để trả về các câu trả lời ở định dạng dễ phân tích cú pháp và đưa vào các tập lệnh, và đây là đặc điểm chung của các tiện ích dòng lệnh Linux.

### **ipconfig/ifconfig**

Các câu lệnh *ipconfig* (dành cho Windows) và *ifconfig* (dành cho Linux) là những công cụ dòng-lệnh để thao tác trên các giao diện mạng trên một hệ thống. Chúng có khả năng liệt kê ra những tham số của giao diện và kết nối mạng, các tham số thay thế, và ngắt/gia hạn (release/renew) các kết nối. Nếu bạn gặp các vấn đề với kết nối mạng, đây là một trong số những công cụ đầu tiên mà bạn nên sử dụng để xác minh thiết lập mạng của hệ điều hành và các giao diện của nó.

Câu lệnh ip trong Linux được sử dụng để hiển thị và thao tác việc định tuyến, các thiết bị, định tuyến theo chính sách và các đường hầm. Câu lệnh ifconfig là một câu lệnh quan trọng đối với khắc phục sự cố vì nó hiển thị các cấu hình TCP/IP hiện hành trên một hệ thống cục bộ. Câu lệnh này hiển thị những thông tin về bộ tiếp hợp (adapter) chẳng hạn như địa chỉ MAC, các địa chỉ IP hiện tại (cả IPv4 và IPv6), mặt nạ mạng con, cửa sổ mặc định, cũng như là các máy chủ DNS và liệu DHCP có được kích hoạt hay không. Hình 26-4 hiển thị một số thông tin sẵn có từ câu lệnh ipconfig trên một máy tính Windows. Đây là một công cụ khắc phục sự cố quan trọng vì khi bạn không thể kết nối tới một thứ gì đó, đây là vị trí đầu tiên để bắt đầu khám phá các kết nối mạng, vì nó sẽ cung cấp cho bạn tất cả những thiết lập của bạn.



```
Wireless LAN adapter Wireless Network Connection:

Connection-specific DNS Suffix . : lan
Description . . . . . : Intel(R) Dual Band Wireless-AC 7260
Physical Address. . . . . : 48-51-B7-B7-7B-77
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . : fe80::d452:6002:630c:aeae%4(Preferred)
IPv4 Address. . . . . : 192.168.86.76(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Monday, November 23, 2020 10:12:49 AM
Lease Expires . . . . . : Tuesday, November 24, 2020 10:12:50 AM
Default Gateway . . . . . : 192.168.86.1
DHCP Server . . . . . : 192.168.86.1
DHCPv6 IAID . . . . . : 357061047
DHCPv6 Client DUID. . . . . : 00-01-00-01-26-6E-0E-28-48-51-B7-B7-7B-77
DNS Servers . . . . . : 192.168.86.1
NetBIOS over Tcpip. . . . . : Enabled
```

**Hình 26-4** Ví dụ về ipconfig

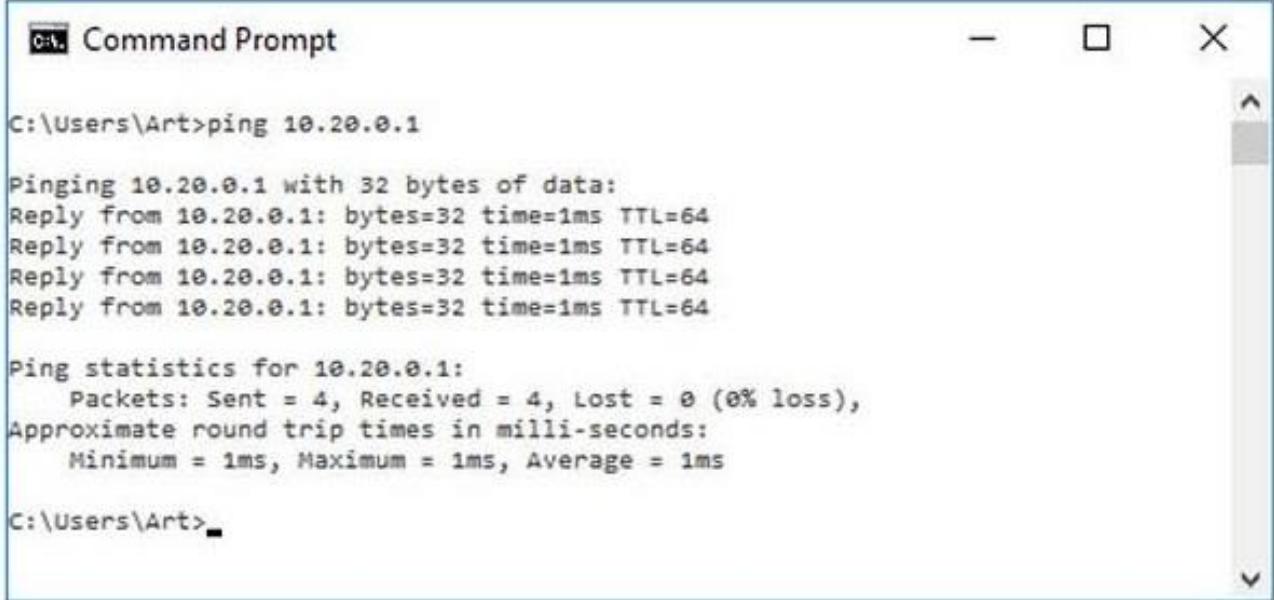
### nmap

nmap là một công cụ quét công mã nguồn mở hoàn toàn miễn phí được phát triển bởi Gordon Lyon và đã trở thành tiện ích lập bản đồ mạng tiêu chuẩn dành cho Windows và Linux kể từ năm 1999. Câu lệnh *nmap* là một câu lệnh để khởi đầu và chạy tiện ích nmap. Nmap được sử dụng để khám phá những hệ thống đang ở trên một mạng và các cổng và dịch vụ đang mở trên những hệ thống đó. Công cụ này có rất nhiều tính năng bổ sung, chẳng hạn như in dấu vân tay của Hệ điều hành, tìm kiếm các thiết bị giả mạo và khám phá các dịch vụ và thậm chí cả các phiên bản của ứng dụng. Nó hoạt động thông qua dòng lệnh, vì vậy nó rất dễ được lập trình theo tập lệnh kịch bản (script). Nó cũng có một giao diện GUI (giao diện đồ họa người dùng – graphical user interface) được gọi là Zenmap. Nmap hoạt động trên một loạt các hệ điều hành, bao gồm Microsoft Windows, Linux và macOS. Đây là một trong số 10 công cụ hàng đầu được sử dụng

thường xuyên bởi các quản trị viên hệ thống. Nmap bao gồm một công cụ lập trình tập lệnh kịch bản sử dụng ngôn ngữ lập trình Lua để viết, lưu lại và chia sẻ các tập lệnh kịch bản để có thể tự động hóa những kiểu quét khác nhau. Tất cả các loại nhiệm vụ có thể được tự động hóa, bao gồm những quá trình kiểm tra thường xuyên các lỗ hổng cơ sở hạ tầng mạng nổi tiếng.

### **ping / pathping**

Lệnh *ping* gửi các yêu cầu dội lại (echo) cho một máy được chỉ định để xác định xem liệu giao tiếp có khả thi không. Cú pháp là **ping** [*tùy chọn*] **tên/địa chỉ máy đích**. Các tùy chọn bao gồm những mục chẳng hạn như phân giải tên, ping bao nhiêu gói, kích cỡ dữ liệu, đếm TTL, v.v... Hình 26-5 minh họa một lệnh ping trên một máy tính Windows.



```
C:\Users\Art>ping 10.20.0.1

Pinging 10.20.0.1 with 32 bytes of data:
Reply from 10.20.0.1: bytes=32 time=1ms TTL=64

Ping statistics for 10.20.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Users\Art>
```

**Hình 26-5** Lệnh ping

Lệnh pathping là một tiện ích dựa-trên-TCP/IP cung cấp thêm dữ liệu bổ sung ngoài những gì có được từ lệnh ping. Pathping trước tiên sẽ hiển thị kết quả đường dẫn của bạn như thể bạn đang sử dụng lệnh tracert

hoặc traceroute. Pathping sau đó sẽ tính toán thông tin tổn thất [các gói tin bị mất], như được minh họa trong Hình 26-6.

```
C:\>pathping 96.120.17.9

Tracing route to 96.120.17.9 over a maximum of 30 hops

0 Art-PC.lan [192.168.86.76]
1 192.168.86.1
2 10.0.0.1
3 96.120.17.9

Computing statistics for 75 seconds...
      Source to Here   This Node/Link
Hop  RTT     Lost/Sent = Pct  Lost/Sent = Pct  Address
  0          |           0/ 100 = 0%    |  Art-PC.lan [192.168.86.76]
  1  14ms    0/ 100 = 0%    0/ 100 = 0%    |  192.168.86.1
  2  19ms    0/ 100 = 0%    0/ 100 = 0%    |  10.0.0.1
  3  26ms    1/ 100 = 1%    0/ 100 = 0%    96.120.17.9

Trace complete.

C:\>
```

**Hình 26-6** Ví dụ về pathping



# MÁCH NƯỚC CHO KỲ THI

nối giữa các hệ thống.

Lệnh ping được sử dụng để kiểm tra kết

## hping

*Hping* là một công cụ tạo ra gói tin TCP / IP cho phép người dùng tạo các gói IP, TCP, UDP và ICMP thô ngay từ ban đầu. Công cụ này cung cấp một phương tiện để thực hiện một loạt các hoạt động mạng, bao gồm điều

gì bạn có thể thực hiện với các giao thức đó đều có thể được tạo thành trong một gói. Điều này bao gồm quét cổng, tạo các gói tin ICMP, khám phá máy chủ và hơn thế nữa. Phiên bản hiện tại là hping3 và nó có sẵn trên hầu hết các hệ điều hành, bao gồm cả Windows và Linux.

Giống như tất cả các lệnh Linux, hping có thể được lập trình trong các tập lệnh kịch bản Bash để đạt được chức năng cao hơn. Kết quả đầu ra cũng có thể được chuyển đến các lệnh khác. Hping cũng hoạt động với chức năng lập trình kịch bản Tcl được nhúng, giúp mở rộng thêm tính hữu ích của nó cho các quản trị viên hệ thống. Giữa rất nhiều tùy chọn và khả năng tạo kịch bản nguyên thủy, hping cung cấp một loạt các chức năng, bao gồm cả việc tạo ra các backdoor được-bảo-vệ-bằng-mật-khẩu được chuyển đến các dịch vụ khác. Sức mạnh đến từ khả năng lập trình, các tùy chọn và công việc sáng tạo của quản trị viên hệ thống.

### **netstat**

Lệnh *netstat* được sử dụng để giám sát các kết nối mạng đến và đi từ hệ thống. Dưới đây là một số ví dụ về cách bạn có thể sử dụng netstat:

- **netstat -a** Liệt kê mọi kết nối hoạt động và các cổng đang lắng nghe
- **netstat -at** Liệt kê mọi kết nối TCP đang hoạt động
- **netstat -an** Liệt kê mọi kết nối UDP đang hoạt động.

Có rất nhiều tùy chọn khác đang sẵn có và rất hữu ích. Lệnh netstat có sẵn trên Windows và Linux, nhưng tính khả dụng của một số khóa chuyển lệnh netstat và cú pháp lệnh netstat khác có thể khác nhau giữa các hệ điều hành.



**MÁCH NƯỚC CHO KỲ THI** Lệnh netstat rất hữu ích để xem xét mọi cổng đang lắng nghe trên một máy tính và xác định những kết nối nào đang hoạt động.

### **netcat**

*Netcat* là một tiện ích mạng được thiết kế cho các môi trường Linux. Nó đã được chuyển sang Windows nhưng không được sử dụng một cách thường xuyên trong môi trường Windows. Lệnh thực sự để gọi netcat là **nc -options - address**.

Tiện ích netcat là công cụ được lựa chọn trong Linux để đọc và ghi vào các kết nối mạng sử dụng TCP hoặc UDP. Giống như tất cả các tiện ích dòng-lệnh của Linux, nó được thiết kế cho các tập lệnh kịch bản và tự động hóa. Netcat có một loạt các chức năng. Nó hoạt động như một kết nối với mạng và có thể đóng vai trò như một bộ phát hoặc một bộ thu, và với sự chuyển hướng, nó có thể biến hầu như bất kỳ tiến trình đang hoạt động nào thành một máy chủ. Nó có thể lắng nghe trên một cổng và chuyển đầu vào mà nó nhận được cho tiến trình đã được xác định.



**MÁCH NƯỚC CHO KỲ THI** Bạn nên tìm hiểu mỗi công cụ này trông sẽ như thế nào khi được sử dụng. Nếu được trình bày với kết quả từ một trong các công cụ, bạn nên có khả năng xác định công cụ đã được sử dụng và công cụ đang thực hiện hành động nào.

### **Máy Quét IP**

*Máy quét IP* đúng như ý nghĩa của tên gọi của chúng: chúng quét các mạng IP và có thể báo cáo về trạng thái của các địa chỉ IP. Có rất nhiều công cụ quét miễn phí và thương mại, và hầu hết đều đi kèm với chức

năng nhiều hơn đáng kể so với việc chỉ báo cáo về việc sử dụng địa chỉ. Nếu tất cả những gì bạn muốn là địa chỉ, có nhiều công cụ khám phá mạng dạng dòng-lệnh đơn giản có thể cung cấp những câu trả lời đó. Ví dụ, nếu bạn chỉ muốn quét mạng LAN cục bộ của mình, lệnh **arp - a** sẽ thực hiện điều đó. Nếu bạn muốn có nhiều chức năng hơn, bạn có thể sử dụng chương trình nmap đã được đề cập trước đó trong chương. Một giải pháp khác là Nessus, một sản phẩm thương mại sẽ được đề cập ở phần sau của chương.

### **arp**

Lệnh *arp* được thiết kế để tương tác với bộ nhớ đệm Giao thức Phân giải Địa chỉ (Address Resolution Protocol - ARP) của hệ điều hành trên một hệ thống. Trong việc di chuyển các gói tin giữa các máy, một thiết bị đôi khi cần phải biết được nơi để gửi gói tin đến bằng cách sử dụng MAC hoặc địa chỉ lớp 2. ARP giải quyết vấn đề này thông qua 4 kiểu thông điệp cơ bản sau:

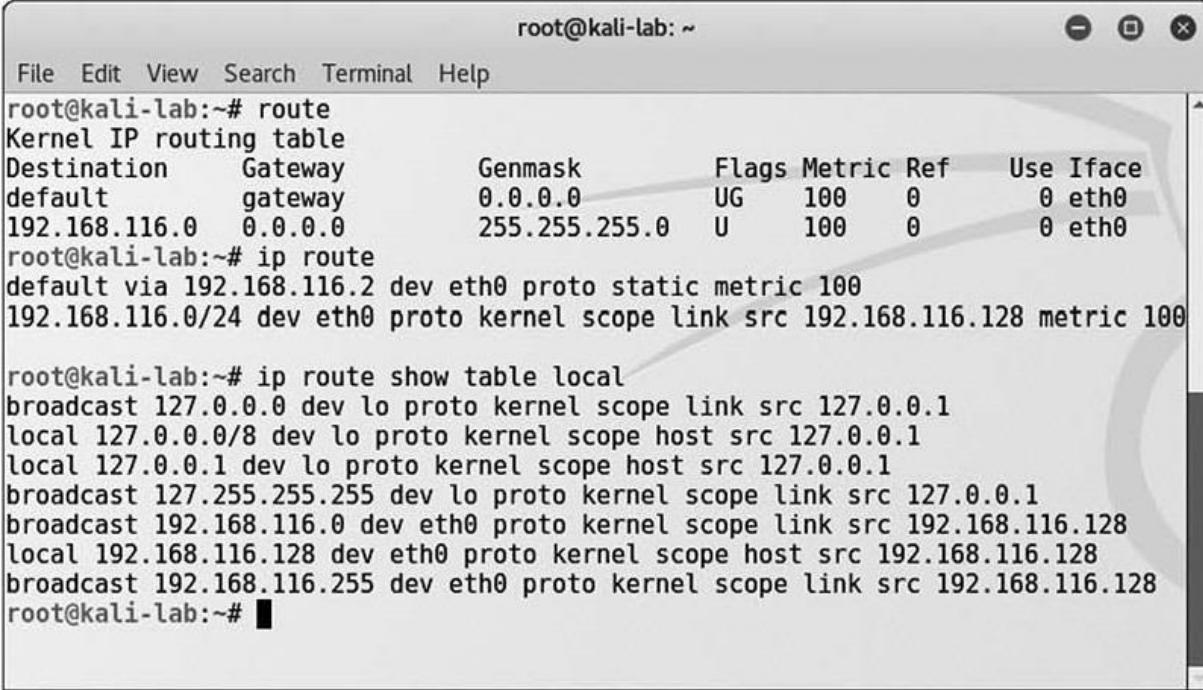
- **yêu cầu ARP** "Địa chỉ IP này là của ai?"
- **phản hồi ARP** "Tôi có địa chỉ IP đó, địa chỉ MAC của tôi là..."
- **yêu cầu ARP đảo ngược (RARP)** "Địa chỉ MAC này là của ai?"
- **phản hồi RARP** "Tôi có địa chỉ MAC đó, địa chỉ IP của tôi là..."

Các thông điệp này được sử dụng cùng với một bảng ARP của thiết bị, nơi chứa một dạng bộ nhớ ngắn-hạn được liên kết với các phần tử dữ liệu này. Các lệnh được sử dụng như một dạng tra cứu đơn giản. Khi một máy gửi một yêu cầu ARP đến mạng, phản hồi sẽ được nhận và được nhập vào tất cả các thiết bị nghe thấy câu trả lời. Điều này tạo điều kiện thuận lợi cho việc tra cứu địa chỉ hiệu quả, nhưng cũng khiến hệ thống trở thành đối tượng của cuộc tấn công.

Lệnh arp cho phép quản trị viên hệ thống có khả năng xem xét và thao tác với bộ đệm ARP trên hệ thống. Bằng cách này, họ có thể xem liệu các mục nhập có bị giả mạo hay không hoặc liệu các vấn đề khác, chẳng hạn như lỗi, có xảy ra hay không.

### route

Lệnh *route* hoạt động trong cả các hệ thống Linux lẫn Windows để cung cấp thông tin về các tham số định tuyến hiện tại và để thao tác trên các tham số này. Ngoài việc liệt kê bảng định tuyến hiện tại, nó [lệnh route] còn có khả năng sửa đổi bảng định tuyến. Hình 26-7 minh họa 3 ví dụ về định tuyến trên một hệ thống Linux. Đầu tiên là một hiển thị đơn giản của bảng định tuyến IP của kernel. Thứ hai trình bày một kết quả tương tự như khi sử dụng lệnh ip. Và cuối cùng là sử dụng lệnh ip để có được thông tin chi tiết về bảng [định tuyến] cục bộ với các địa chỉ đích được chỉ định cho localhost.



```
root@kali-lab: ~
File Edit View Search Terminal Help
root@kali-lab:~# route
Kernel IP routing table
Destination      Gateway          Genmask        Flags Metric Ref  Use Iface
default          gateway          0.0.0.0        UG    100    0        0 eth0
192.168.116.0   0.0.0.0        255.255.255.0  U     100    0        0 eth0
root@kali-lab:~# ip route
default via 192.168.116.2 dev eth0 proto static metric 100
192.168.116.0/24 dev eth0 proto kernel scope link src 192.168.116.128 metric 100

root@kali-lab:~# ip route show table local
broadcast 127.0.0.0 dev lo proto kernel scope link src 127.0.0.1
local 127.0.0.0/8 dev lo proto kernel scope host src 127.0.0.1
local 127.0.0.1 dev lo proto kernel scope host src 127.0.0.1
broadcast 127.255.255.255 dev lo proto kernel scope link src 127.0.0.1
broadcast 192.168.116.0 dev eth0 proto kernel scope link src 192.168.116.128
local 192.168.116.128 dev eth0 proto kernel scope host src 192.168.116.128
broadcast 192.168.116.255 dev eth0 proto kernel scope link src 192.168.116.128
root@kali-lab:~#
```

**Hình 26-7** Các câu lệnh route và ip trong Linux

## **curl**

*Curl* là một công cụ được thiết kế để truyền dữ liệu đến hoặc đi từ một máy chủ mà không cần sự tương tác của người dùng. Nó hỗ trợ một loạt các giao thức (bao gồm DICT, FILE, FTP, FTPS, Gopher, HTTP, HTTPS, IMAP, IMAPS, LDAP, LDAPS, MQTT, POP3, POP3S, RTMP, RTMPS, RTSP, SCP, SFTP, SMB, SMBS, SMTP, SMTPL, Telnet và TFTP) và hoạt động giống như một con dao của quân đội Thụy Sĩ để tương tác với máy chủ. Ban đầu được thiết kế để tương tác với các URL, curl đã được mở rộng thành một công cụ đa năng hỗ trợ cho nhiều giao thức. Nó hoạt động trên cả hệ thống Linux lẫn Windows, mặc dù các tùy chọn lệnh hơi khác nhau.

Dưới đây là một ví dụ đơn giản về việc sử dụng curl để mô phỏng một yêu cầu GET cho một URL trang web:

```
curl https://www.example.com
```

## **theHarvester**

*theHarvester* là một chương trình dựa-trên-Python được thiết kế để hỗ trợ cho người kiểm tra thâm nhập thu thập thông tin trong phần thăm dò của kiểm tra thâm nhập. Đây là một công cụ rất hữu ích để khám phá những gì đang có sẵn công khai về tổ chức của bạn trên Web và nó có thể cung cấp thêm thông tin về nhân viên, email và tên miền phụ bằng cách sử dụng các nguồn công khai khác nhau như công cụ tìm kiếm, các máy chủ khóa PGP và cơ sở dữ liệu Shodan. Được thiết kế cho Linux và được bao gồm như một phần của Kali và các bản phân phối kiểm nghiệm thâm nhập khác, *theHarvester* được minh họa trong Hình 26-8 để tìm kiếm 500 email đầu tiên từ miền kali.org bằng cách sử dụng Google.

```
root@kali-lab: ~
File Edit View Search Terminal Help
Firmware
*****
* [+] TheHarvester Ver. 2.7
* Coded by Christian Martorella
* Edge-Security Research
* cmartorella@edge-security.com
*****
[-] Searching in Google:
    Searching 0 results...
    Searching 100 results...
    Searching 200 results...

[+] Emails found:
-----
devel@kali.org
steev@kali.org
dookie@kali.org

[+] Hosts found in search engines:
-----
[-] Resolving hostnames IPs...
192.99.200.113:Http.kali.org
192.99.45.140:archive.kali.org
192.124.249.169:bugs.kali.org
192.99.200.113:cimage.kali.org
50.116.58.136:docs.kali.org
54.39.243.51:downloads.kali.org
192.124.249.12:forums.kali.org
192.99.200.113:http.kali.org
54.39.49.227:old.kali.org
192.124.249.9:pkg.kali.org
192.99.200.113:security.kali.org
192.124.249.56:status.kali.org
192.124.249.6:tools.kali.org
192.124.249.10:www.kali.org
root@kali-lab:~#
```

## Hình 26-8 theHarvester

**sn1per**

*Sn1per* là một công cụ dựa-trên-Linux được sử dụng bởi người kiểm nghiệm xâm nhập. *Sn1per* là một máy quét tự động được thiết kế để thu thập một lượng lớn thông tin khi quét các lỗ hổng. Nó chạy một loạt các tập lệnh được tự động hóa để liệt kê các máy chủ, cổng đang mở và

những lỗ hổng bảo mật, đồng thời được thiết kế để tích hợp với công cụ kiểm tra xâm nhập Metasploit. Sn1per còn đi xa hơn việc chỉ quét, nó cũng có thể brute force các cổng đang mở, brute force tên miền phụ và hệ thống DNS, quét các ứng dụng web để tìm ra các lỗ hổng phổ biến và chạy các tập lệnh nmap được nhắm mục tiêu trên các cổng đang mở cũng như các mô-đun khai thác và quét Metasploit đã được nhắm mục tiêu. Bộ công cụ này xuất hiện dưới dạng phiên bản cộng đồng miễn phí, với phạm vi hạn chế, cũng như phiên bản chuyên nghiệp không giới hạn cho các công ty và người kiểm tra xâm nhập.

### **scanless**

*Scanless* là một tiện ích dòng-lệnh để tương tác với các trang web để có thể thực hiện việc quét các cổng như là một phần của công việc kiểm tra xâm nhập. Khi bạn sử dụng công cụ này, địa chỉ IP nguồn đổi với quá trình quét là của trang web, không phải là địa chỉ IP của máy của bạn. Được viết bằng Python, với một giao diện đơn giản, scanless ẩn danh các lần quét cổng của bạn.

### **dnsenum**

*dnsenum* là một tập lệnh kịch bản Perl được thiết kế liệt kê thông tin DNS. Dnsenum sẽ liệt kê các mục nhập DNS, bao gồm tên miền phụ, các bản ghi MX và địa chỉ IP. Nó có thể tương tác với Whois, một bản ghi công khai xác định chủ sở hữu miền, để thu thập thêm thông tin bổ sung. Dnsenum hoạt động trên các bản phân phối Linux hỗ trợ Perl.



**MÁCH NƯỚC CHO KỲ THI**      Liệt kê DNS có thể được sử dụng để thu thập thông tin chặng hạn như các tên và địa chỉ IP của các hệ thống được nhắm mục tiêu.

## Nessus

Nessus là một trong những công cụ quét lỗ hổng bảo mật hàng đầu trên thị trường. Nó có phiên bản miễn phí, với khả năng địa chỉ IP bị hạn chế và các phiên bản thương mại với đầy đủ chức năng. Nessus được thiết kế để thực hiện nhiều loại thử nghiệm trên hệ thống, bao gồm việc sử dụng thông tin đăng nhập của người dùng, kiểm tra mức bản vá, các cấu hình sai phỏng biển, tấn công mật khẩu, v.v... Được thiết kế như một bộ công cụ kiểm tra cấu hình và lỗ hổng đầy đủ, Nessus thường được sử dụng để kiểm tra các hệ thống tuân thủ các tiêu chuẩn bảo mật khác nhau như PCI DSS, SOX và các sơ đồ tuân thủ khác. Phiên bản miễn phí của Nessus là nguồn gốc của OpenVAS fork, đây là một trình quét lỗ hổng bảo mật miễn phí phổ biến.

## Cuckoo

Cuckoo là một hộp cát (sandbox) được sử dụng để phân tích phần mềm độc hại. Cuckoo được thiết kế để cho phép một phương tiện kiểm tra một tập tin đáng ngờ và xác định xem nó thực hiện những gì. Nó là phần mềm mã nguồn mở, miễn phí có thể chạy trên cả Linux lẫn Windows. Cuckoo là một công cụ bảo mật phổ biến được sử dụng để điều tra các tập tin đáng ngờ, vì nó có thể cung cấp báo cáo về các lệnh gọi hệ thống, lệnh gọi API, phân tích mạng và phân tích bộ nhớ.



**MÁCH NƯỚC CHO KỲ THI** Kỳ thi Security+ sẽ kiểm tra kiến thức của bạn về các công cụ thăm dò và khám phá mạng đã được nêu chi tiết trước đây. Hãy thực hành với từng công cụ trong sổ chúng và, với một kịch bản, hãy có khả năng xác định và sử dụng công cụ thích hợp!

## Thao tác Tập tin

Trong các hệ thống máy tính, hầu hết thông tin đều có thể được biểu diễn dưới dạng tập tin. Tập tin là tập tin, cũng như các thư mục và thậm chí toàn bộ hệ thống lưu trữ. Khái niệm tập là giao diện cơ bản của thông tin. Do điều này, các công cụ thao tác tập tin có khả năng quản lý rất nhiều tác vụ. Khi nhiều thao tác được viết theo kịch bản, khả năng thao tác một tập tin, trả về các phần tử hoặc bản ghi cụ thể, có tính tiện dụng tuyệt vời. Phần tiếp theo này xem xét một loạt các công cụ được sử dụng để thao tác các tập tin trong hệ thống Linux.

### **head**

*Head* là một tiện ích được thiết kế để trả về dòng đầu tiên của một tập tin. Một tùy chọn phổ biến là số lượng dòng mà một người muốn được trả về. Ví dụ, **head -5** trả về kết quả là 5 dòng đầu tiên của một tập tin.

### **tail**

*Tail* là một tiện ích được thiết kế để trả về các dòng cuối cùng của một tập tin. Một tùy chọn phổ biến là số lượng dòng mà một người muốn được trả về. Ví dụ, **tail -5** sẽ trả về 5 dòng cuối của một tập tin.

### **cat**

*Cat* là một câu lệnh Linux, là từ viết tắt của concatenate, có thể được sử dụng để tạo ra và thao tác các tập tin. Nó có thể hiển thị nội dung của một tập tin, xử lý nhiều tập tin, và có thể được sử dụng để nhập dữ liệu vào từ stdin, vốn là một luồng đầu vào, vào một tập tin nếu tập tin không tồn tại. Dưới đây là một ví dụ

```
#cat textfile.txt
```

Lệnh **cat** có thể được kết chuyển thông qua **more** hoặc **less** để giới hạn việc cuộn các tập tin dài:

```
#cat textfile.txt | more
```

Nếu bạn muốn có một số dòng trong kết quả đầu ra, bạn có thể bổ sung thêm tùy chọn **-n**. Kết quả đầu ra có thể được kết chuyển thông qua một loạt các câu lệnh Linux khác, mang lại khả năng thao tác đáng kể. Ví dụ, bạn có thể tổng hợp 4 tập tin và sắp xếp kết quả đầu ra thành một tập tin thứ năm, giống như:

```
#cat  textfile1.txt  textfile2.txt  textfile3.txt  
textfile4.txt | sort > textile5.txt
```

### **grep**

*Grep* là một tiện ích Linux có thể thực hiện tìm kiếm đối-sánh-mẫu theo nội dung tập tin. Tên grep xuất phát từ “Tìm kiếm trên toàn cầu cho Cụm từ Thông dụng và In các dòng phù hợp” (Globally search for Regular Expression and Print the matching files). Grep xuất hiện ngay từ đầu của Hệ điều hành Unix và được viết bởi Ken Thompson. Ngày nay, việc sử dụng grep là rất phổ biến. Nó có thể đếm số lượng kết quả phù hợp và có thể tìm các dòng có cụm từ phù hợp, phân biệt chữ hoa chữ thường hoặc không phân biệt chữ hoa chữ thường. Nó có thể sử dụng các neo (đối sánh dựa trên bắt đầu hoặc kết thúc của một từ), các ký tự đại diện và tìm kiếm phủ định (tìm các dòng không chứa một phần tử được chỉ định) và nó hoạt động với các công cụ khác thông qua việc chuyển hướng các đầu vào và đầu ra.

Grep có rất nhiều tùy chọn, bao gồm cả việc sử dụng các cụm từ chính quy để thực hiện đối sánh. Dưới đây là một ví dụ về các tùy chọn phổ biến hơn:

```
grep [options] pattern [files]
Options Description
-c : This prints only a count of the lines that match a pattern
-h : Display the matched lines, but do not display the filenames.
-i : Ignores, case for matching
-l : Displays list of a filenames only.
-n : Display the matched lines and their line numbers.
-v : This prints out all the lines that do not matches the pattern
-w : Match whole word
-o : Print only the matched parts of a matching line, with each such part on
a separate output line.
```

Có rất nhiều tùy chọn khác, bao gồm hiển thị các dòng trước và sau đối sánh. Để có cảm nhận đầy đủ về phạm vi của các lựa chọn, hãy tham khảo man page về grep.

## chmod

*chmod* là một câu lệnh Linux được sử dụng để thay đổi các quyền truy cập của một tập tin. Định dạng chung của câu lệnh là

```
chmod <các tùy chọn> <các quyền> <tên tập tin>
```

```
sdfg
```

```
chmod u=rwx, g=rx, o=r <tên tập tin>
```

```
chmod 754 <tên tập tin>
```

Ký hiệu bát phân hoạt động như sau: 4 – “đọc”, 2 – “ghi”, 1 – “thực thi” và 0 – “không có quyền”. Do đó, đối với người dùng, 7 là sự kết hợp của các quyền 4 + 2 + 1 (đọc, ghi và thực thi). Đối với nhóm, 5 là 4 + 0 + 1 (đọc, không ghi, và thực thi), và với tất cả những người khác, 4 là 4 + 0 + 0 (đọc, không ghi, không thực thi).

## logger

Câu lệnh Linux *logger* là cách mà bạn có thể bổ sung thêm thông tin nhật ký tập tin vào /var/log/syslog. Câu lệnh logger hoạt động từ giao diện dòng lệnh, từ các tập lệnh kịch bản, hoặc từ các tập tin khác, do đó cung

cấp một phương tiện linh hoạt để tạo ra các mục nhập nhật ký. Cú pháp khá đơn giản:

Logger <thông điệp để thêm vào nhật ký>

Câu lệnh này sẽ bổ sung đoạn văn bản vào trong phần tùy chọn vào tập tin syslog.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy tìm hiểu về mục đích của các câu lệnh thao tác tập tin trong Linux. Với một kịch bản, hãy được chuẩn bị (sẵn sàng) để thực hiện câu lệnh thích hợp.

### **Môi trường Shell và Script**

Một trong những khía cạnh mạnh mẽ hơn của môi trường Linux là khả năng tạo các tập lệnh shell. Bằng cách kết hợp một loạt các chức năng và thông qua việc sử dụng chuyển hướng đầu vào và kết quả đầu ra, người ta có thể thao túng những dữ liệu quan trọng. Hãy lấy một tập tin PCAP làm ví dụ. Giả sử rằng bạn cần trích xuất các phần tử dữ liệu cụ thể. Bạn chỉ muốn trả lời ping (echo) đến một địa chỉ IP cụ thể. Và đối với những bản ghi đó, bạn chỉ muốn một byte trong phần dữ liệu. Sử dụng một loạt lệnh trong tập lệnh shell, bạn có thể tạo một bộ tách lấy PCAP, đọc nó bằng tcpdump, trích xuất các trường, sau đó ghi các phần tử mong muốn vào một tập tin. Bạn cũng có thể làm điều này với Python và với một số công cụ, bạn có thể đi đến đó. Điểm mấu chốt: có rất nhiều điều bạn có thể thực hiện bằng cách sử dụng hệ điều hành và các tập lệnh.

### **SSH**

SSH (Secure Shell) là một phương tiện được bảo mật bằng mật mã để giao tiếp và quản lý một mạng qua một kết nối không an toàn. Ban đầu

nó được thiết kế để thay thế cho các giao thức văn bản dạng rõ ràng (plaintext) của Telnet và các công cụ khác. Khi truy cập từ xa vào một hệ thống, điều quan trọng là không được sử dụng kênh giao tiếp dạng văn bản rõ ràng vì điều đó sẽ làm lộ những thông tin như mật khẩu và các mục nhạy cảm khác để bị đánh chặn.

---



**MÁCH NƯỚC CHO KỲ THI** SSH là một phương tiện được bảo mật bằng mật mã để giao tiếp và quản lý một mạng. SSH sử dụng cổng 22 và là sự thay thế được bảo mật cho Telnet.

### **PowerShell**

PowerShell là một khuôn khổ quản lý cấu hình và tự động hóa tác vụ dựa-trên-Microsoft Windows, bao gồm một shell dòng-lệnh và ngôn ngữ lập kịch bản. PowerShell được xây dựng dựa trên .NET Common Language Runtime (CLR) và chấp nhận và trả về các đối tượng .NET. Các lệnh được sử dụng trong PowerShell được gọi là cmdlets, và chúng có thể được kết hợp để xử lý các tác vụ phức tạp. PowerShell có thể được chạy từ lời nhắc PowerShell Console hoặc thông qua Windows PowerShell Integrated Scripting Environment (ISE), là một ứng dụng chủ cho Windows PowerShell. Ví dụ sau tìm kiếm tất cả các tập tin thực thi trong thư mục Program Files được sửa đổi lần cuối sau ngày 1 tháng 10 năm 2005 và không nhỏ hơn 1MB cũng không lớn hơn 10MB:

```
Get-ChildItem -Path $env:ProgramFiles -Recurse -Include *.exe | Where-Object -FilterScript {($_.LastWriteTime -gt '2005-10-01') -and ($_.Length -ge 1mb) -and ($_.Length -le 10mb)} | out-host -paging
```

Bởi vì mô hình đối tượng Microsoft Windows được bao gồm, cũng như một lượng lớn các cmdlets được thiết kế để thực hiện các hoạt động truy cập dữ liệu cụ thể, PowerShell là một công cụ cực kỳ mạnh mẽ để quản lý các

hệ thống Windows trong một doanh nghiệp. Với bản phát hành mới nhất của nó, PowerShell đã được sửa đổi để chạy trên rất nhiều nền tảng, bao gồm Windows, macOS, và Linux.

---



**MÁCH NƯỚC CHO KỲ THI** PowerShell là một giao diện kịch bản dòng-lệnh rất mạnh mẽ. Các tập tin PowerShell sử dụng .ps1 làm phần mở rộng tập tin.

### **Python**

Python là một ngôn ngữ máy tính thường được sử dụng cho các tác vụ phân tích dữ liệu và lập kịch bản mà các quản trị viên hệ thống và nhân viên bảo mật phải đối mặt. Python là một ngôn ngữ máy tính chính thức và đầy đủ. Nó hỗ trợ các đối tượng, lập trình chức năng và thu thập rác, và quan trọng nhất là nó có một loạt các thư viện rất lớn có thể được sử dụng để cung cấp chức năng cho một chương trình. Nhược điểm là nó được diễn giải, vì vậy tốc độ không phải là một thuộc tính mạnh của nó. Tuy nhiên, do tính hữu ích cao và cùng với sự hỗ trợ của thư viện, Python là ngôn ngữ phải học đối với hầu hết các chuyên gia bảo mật.

---



**MÁCH NƯỚC CHO KỲ THI** Python là một ngôn ngữ lập trình máy tính thông dụng sử dụng phần mở rộng tập tin là .py.

### **OpenSSL**

OpenSSL là một thư viện mã thông dụng cung cấp một loạt các chức năng mã trên các hệ thống Windows và Linux. Được thiết kế để trở thành một bộ công cụ có đầy-đủ-tính-năng dành cho các giao thức Bảo mật Lớp Truyền tải (TLS) và Lớp Cổng Bảo mật (SSL), nó còn cung cấp nhiều hơn nữa cho những thách thức hàng ngày trong thế giới thực.

OpenSSL có thể thực hiện các tác vụ sau trong các tập lệnh kịch bản hoặc chương trình, cung cấp quyền truy cập vào các chức năng mật mã mà không cần phải phát triển mã:

- Làm việc với các khóa RSA và ECDSA,
- Tạo ra các yêu cầu ký chứng nhận (CSR),
- Xác minh các CSR,
- Tạo ra các chứng nhận,
- Tạo ra các chứng nhận được-tự-ký,
- Chuyển đổi giữa các định dạng mã hóa (encoding) (PEM, DER) và định dạng vùng chứa (PKCS12, PKCS7).
- Kiểm tra trạng thái thu hồi chứng nhận,
- V.v...

Người ta có thể xem OpenSSL như một con dao găm của quân đội Thụy Sĩ dành cho tất cả những thứ liên quan đến các chức năng mật mã.

## **Bắt và Phát lại Gói tin**

Máy tính giao tiếp và trao đổi dữ liệu thông qua các kết nối mạng bằng các gói tin. Các công cụ phần mềm cho phép thu thập, chỉnh sửa và phát lại các luồng gói tin có thể rất hữu ích cho một chuyên gia bảo mật. Cho dù bạn đang kiểm tra một hệ thống hay chẩn đoán một sự cố thì việc có khả năng quan sát một cách chính xác những gì đang diễn ra giữa các máy và có thể điều chỉnh các luồng là một tiện ích tuyệt vời. Các công cụ trong phần này cung cấp khả năng này. Chúng có thể hoạt động trên lưu lượng mạng đang hoạt động hoặc lưu lượng được ghi lại dưới dạng các tập tin bắt gói (packet capture - PCAP).

## **Tcpreplay**

*Tcpreplay* là tên gọi của cả một công cụ và một bộ các công cụ. Là một bộ phần mềm, *tcpreplay* là một nhóm các tiện ích mã nguồn mở miễn phí để điều chỉnh và phát lại lưu lượng mạng đã thu thập được trước đó. Là

**CompTIA Security+ - All in One - Exam Guide**

939 | Page

một công cụ, nó đặc biệt phát lại tập tin PCAP trên mạng. Ban đầu được thiết kế như một công cụ ứng phó sự cố, tcpreplay khá tiện dụng trong rất nhiều trường hợp khi các gói tin mạng được sử dụng. Nó có thể được sử dụng để kiểm tra tất cả mọi kiểu hệ thống bảo mật thông qua việc sử dụng các tập tin PCAP đã được tạo ra để phát động một số biện pháp kiểm soát nhất định. Nó cũng được sử dụng để kiểm tra các dịch vụ trực tuyến chẳng hạn như các máy chủ web. Nếu bạn có nhu cầu gửi gói tin mạng đến máy khác, tcpreplay suite có câu trả lời cho bạn.

### **Tcpdump**

Tiện ích *tcpdump* được thiết kế để phân tích các gói mạng bắt kể là từ kết nối mạng hoặc tập tin đã được ghi lại. Bạn cũng có thể sử dụng tcpdump để tạo ra tập tin chụp gói, được gọi là tập tin PCAP và thực hiện việc lọc giữa đầu vào và đầu ra, khiến cho nó trở thành một công cụ có giá trị để giảm tải dữ liệu trên các công cụ khác. Ví dụ, nếu bạn có một tập tin chụp gói hoàn chỉnh có đến hàng trăm triệu bản ghi nhưng bạn chỉ quan tâm đến các kết nối của một máy chủ, bạn có thể tạo ra một bản sao của tập tin PCAP chỉ chứa các gói được liên kết với máy chủ đang được quan tâm. Tập tin này sẽ nhỏ hơn và dễ phân tích hơn bằng các công cụ khác.

### **Wireshark**

Wireshark là tiêu chuẩn vàng để phân tích đồ họa của các giao thức mạng. Với các bộ phân tách cho phép phân tích hầu như bất kỳ giao thức mạng nào, công cụ này có thể cho phép bạn kiểm tra các gói tin riêng lẻ, giám sát các cuộc hội thoại, chạm khắc các tập tin, v.v... Khi nói đến việc kiểm tra các gói, Wireshark là công cụ. Khi nói đến việc sử dụng chức năng này trong môi trường tập lệnh, TShark cung cấp quá trình xử lý tương tự ở dạng có thể tập lệnh, tạo ra nhiều loại đầu ra, tùy thuộc vào các tùy

chọn được đặt. Wireshark có khả năng nắm bắt lưu lượng truy cập trực tiếp hoặc nó có thể sử dụng các gói đã được ghi lại từ các nguồn khác.



**MÁCH NƯỚC CHO KỲ THI** Khi bạn đang kiểm tra các gói tin, sự khác biệt là những gì bạn cần phải thực hiện. Wireshark cho phép khám phá dễ dàng. Tcpdump bắt các gói tin thành tập tin PCAP và tcpreplay có một bộ các công cụ chỉnh sửa.

### **Điều tra pháp y**

Điều tra pháp y kỹ thuật số là việc sử dụng các phương pháp cụ thể để xác định ai đã thực hiện điều gì trên một hệ thống tại một thời điểm cụ thể hoặc một số biến thể của câu hỏi này. Các máy tính có một loạt các hiện vật có thể được phân tích để đưa ra những quyết định này. Có những công cụ để thu thập các hiện vật này, và những công cụ được sử dụng để phân tích dữ liệu đã thu thập được. Trong phần này, chúng ta sẽ xem xét một số công cụ chính được sử dụng trong những nỗ lực này. Các quy trình và thủ tục điều tra pháp y kỹ thuật số được đề cập chi tiết trong Chương 30, "Điều tra pháp y Kỹ thuật số". Đây chỉ là một quá trình xem xét một số công cụ được sử dụng.

### **dd**

Kết xuất dữ liệu (data dump - dd) là một tiện ích dòng-lệnh Linux được sử dụng để chuyển đổi và sao chép các tập tin. Trên các hệ thống Linux, hầu như mọi thứ đều được lưu trữ dưới dạng tập tin và dd có thể đọc từ và/hoặc ghi vào các tập tin này, miễn là chức năng đó được triển khai trong các trình điều khiển tương ứng. Do đó, dd có thể được sử dụng cho các tác vụ như sao lưu khu vực khởi động của ổ cứng, lấy một lượng dữ liệu ngẫu nhiên cố định hoặc sao chép (sao lưu) toàn bộ đĩa. Chương trình dd cũng có thể thực hiện các chuyển đổi trên dữ liệu khi nó được

sao chép, bao gồm hoán đổi thứ tự byte và chuyển đổi sang và từ các mã hóa văn bản ASCII và EBCDIC. dd có khả năng sao chép mọi thứ, sao lưu/khôi phục phân vùng và tạo ra/khôi phục hình ảnh của toàn bộ đĩa. Một số ví dụ phổ biến được trình bày dưới đây.

Dưới đây là cách sao lưu toàn bộ đĩa cứng:

```
# dd if = / dev / sda of = / dev / sdb
```

Ở đây, **if** đại diện cho tập tin đầu vào và **of** đại diện cho tập tin đầu ra. Do đó, bản sao chính xác của /dev/sda sẽ có trong /dev/sdb. Nếu có bất kỳ lỗi nào, lệnh trước đó sẽ bị lỗi. Nếu bạn cung cấp tham số **conv = noerror**, nó vẫn sẽ tiếp tục sao chép nếu xảy ra lỗi khi đọc. Hãy lưu ý rằng tập tin đầu vào và tập tin đầu ra cần được kiểm tra một cách rất cẩn thận vì sai sót có thể ghi đè lên dữ liệu, khiến bạn bị mất hết dữ liệu.

Dưới đây là cách tạo ra hình ảnh của một đĩa cứng:

```
# dd if = /dev/hda of = ~/hdadisk.img
```

Khi thực hiện thu thập dữ liệu điều tra pháp y, thay vì sao lưu đĩa cứng, bạn nên tạo ra một tập tin hình ảnh của đĩa cứng và lưu nó trên một thiết bị lưu trữ khác. Có rất nhiều ưu điểm khi sao lưu dữ liệu của bạn vào một ảnh đĩa, một trong số đó là dễ sử dụng. Tập tin hình ảnh chứa tất cả thông tin về nguồn đã được liên kết, bao gồm cả dung lượng chưa sử dụng và đã sử dụng trước đó.

### **memdump**

Linux có một chương trình tiện ích được gọi là trình kết xuất bộ nhớ, hoặc *memdump*. Chương trình này kết xuất bộ nhớ hệ thống vào luồng đầu ra tiêu chuẩn, bỏ qua bất kỳ lỗi hỏng nào trong bản đồ bộ nhớ. Theo mặc định, chương trình kết xuất nội dung của bộ nhớ vật lý (/dev/mem).

Kết quả đầu ra từ memdump có định dạng kết xuất thô. Bởi vì việc chạy chương trình memdump sẽ sử dụng bộ nhớ nên điều quan trọng là phải gửi đầu ra đến một vị trí không phải là máy chủ đang được sao chép, bằng cách sử dụng một công cụ như netcat.

## WinHex

*WinHex* là một trình chỉnh sửa tập tin thập lục phân. Công cụ này rất hữu ích trong các tập tin điều tra pháp y và nó cung cấp một loạt các chức năng điều tra pháp y như khả năng đọc hầu hết bất kỳ tập tin nào, hiển thị nội dung của tập tin, chuyển đổi giữa các bộ ký tự và mã hóa, thực hiện các chức năng xác minh băm và so sánh các tập tin. Là một trình đọc tập tin/trình chỉnh sửa thập lục phân nguyên bản, nó có thể kiểm tra các tập tin ứng dụng cụ thể mà không cần phải gọi ứng dụng và làm thay đổi dữ liệu. WinHex là một chương trình thương mại nằm trong bộ điều tra pháp y X-Ways, là một bộ công cụ điều tra pháp y kỹ thuật số toàn diện.

## FTK Imager

*FTK Imager* là câu trả lời của công ty AccessData dành cho dd. FTK Imager là một chương trình thương mại, miễn phí sử dụng và được thiết kế để ghi lại một hình ảnh của một ổ cứng (hoặc thiết bị khác) theo cách thức điều tra pháp y. Các bản sao pháp y là các bản sao từng-bit, được hỗ trợ bởi hàm băm để chứng minh rằng bản sao và bản gốc là bản sao chính xác theo mọi cách. Như với tất cả các công cụ thu thập hợp lý về mặt pháp y, FTK Imager giữ lại siêu dữ liệu hệ thống tập tin (và đường dẫn tập tin) và tạo ra nhật ký các tập tin đã được sao chép. Quá trình này không làm thay đổi các thuộc tính truy cập tin. FTK Imager là một phần của bộ công cụ điều tra pháp y FTK thương mại lớn hơn.

## Autopsy

Autopsy là câu trả lời mã nguồn mở đối với các bộ công cụ điều tra pháp y kỹ thuật số. Bộ phần mềm này, được phát triển bởi Brian Carrier, đã tiến hóa trong vài thập kỷ qua để trở thành một dự án nguồn mở được cộng đồng hỗ trợ có thể thực hiện hầu như tất cả các chức năng điều tra pháp y kỹ thuật số. Nó hoạt động trên Windows và cung cấp một bộ công cụ toàn diện có thể cho phép sự cộng tác dựa-trên-mạng và quy trình làm việc tự động và trực quan. Nó có các công cụ hỗ trợ ổ cứng, thiết bị di động và điện thoại thông minh. Nó cũng hỗ trợ tạo ra và tra cứu mã băm MD5, khắc các tập tin đã bị xóa, trích xuất dữ liệu EXIF từ những hình ảnh JPEG, tìm kiếm từ khóa đã được đánh chỉ mục, phát hiện tiện ích mở rộng không khớp, trích xuất thông điệp email và trích xuất hiện vật từ trình duyệt web.

Nó có các công cụ quản lý trường hợp để hỗ trợ cho các chức năng phân tích và báo cáo về trường hợp, bao gồm cả việc quản lý các mốc thời gian.



## MÁCH NƯỚC CHO KỲ THI

Hãy có khả năng xác định các công cụ điều tra pháp y kỹ thuật số khác nhau đã được thảo luận và biết được mục đích của từng công cụ. Ví dụ, hãy biết rằng dd là một tiện ích dòng lệnh của Linux được sử dụng để chuyển đổi và sao chép tập tin, trong khi FTK Imager là một chương trình thương mại được thiết kế để chụp ảnh một ổ cứng (hoặc thiết bị khác) theo cách thức điều tra pháp y.

## Những Khuôn khổ Khai thác

Các *khuôn khổ khai thác* là các bộ công cụ được thiết kế để hỗ trợ tin tặc trong các tác vụ liên quan đến việc khai thác các lỗ hổng trong một hệ thống. Những khuôn khổ này rất quan trọng vì lộ trình khai thác thường

bao gồm rất nhiều bước, tất cả đều được thực hiện theo một thứ tự chính xác trên một hệ thống để đạt được hiệu quả có ý nghĩa. Khuôn khổ được sử dụng phổ biến nhất là Metasploit, một bộ “các công cụ” được thiết kế để hỗ trợ người kiểm tra xâm nhập thực hiện các bước cần thiết để khai thác một lỗ hổng trên hệ thống. Các khuôn khổ này cũng có thể được sử dụng bởi nhân viên bảo mật, đặc biệt để kiểm tra khả năng bị khai thác của hệ thống dựa trên những lỗ hổng hiện đang có và các biện pháp kiểm soát bảo mật đã được sử dụng.

### Bẻ khóa Mật khẩu

*Phần mềm bẻ khóa mật khẩu* được tin tặc sử dụng để tìm ra những mật khẩu yếu. Tại sao một quản trị viên hệ thống lại nên sử dụng một trình bẻ khóa mật khẩu? Cùng một lý do. Việc chạy danh sách mật khẩu của hệ thống của bạn thông qua một trình bẻ khóa mật khẩu đem đến hai điều: một cảnh báo sớm về mật khẩu có thể bị bẻ khóa, và yên tâm rằng mật khẩu của bạn an toàn khi bạn không thể bẻ khóa bất kỳ mật khẩu nào trong một khoảng thời gian hợp lý.

Các trình bẻ khóa mật khẩu hoạt động bằng cách sử dụng các danh sách từ điển và bạo lực (brute force). Với các danh sách từ điển, chúng tạo ra mật khẩu bằng cách kết hợp các từ với nhau, với số và ký hiệu đặc biệt, và kiểm tra những mật khẩu đó với hệ thống. Chúng cũng có thể thực hiện các cuộc tấn công kiểu bạo lực. Các trình bẻ khóa mật khẩu có thể hoạt động trực tuyến dựa trên hệ thống đang hoạt động, nhưng sau đó chúng có thể bị hết thời gian chờ sau một số lần nhập sai mật khẩu có giới hạn. Tuy nhiên, nếu chúng có thể đánh cắp tập tin mật khẩu, chúng có thể hoạt động ở tốc độ tối đa cho đến khi tìm thấy một điểm khớp. Trên một máy tính có bộ vi xử lý Core i9 hiện đại có GPU, mật khẩu gồm 10 ký tự sẽ rơi vào khoảng một tuần làm việc để bị bẻ khóa. Với việc sử

dụng nhiều GPU thông qua một nhà cung cấp đám mây, điều này có thể giảm xuống chỉ còn vài giờ.

## Vệ sinh Dữ liệu

Công cụ *vệ sinh dữ liệu* là những công cụ được sử dụng để phá hủy, xóa hoặc xác định theo cách khác để phá hủy các loại dữ liệu cũ thể trên các hệ thống. Trước khi một hệ thống có thể được dừng hoạt động và loại bỏ, bạn cần phải làm sạch các nhu cầu dữ liệu. Có một số phương pháp tiếp cận, đầu tiên là phương pháp tiếp cận toàn bộ đĩa. Bạn có thể sử dụng công cụ vệ sinh dữ liệu để xóa hoặc làm sạch toàn bộ bộ lưu trữ của hệ thống, khiến cho dữ liệu không còn có thể khôi phục được nữa. Một phương pháp để thực hiện điều này là sử dụng đĩa tự mã hóa và việc phá hủy khóa sẽ khiến đĩa trở nên không thể khôi phục được. Phương pháp tiếp cận thứ hai, có đích nhắm mục tiêu hơn là xác định dữ liệu nhạy cảm và xử lý nó một cách cụ thể. Các công cụ như Identity Finder vượt trội về khía cạnh làm sạch dữ liệu này. Như với tất cả các công cụ, nó không phải là công cụ mang lại giá trị đích thực mà là các quy trình và thủ tục để đảm bảo rằng công việc được thực hiện, và được thực hiện một cách chính xác khi được yêu cầu.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các công cụ được sử dụng trong bảo mật. Chương này đã bắt đầu với một phần về thăm dò và khám phá mạng. Trong phần này, các công cụ tracert/traceroute, nslookup/dig, ipconfig/ifconfig, nmap, ping/pathping, hping, netstat, netcat, máy quét IP, arp, route, curl, theHarvester, sn1per, scanless, dnsenum, Nessus, và Cuckoo đã được trình bày.

Phần tiếp theo đề cập đến các công cụ được sử dụng trong thao tác với tập tin. Trong phần này, các công cụ được đề cập bao gồm head, tail, cat, grep, chmod và logger. Phần tiếp theo là về môi trường shell và script. Ở đây, SSH, PowerShell, Python và OpenSSL đã được nói đến. Phần tiếp theo bao gồm chụp và phát lại gói tin, và các công cụ tcpreplay, tcpdump và Wireshark cũng đã được đề cập.

Các công cụ điều tra pháp y kỹ thuật số đã được đề cập trong phần chính tiếp theo. Tại đây, dd, memdump, WinHex, FTK Imager, và Autopsy đã được trình bày. Chương này kết thúc với việc kiểm tra các khuôn khổ khai thác, các trình bẻ khóa mật khẩu và các công cụ làm sạch dữ liệu.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Để bảo mật các giao tiếp trong khi truy cập từ xa đến một hệ thống, người ta có thể sử dụng những công cụ nào dưới đây?

  - A. OpenSSL,
  - B. SSH,
  - C. dd,
  - D. tcpdump.
2. Công cụ nào sau đây không phải là công cụ thu thập/phân tích gói tin?

  - A. Wireshark
  - B. tcpreplay
  - C. tcpdump
  - D. dd.
3. Để chụp ảnh bộ nhớ trong một hệ thống đang hoạt động, người ta có thể sử dụng cách nào sau đây?

  - A. grep
  - B. dumpmem
  - C. memdump
  - D. logger.
4. Những công cụ nào được sử dụng trong điều tra địa chỉ IP? (Chọn tất cả các đáp án đúng).

  - A. tracert
  - B. theHarvester
  - C. dnsenum
  - D. chmod.

5. Để tìm kiếm thông qua một hệ thống để tìm các tập tin có chứa một cụm từ, công cụ tốt nhất sẽ là gì?
  - A. curl
  - B. logger
  - C. chmod
  - D. grep.
6. Chmod thực hiện điều gì?
  - A. Thiết lập quyền trên một tập tin
  - B. Bắt đầu một mục sửa đổi thay đổi trong một tập tin nhật ký
  - C. Băm mã hóa một tập tin
  - D. Liệt kê các tập tin trong một thư mục đang làm việc.
7. Bạn cần phân tích dữ liệu gói đã được thu thập trước đó trên mạng, bao gồm cả việc chỉnh sửa một số dữ liệu. Công cụ tốt nhất để sử dụng là gì?
  - A. tcpreplay
  - B. tcpdump
  - C. netstat
  - D. Wireshark.
8. Công cụ nào trong số những công cụ dưới đây được sử dụng trong kiểm nghiệm cảm nhận? (Chọn tất cả các đáp án đúng).
  - A. nmap
  - B. Nessus
  - C. scanless
  - D. theHarvester.
9. Để tự động hóa việc quản trị hệ thống trên một mạng Windows của doanh nghiệp, bao gồm cả việc sử dụng các đối tượng Windows, lựa chọn tốt nhất sẽ là lựa chọn nào sau đây?
  - A. Bash scripting (tập lệnh theo lô)
  - B. Python

- C. Wireshark**
  - D. PowerShell.**
- 10.** Bạn nghĩ rằng một tập tin là phần mềm độc hại. Công cụ đầu tiên bạn nên sử dụng là gì?
- A. Cuckoo**
  - B. WinHex**
  - C. OpenSSL**
  - D. Autopsy.**

## Đáp án

1. **B.** SSH mã hóa kênh liên lạc trên tuyến đường mà các gói tin của nó đi qua.
2. **D.** Tiện ích dd bắt các tập tin từ hệ thống tập tin chứ không phải các gói tin trên mạng.
3. **C.** Memdump là một chương trình dùng để sao chép những gì hiện có trong bộ nhớ.
4. **A** và **C.** Tracert cung cấp địa chỉ IP của một kênh liên lạc và dnseenum lấy thông tin từ máy chủ DNS.
5. **D.** Grep là công cụ so-khớp-mẫu có thể được sử dụng để so khớp các hình mẫu và tìm kiếm các kết quả phù hợp.
6. **A.** Chmod được sử dụng để thiết lập/quản lý quyền đối với các tập tin trong môi trường Linux.
7. **A.** Tcpreplay là công cụ tốt nhất để sử dụng trong trường hợp này vì câu hỏi yêu cầu chỉnh sửa gói tin.
8. **A, B, C** và **D.** Tất cả các công cụ này đều được sử dụng trong kiểm nghiệm xâm nhập. Nmap tìm kiếm các hệ thống, Nessus quét các lỗ hổng, scanless ẩn địa chỉ IP của máy quét và theHarvester thu thập thông tin về các mục tiêu tiềm năng.
9. **D.** PowerShell là công cụ tốt nhất để sử dụng trong trường hợp này. Chìa khóa là bao gồm các đối tượng Windows.
10. **A.** Cuckoo là một chương trình hộp cát được thiết kế để phân tích phần mềm độc hại, tách biệt phần mềm khỏi kết nối trực tiếp với hệ điều hành.

## Chương 27 Các Chính sách, Quy trình và Thủ tục Ứng phó Sự cố

### Các Chính sách, Quy trình và Thủ tục Ứng phó Sự cố

Trong chương này bạn sẽ

- Kiểm tra các khái niệm về quản lý cấu hình,
- Nghiên cứu về chủ quyền và các phương pháp bảo vệ dữ liệu,
- Kiểm tra một loạt các công nghệ được sử dụng trong các kiến trúc để bảo vệ dữ liệu,
- Kiểm tra các phương pháp được sử dụng để bảo vệ dữ liệu, bao gồm khả năng phục hồi địa điểm và các kỹ thuật đánh lừa dữ liệu.

Những hoạt động thông thường trong một doanh nghiệp CNTT bao gồm việc chuẩn bị cho tình huống khi xảy ra sự cố. Một khía cạnh của điều này là khi mọi thứ hoạt động không chính xác, không rõ lý do và quy trình ứng phó sự cố (incident response - IR) được sử dụng để xác định cái gì, nguyên nhân tại sao và vị trí của vấn đề. Một vấn đề lớn hơn là một thảm họa, trong đó việc khôi phục sau thảm họa và tính liên tục của các hoạt động là những vấn đề cấp bách. Mỗi một tình huống này đòi hỏi doanh nghiệp phải có sự chuẩn bị và sẵn sàng để đối phó với tất cả sự phức tạp của các kiểu hoạt động này. Chương này xem xét các khái niệm và thủ tục đằng sau những hoạt động chuyên biệt này.

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 4.2 của kỳ thi CompTIA Security+: Tóm tắt tầm quan trọng của các chính sách, quy trình và thủ tục ứng phó sự cố.

## Các Kế hoạch Ứng phó Sự cố

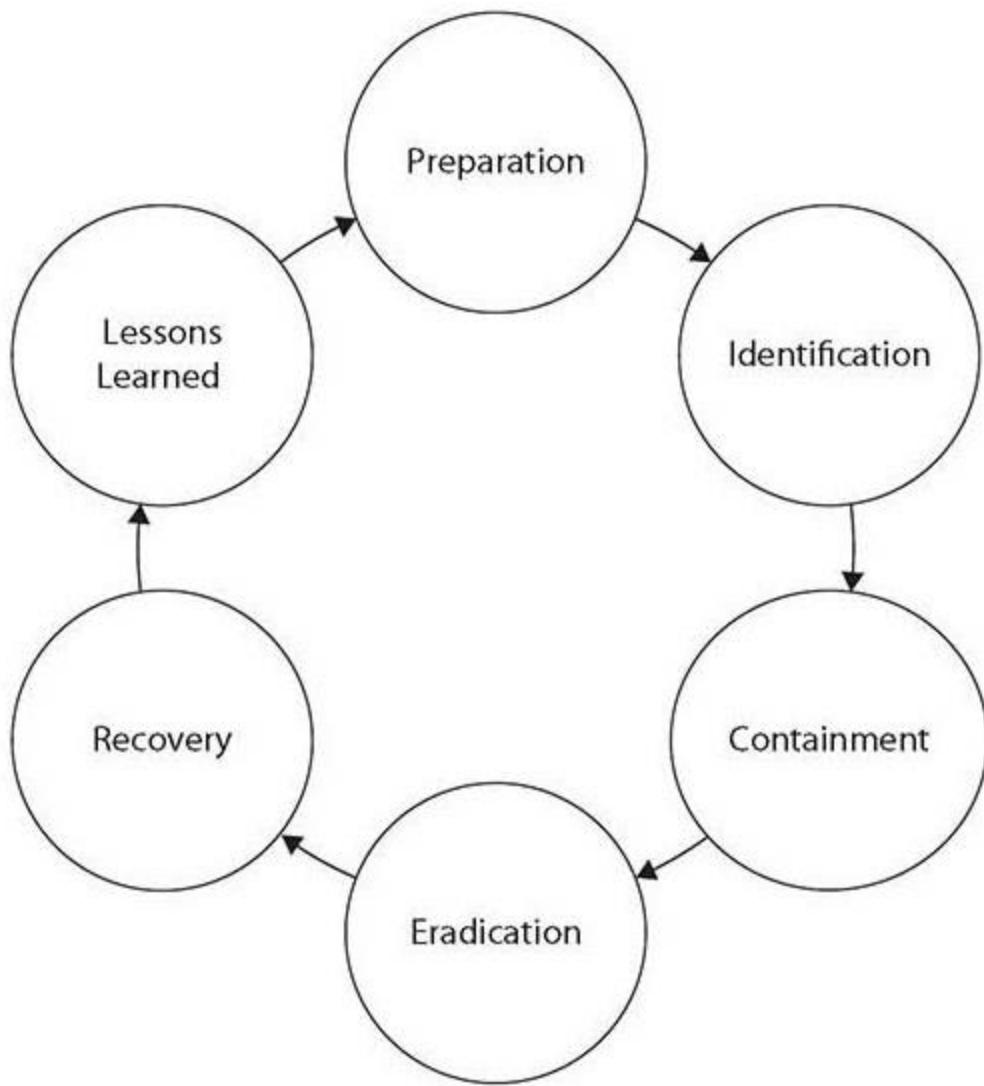
Một *kế hoạch ứng phó sự cố* mô tả các bước mà một tổ chức thực hiện nhằm ứng phó với bất kỳ tình huống nào được xác định là bất thường trong vận hành của hệ thống máy tính hoặc mạng. Có rất nhiều nguyên nhân của sự cố - từ môi trường (các cơn bão) đến lỗi người dùng, đến các hoạt động trái phép bởi những người dùng trái phép, v.v... Mặc dù có rất nhiều nguyên nhân nhưng những kết quả có thể được phân loại thành các lớp. Một sự cố có tác-động-thấp có thể không dẫn đến bất kỳ rủi ro rủi ro đáng kể nào, do đó không cần có hành động nào khác hơn việc sửa chữa hệ thống bị hư hỏng. Một sự cố có mức rủi-ro-trung-bình sẽ đòi hỏi những nỗ lực khảo sát và giám sát cẩn thận hơn, và một sự cố có rủi ro ở mức-độ-cao sẽ đòi hỏi những nỗ lực ứng phó và giám sát chặt chẽ nhất. Để quản lý các sự cố khi chúng xảy ra, nhóm CNTT cần tạo ra một kế hoạch ứng phó sự cố bao gồm một bảng hướng dẫn để hỗ trợ cho việc xác định mức độ của biện pháp ứng phó.

Có hai yếu tố chính đóng vai trò quyết định mức độ của biện pháp ứng phó. Mức độ quan trọng của thông tin là yếu tố quyết định chính, và điều này xuất phát từ việc phân loại dữ liệu và số lượng dữ liệu có liên quan. Ví dụ, việc mất một mật khẩu quản trị viên ít nghiêm trọng hơn việc mất tất cả mật khẩu và do đó yêu cầu mức độ ứng phó thấp hơn. Yếu tố thứ hai chính là cách sự cố có thể ảnh hưởng đến hoạt động của tổ chức như thế nào. Một loạt các vi phạm, dù nhỏ hay không, đều cho thấy một mô hình có thể có các vấn đề về quan hệ công chúng và các quy định.

Kế hoạch ứng phó sự cố sẽ bao gồm rất nhiều hạng mục, sẽ được thảo luận trong một số phần tiếp theo. Mặc dù một kế hoạch ứng phó sự cố có thể bao gồm nhiều hạng mục hơn trong một doanh nghiệp nhất định nhưng các mục tiêu Security+ sẽ xem xét các bước, bài tập, khuôn khổ, kế hoạch và chính sách của quy trình ứng phó sự cố.

## Quy trình Ứng phó Sự cố

*Quy trình ứng phó sự cố* là một tập hợp các hành động mà nhân viên bảo mật thực hiện nhằm ứng phó với một loạt các sự kiện kích hoạt. Những hành động này rất rộng và rất khác nhau, vì chúng phải xử lý một loạt các nguyên nhân và hậu quả khác nhau. Các hoạt động ứng phó sự cố đôi khi có liên quan mật thiết đến các hoạt động CNTT khác liên quan đến vận hành CNTT. Các hoạt động ứng phó sự cố không được thực hiện trong môi trường chân không mà thay vào đó, được kết nối một cách mật thiết với rất nhiều quy trình vận hành, và kết nối này chính là chìa khóa cho tính hiệu quả tổng thể của hệ thống. Sáu giai đoạn của quá trình ứng phó sự cố và trình tự của chúng được minh họa trong Hình 27-1.



**Hình 27-1** Quy trình ứng phó sự cố



### MÁCH NƯỚC CHO KỲ THI

Hãy tìm hiểu 6 giai đoạn của quá trình ứng phó sự cố và trình tự mà theo đó chúng được thực hiện: chuẩn bị, xác định, ngăn chặn, diệt trừ, khôi phục và bài học kinh nghiệm.

## **Chuẩn bị**

*Chuẩn bị* là giai đoạn trong quy trình ứng phó sự cố xảy ra trước một sự cố cụ thể. Chuẩn bị bao gồm tất cả các nhiệm vụ cần thiết để được tổ chức và sẵn sàng ứng phó khi xảy ra sự cố. Thông qua việc sử dụng một khuôn khổ có cấu trúc được kết hợp với các quy trình được chuẩn bị đúng cách, ứng phó sự cố sẽ trở thành một nhiệm vụ có thể quản lý được. Nếu không có sự chuẩn bị thích hợp, nhiệm vụ này có thể nhanh chóng trở nên bất khả thi hoặc rất tốn kém. Việc xử lý thành công một sự cố là kết quả trực tiếp của sự chuẩn bị thích hợp. Các hạng mục được thực hiện trong quá trình chuẩn bị bao gồm việc đảm bảo rằng các sự kiện dữ liệu chính xác đang được ghi nhận lại, báo cáo các sự cố tiềm ẩn đang xảy ra và mọi người đã được đào tạo về quy trình IR và trách nhiệm cá nhân của họ.

## **Xác định**

*Xác định* là quá trình khi một thành viên của nhóm nghi ngờ rằng một vấn đề còn lớn hơn một sự cố độc lập và thông báo cho nhóm ứng phó sự cố để điều tra thêm. Một sự cố được xác định khi một tình huống sai lệch khỏi những hoạt động như bình thường. Liệu đó có phải là một sự cố quan trọng hay không là điểm quyết định đầu tiên như một phần của quy trình ứng phó sự cố. Một lần đăng nhập thất bại đơn lẻ là một sự cố về mặt kỹ thuật, nhưng nếu nó tiếp tục bởi một lần đăng nhập thành công thì việc này sẽ không có bất kỳ hậu quả nào. Trong thực tế, điều này thậm chí có thể được coi là bình thường. Tuy nhiên, 10.000 lần cố gắng đăng nhập thất bại vào một hệ thống, hoặc đăng nhập thất bại với một lượng lớn các tài khoản là một điều khác biệt hoàn toàn và có thể xứng đáng được điều tra thêm. Hoạt động xác định liên quan đến việc đi đến một quyết định rằng thông tin có liên quan đến sự cố là xứng đáng được điều tra thêm bởi nhóm IR.

Xác định có thể được thực hiện bởi trên rất nhiều nhóm IT chẳng hạn như bộ phận hỗ trợ dịch vụ, quản trị viên, nhân viên cơ sở dữ liệu – về cơ bản là bất kỳ ai đang tìm kiếm điều gì đó bất thường có thể là một vấn đề thực sự. Một số quá trình đào tạo là cần thiết để ngăn chặn những cảnh báo giả, một lần truy cập tập tin bị thất bại đơn lẻ, ví dụ, hoặc một máy chủ bị khởi động lại đột ngột chỉ là những điều đã xảy ra và có khả năng không phải là một lý do để cảnh báo IR. Nhưng khi các sự cố đơn lẻ trở thành rất nhiều sự cố, một cuộc điều tra có thể cần được đảm bảo và các tình huống nên được xác định như là một vấn đề IR tiềm ẩn.

Một bước then chốt đầu tiên là xử lý thông tin và xác định xem liệu có cần phải việ dẫn quy trình ứng phó sự cố hay không. Thông tin về sự cố có thể đến từ một loạt các nguồn, bao gồm các nhật ký, nhân viên, các cuộc gọi hỗ trợ dịch vụ, giám sát hệ thống, các thiết bị bảo mật, v.v... Thách thức nằm ở chỗ xác định đang xảy ra điều gì đó khác với các lỗi theo thông lệ. Khi tíc lũy các bằng chứng – hoặc, trong một số trường hợp, những hạng mục cụ thể như các nhật ký của thiết bị chỉ ra một sự cố tiềm ẩn – bước tiếp theo là báo cáo leo thang tình huống cho nhóm IR.

Nhóm IR xem xét thông tin, thu thập thêm thông tin bổ sung nếu cần thiết, để xác định nguyên nhân của sự cố. Nếu như nó đáp ứng các ngưỡng đã được xác định của tổ chức, một sự cố sẽ được ghi lại và điều tra một cách đầy đủ. Bất kể nguyên nhân cốt lỗi là gì, nếu nó thực sự khác với một lỗi ngẫu nhiên, bước tiếp theo là sẽ là ngăn chặn.

### **Ngăn chặn**

Một khi nhóm IR đã xác định được rằng một sự cố trong thực tế đã xảy ra và đòi hỏi một phản ứng, bước đầu tiên của họ (nhóm IR) là đóng gói sự cố và ngăn chặn nó mở rộng. Ví dụ, nếu một sự cố liên quan đến một vi-rút hoặc sâu máy tính đang tấn công vào các máy chủ cơ sở dữ liệu thì

việc bảo vệ các máy chủ chưa bị lây nhiễm là mục tiêu ưu tiên hàng đầu. *Ngăn chặn* là tập hợp các hành động được thực hiện để hạn chế sự cố chỉ trong một lượng các máy tính tối thiểu. Việc này bảo quản hệ thống sản xuất càng nhiều càng tốt và cuối cùng, khiến cho việc xử lý sự cố trở nên dễ dàng hơn. Việc này có thể khá phức tạp bởi vì, trong rất nhiều trường hợp, việc ngăn chặn vẫn đề đòi hỏi việc hiểu hoàn toàn về nó cũng như nguyên nhân gốc rễ của nó và các lỗ hổng có liên quan.

### **Loại bỏ**

Khi nhóm IR đã ngăn chặn được một vấn đề về một kế hoạch được thiết lập, bước tiếp theo là loại bỏ vấn đề. *Loại bỏ* liên quan đến việc loại bỏ vấn đề, và trong các môi trường hệ thống phức tạp ngày nay điều này có nghĩa là xây dựng lại một máy hoàn toàn sạch. Một phần then chốt của hoạt động loại bỏ là sự ngăn chặn việc tái lây nhiễm. Có lẽ, hệ thống đã từng tồn tại trước khi vấn đề xảy ra sẽ dễ bị tái nhiễm trở lại, do đó, việc này cần phải được bảo vệ một cách đặc biệt để chống lại nó. Một trong những điều xuất giá trị mạnh mẽ nhất đối với các máy ảo là khả năng được dựng lại một cách nhanh chóng, khiến cho bước loại bỏ trở nên tương đối dễ dàng.

### **Khôi phục**

Sau khi sự cố đã được loại bỏ, quá trình khôi phục sẽ bắt đầu. Tại thời điểm này, cuộc điều tra được hoàn tất và được ghi lại thành văn bản. *Khôi phục* là quá trình đưa tài sản trở lại về chức năng nghiệp vụ của nó và khôi phục các hoạt động kinh doanh như bình thường. Loại bỏ, bước trước đó, đã loại bỏ vấn đề, nhưng trong hầu hết các trường hợp hệ thống đã được loại bỏ sẽ bị cô lập. Quá trình khôi phục bao gồm các bước cần thiết để đưa hệ thống và các ứng dụng về trạng thái hoạt động. Sau khi khôi phục, nhóm [IR] lập thành văn bản bài học kinh nghiệm từ sự cố.

## Bài học Kinh nghiệm

Một phiên phân tích tỉ mỉ nên thu thập *bài học kinh nghiệm* và chỉ định các hạng mục hành động để khắc phục các điểm yếu và đề xuất những cách thức để cải tiến. Xin được diễn giải một câu trích dẫn nổi tiếng, những ai không học hỏi từ lịch sử sẽ lặp lại thất bại. Giai đoạn rút ra bài học kinh nghiệm phục vụ cho hai mục đích khác nhau. Trước tiên là để ghi lại những gì đã gặp trực tiếp và cho phép sự cố xảy ra trong khu vực đầu tiên. Thất bại trong việc khắc phục điều này nghĩa là một sự lặp lại chắc chắn. Thứ hai là để xem xét chính bản thân quá trình ứng phó sự cố. Nó [quá trình ứng phó] đã làm tốt đến mức nào, các vấn đề đã xảy ra ở đâu, và nó có thể được cải thiện như thế nào? Liên tục cải tiến quy trình ứng phó sự cố thực tế là một nhiệm vụ rất quan trọng.



**MÁCH NƯỚC CHO KỲ THI** Hai thành phần chính đã được đề cập khá chồng chéo: việc hoạch định ứng phó sự cố và quy trình ứng phó sự cố đều là những hạng mục bao gồm nhiều bước có thể dễ dàng xuất hiện trong các câu hỏi của kỳ thi. Hãy đảm bảo sự chú ý vào thành phần nào (dù là hoạch định hay quy trình) đang được thảo luận đến trong câu hỏi cũng như là khía cạnh nào của chủ đề đó. Nói cách khác, trước tiên hãy xác định xem liệu câu hỏi đang quan tâm đến quy trình hoạch định hay quy trình IR và sau đó chọn cụm từ chính xác.

## Thực hành

Người ta thực sự không biết được rằng một kế hoạch được soạn thảo tốt đến mức nào cho đến khi nó được kiểm nghiệm. Các bài *thực hành* có nhiều hình thức, và việc thực hiện một bài thực hành trên giấy tờ khi các bước hoạch định và chuẩn bị được kiểm nghiệm là một bước sau cùng quan trọng trong quy trình hoạch định. Việc có một quy trình và một

nhóm được kết hợp là không đủ trừ khi nhóm đã thực hành quy trình trên các hệ thống của doanh nghiệp.



**MÁCH NƯỚC CHO KỲ THI** Nếu bạn được cung cấp một kịch bản, các chi tiết của kịch bản sẽ chỉ đến phần tương ứng của quy trình hoạch định. Do đó, hãy chú ý đến các chi tiết để có được đáp án đúng nhất.

### Tabletop

Một *bài tập tabletop* là một bài kiểm tra được thiết kế để các bên tham gia diễn tập tất cả các bước của một quy trình, đảm bảo rằng mọi thành phần đã được bao gồm và rằng kế hoạch đang không bỏ sót một tập dữ liệu hoặc một cá nhân quan trọng nào. Đây thường là một quá trình đánh giá cấp-cao, được thiết kế để khám phá các thành phần đang bị bỏ sót hoặc được đề cập một cách sơ sài và những lỗ hổng trong truyền thông, cả giữa con người và những hệ thống. Bài tập tabletop này là một bước cuối cùng tối quan trọng bởi vì nó xác minh việc lập kế hoạch đã bao gồm các thành phần cần thiết hay chưa. Các bước trong bài tập này nên được thực hiện bởi các lãnh đạo chủ yếu của doanh nghiệp và các chức năng CNTT để đảm bảo rằng tất cả các bước đều đang chính xác. Mặc dù việc này có thể mất thời gian của các thành viên cấp cao nhưng với tính quan trọng nhất định của quy trình nghiệp vụ này, khi nó được thực hiện cho các hoạt động đã được xác định là mang tính sống còn đối với doanh nghiệp, nó hầu như trông không có vẻ gì là quá mức cần thiết. Khía cạnh bài tập này không phải điều gì đó chỉ diễn ra một-lần, nó nên được lặp lại sau những thay đổi lớn đối với các hệ thống chặng hạn có tác động đến tính liên tục của kế hoạch vận hành hoặc những thay đổi lớn như tỷ lệ luân chuyển nhân viên. Do vậy, các tập đoàn lớn thường xuyên kiểm tra những hệ thống này theo một lịch trình đã được xác định trước, luân

chuyển giữa các ca làm việc ban ngày và ban đêm, nhân viên sao lưu chính và dự phòng, và các hệ thống khác.

**LƯU Ý:** *Tabletop là một diễn tập trong đó các hoạt động diễn tập chỉ diễn ra trên giấy tờ bằng cách xem xét các bước của một quy trình.*

## Điễn tập

Điễn tập kiểm tra các bước thực tế diễn ra liên quan đến một quy trình, thủ tục hoặc sự kiện. Diễn tập về bản chất là một quan sát viên thứ hai, nơi một bên giải thích hoặc trình bày các bước để thực hiện một nhiệm vụ trong khi người thứ hai sẽ quan sát. Công việc của quan sát viên là kiểm tra hoạt động để tuân thủ các chính sách và chỉ thị hiện hành. Nhiệm vụ có được hoàn thành một cách chính xác về mặt quy trình không? Các biện pháp kiểm soát, quy trình và thủ tục thích hợp có được tuân thủ không? Diễn tập có thể được thực hiện trên các phần tử như mã máy tính, nơi người viết mã hiển thị nó cho những người khác trong nhóm và diễn tập qua chương trình, từng dòng lệnh một. Việc giải thích cách thức nó hoạt động và cho thấy nó đã được mã hóa như thế nào cho phép những người khác kiểm tra cả cú pháp và luồng quy trình và đưa ra những phản hồi có giá trị về mã trước khi nó được triển khai trong một dự án. Việc có được một giám sát viên quan sát quy trình đối với bất kỳ chức năng nào cho phép xác định một cách độc lập xem liệu các hành động của họ có phù hợp với các chính sách bảo mật của công ty hay không. Bởi vì người đang thực hiện công việc dựa vào quá trình đào tạo và thực hành lặp đi lặp lại, một diễn tập định kỳ cung cấp bằng chứng rằng các thủ tục thích hợp đang thực sự được tuân thủ. Các diễn tập thường được sử dụng bởi nhân viên kiểm toán để đảm bảo rằng các quy trình phù hợp đang được tuân thủ.

## Mô phỏng

*Mô phỏng* là một bản mô phỏng gần đúng hoạt động của một quy trình hoặc hệ thống được thiết kế để đại diện cho các hoạt động thực tế của hệ thống trong một khoảng thời gian. Mô phỏng có thể được sử dụng thay cho các hệ thống hoặc phần tử không tái tạo được một cách thực tế trong quá trình thực hiện bài tập, chẳng hạn như một phần tử phức tạp như nhà máy hóa chất hoặc một hoạt động tốn-nhiều-thời-gian như hoạt động dự phòng. Các mô phỏng được sử dụng trong các bài tập để cung cấp bối cảnh cho những người tham gia mà không phải chi tiêu cho những gì liên quan đến việc sử dụng một hệ thống thực.



## MÁCH NƯỚC CHO KỲ THI

Các kiểu yếu tố bài tập khác nhau, các bài tập tabletop, diễn tập và mô phỏng có thể được sử dụng để cùng nhau như một phần của một gói bài tập.

## Các Khuôn khổ Tấn công

Các khuôn khổ tấn công cung cấp một lộ trình về các loại hành động và chuỗi trình tự hành động được sử dụng khi tiến hành tấn công một hệ thống. Các khuôn khổ mang lại một cảm giác về cấu trúc và trật tự cho vấn đề đa chiều liên quan đến việc bảo vệ nhiều hệ thống chống lại nhiều kiểu kẻ tấn công khác nhau với nhiều mục tiêu khác nhau. Mục tiêu của việc sử dụng một khuôn khổ là để cải thiện khả năng phát hiện các kẻ thù sau-xâm-phạm (post-compromise) trong doanh nghiệp bằng cách cung cấp hướng dẫn về nơi có thể quan sát được hành động của kẻ thù và nơi có thể thực hiện các hành động cụ thể. Các tổ chức có thể sử dụng các khuôn khổ để xác định các lỗ hổng trong phòng thủ và ưu tiên chúng dựa trên rủi ro tương ứng với các hành động mà kẻ thù có thể thực hiện. Có ba khuôn khổ khác nhau được mô tả trong các phần sau: khuôn khổ

MITER ATT & CK, Mô hình Kim cương về Phân tích Xâm nhập (Diamond Model of Intrusion Analysis) và Chuỗi Tiêu diệt Mạng (Cyber Kill Chain).

### **MITRE ATT & CK**

Khuôn khổ MITRE ATT&CK là một ma trận toàn diện về các yếu tố tấn công, bao gồm các chiến thuật và kỹ thuật được sử dụng bởi những kẻ tấn công trên một hệ thống. Khuôn khổ này có thể được sử dụng bởi những người săn lùng mối đe dọa - những người đồng đội đỏ và những người bảo vệ để phân loại các cuộc tấn công tốt hơn và hiểu tốt hơn về các bước tuần tự mà kẻ thù sẽ thực hiện khi tấn công một hệ thống. Khuôn khổ này cho phép nhân viên lập kế hoạch và bảo vệ, thậm chí ngay cả trong một cuộc tấn công và hơn nữa, nó hoạt động như một công cụ hữu ích trong việc đánh giá rủi ro của một tổ chức.

Khuôn khổ MITRE ATT&CK có thiết kế tương đối đơn giản, với dòng trên cùng của ma trận bao gồm các hoạt động như truy cập ban đầu, thực thi, bền bỉ, leo thang đặc quyền, né tránh phòng thủ, truy cập thông tin xác thực, khám phá, di chuyển bên rìa, thu thập, điều khiển và kiểm soát, lọc, và tác động. Bên dưới mỗi hoạt động này là một loạt các kỹ thuật và kỹ-thuật-con. Được kết hợp lại với nhau, ma trận này vẽ nên một bức tranh toàn cảnh về các con đường thông qua doanh nghiệp CNTT của một tổ chức.

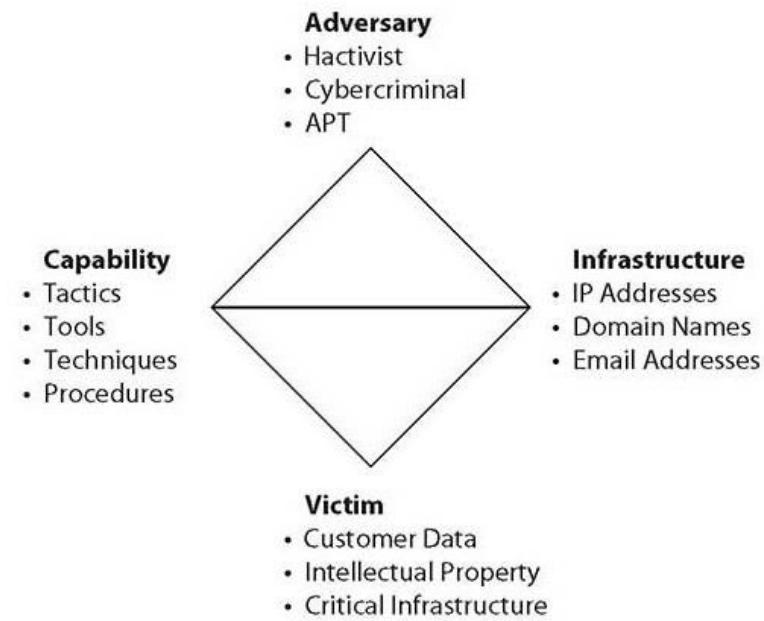


### **MÁCH NƯỚC CHO KỲ THI**

Khuôn khổ MITRE ATT&CK là một cơ sở kiến thức về một loạt các kỹ thuật tấn công và quan sát trong thế-giới-thực khác nhau. Nó thường được sử dụng bởi các tổ chức để lập mô hình về các mối đe dọa.

## Mô hình Kim cương về Phân tích Xâm nhập

*Mô hình Kim cương về Phân tích Xâm nhập* là một mô hình nhận thức được sử dụng bởi cộng đồng tình báo về mối đe dọa để mô tả một sự kiện cụ thể. Nó dựa trên quan điểm cho rằng một sự kiện bao gồm bốn đặc điểm, mỗi đặc điểm bao gồm một góc của hình thoi, như được minh họa trong Hình 27-2. Kết hợp với nhau, các yếu tố này mô tả một sự kiện. Bốn nút tạo nên một sự kiện là kẻ thù, cơ sở hạ tầng, năng lực và nạn nhân. Nút kẻ thù là một mô tả về kẻ tấn công và dữ liệu về chúng, bao gồm bất cứ điều gì bạn biết về chúng (email, tên, vị trí, cách thức, v.v...). Nút cơ sở hạ tầng là một mô tả về những gì đang được sử dụng trong cuộc tấn công, chẳng hạn như địa chỉ IP, tên miền, địa chỉ e-mail, v.v... Nút nạn nhân là đích nhắm mục tiêu và nút năng lực là mô tả về những gì đang được sử dụng (phần mềm độc hại, chứng chỉ/thông tin đăng nhập bị đánh cắp, công cụ, khai thác, v.v...). Ví dụ, một viên kim cương đã hoàn thành có thể có dạng sau:



**Hình 27-2** Mô hình kim cương về Phân tích Xâm nhập

## 5. Kẻ thù

Whois được sử dụng để lấy email của người đăng ký – kẻ tấn công khả dĩ.

## 6. Cơ sở hạ tầng

Tên miền C2 phân giải thành một địa chỉ IP.

## 7. Năng lực

Nhóm ứng phó tìm kiếm tên miền máy chủ C2.

## 8. Nạn nhân

Một nạn nhân phát hiện ra phần mềm độc hại và khởi động quy trình ứng phó sự cố.



## MÁCH NƯỚC CHO KỲ THI

Mô hình Kim cương hỗ trợ phân tích xâm nhập bằng cách đưa hoạt động độc hại vào 4 điểm của viên kim cương: kẻ thù, cơ sở hạ tầng, năng lực và nạn nhân.

## Cyber Kill Chain

Cyber Kill Chain là một mô hình được phát triển bởi Lockheed Martin như là một hình thức quân sự của khuôn khổ giao chiến. Mô hình này có một loạt các bước riêng biệt mà kẻ tấn công sử dụng trong một cuộc tấn công mạng - từ giai đoạn trinh sát ban đầu cho đến khi đánh cắp được dữ liệu. Việc sử dụng Cyber Kill Chain giúp chúng ta hiểu và chống lại các hình thức tấn công khác nhau - từ ransomware đến vi phạm bảo mật và thậm chí là các mối đe dọa dai dẳng được nâng cao (APT).

Chuỗi Cyber Kill có các bước hơi khác nhau tùy thuộc vào phiên bản bạn sử dụng, nhưng các cách triển khai phổ biến nhất bao gồm những bước sau:

1. **Do thám** Nghiên cứu và xác định mục tiêu.
2. **Vũ khí hóa** Khai thác lỗ hổng để xâm nhập.
3. **Phân phối** Phân phối tải trọng (nội dung độc hại).

4. **Khai thác** Bắt đầu tấn công tải trọng vào hệ thống và đạt được sự xâm nhập.
5. **Cài đặt** Triển khai backdoor, truy cập liên tục, các bot, v.v...
6. **Điều khiển và Kiểm soát** Giao tiếp với các máy chủ bên ngoài nhằm mục đích kiểm soát.
7. **Hành động dựa trên mục tiêu** Đạt được mục tiêu của cuộc tấn công (ví dụ: ăn cắp tài sản trí tuệ).

Bằng cách tìm hiểu tiến trình của một cuộc tấn công, những người phòng thủ có thể lựa chọn điểm phòng thủ của họ, cho phép họ phản ứng với một cuộc tấn công có kế hoạch và mục đích.



**MÁCH NƯỚC CHO KỲ THI** Được phát triển bởi Lockheed Martin, Cyber Kill Chain là một khuôn khổ được sử dụng để phòng thủ, chống lại chuỗi các sự kiện mà một kẻ tấn công thực hiện, từ khi bắt đầu cuộc tấn công đến khi kết thúc.

### Quản lý Bên liên quan

Các bên liên quan là các bên có lợi ích trong một quá trình hoặc kết quả của một quá trình. Các bên liên quan có thể là nội bộ hoặc bên ngoài đối với tổ chức. Đối với các tình huống ứng phó sự cố, tất cả các cấp quản lý và nhiều chức năng kinh doanh khác nhau có thể được tham gia nội bộ, bao gồm bộ phận pháp lý doanh nghiệp, truyền thông, đầu mối liên lạc với các cơ quan quản lý, các thành phần hỗ trợ khách hàng và các nhân viên vận hành. Về bên ngoài, có thể có các vấn đề liên quan đến nhà cung cấp và khách hàng, và có thể có các yêu cầu báo cáo cho các cơ quan quản lý và các nhóm bên ngoài khác. Với sự đa dạng của các bên liên quan, việc có được một cấu trúc để quản lý giao tiếp với các bên liên quan khác nhau là điều rất quan trọng để giữ cho họ được thông báo một

cách thích hợp và tách biệt các nhiệm vụ truyền thông khỏi các nhiệm vụ vận hành có liên quan đến ứng phó với sự cố. Có một quy trình *quản lý các bên liên quan*, bao gồm các vai trò và trách nhiệm nhân sự đã được xác định là điều thiết yếu đối với việc quản lý các bên liên quan và các mối quan hệ của họ trong thời gian xảy ra sự cố.

### Kế hoạch Truyền thông

Việc lập kế hoạch về các yêu cầu báo cáo mong muốn, bao gồm các bước leo thang, là một phần quan trọng của kế hoạch hoạt động dành cho một sự cố. Ai sẽ nói chuyện cho nhóm ứng phó sự cố và với ai, và họ sẽ nói gì? Luồng thông tin sẽ đi như thế nào? Ai có nhu cầu cần được tham gia? Khi nào thì vẫn đề được chuyển lên cấp quản lý cao hơn? Đây là tất cả những câu hỏi tốt nhất nên được xử lý trong sự bình tĩnh của cuộc họp lập kế hoạch trước-sự-cố, nơi các thủ tục được phác thảo, thay vì vội vàng khi sự cố đang xảy ra. *Kế hoạch giao tiếp* là một phần của nỗ lực ứng phó sự cố nhằm trả lời các câu hỏi trước đó và xác định trách nhiệm liên lạc là yếu tố chính cần được phát triển trong giai đoạn chuẩn bị.

Các yêu cầu về báo cáo có thể đề cập đến các yêu cầu của ngành, quy định và luật định ngoài giao tiếp nội bộ. Việc hiểu được các yêu cầu báo cáo dành cho các đơn vị bên ngoài là một phần trách nhiệm của người phụ trách truyền thông trong nhóm. Có được thông tin chính xác trong tay của những người thích hợp vào đúng thời điểm là một phần thiết yếu của báo cáo và là trách nhiệm chính của người phụ trách truyền thông trong nhóm

### Kế hoạch Khôi phục Sau thảm họa

Bất kể bạn lo lắng về sự kiện nào - dù là [sự kiện] tự nhiên hay do con người gây ra và được nhắm mục tiêu vào tổ chức của bạn hay ngẫu nhiên hơn - bạn đều có thể chuẩn bị để giảm bớt tác động đến tổ chức của mình và khoảng thời gian tổ chức của bạn phải ngừng hoạt động. Một kế

*hoạch khôi phục sau thảm họa (DRP)* là tối quan trọng đối với các nỗ lực khôi phục sau thảm họa hiệu quả. Một DRP xác định dữ liệu và các nguồn lực cần thiết và các bước cần thiết để khôi phục các quy trình tổ chức tối quan trọng.

Hãy xem xét tổ chức của bạn cần những gì để thực hiện sứ mệnh của mình. Thông tin này đem đến sự khởi đầu của DRP vì nó cho bạn biết những gì cần phải được khôi phục một cách nhanh chóng. Khi xem xét các nguồn tài nguyên, đừng quên bao gồm cả tài nguyên vật lý (chẳng hạn như phần cứng và phần mềm máy tính) và nhân sự (những người biết cách điều hành hệ thống xử lý dữ liệu tối quan trọng của bạn).

Để bắt đầu phác thảo nên DRP của bạn, trước tiên hãy xác định tất cả những chức năng tối quan trọng đối với tổ chức của bạn và sau đó trả lời các câu hỏi sau cho từng chức năng quan trọng này:

- Ai chịu trách nhiệm về hoạt động của chức năng này?
- Những cá nhân này cần gì để thực hiện chức năng đó?
- Khi nào thì nên hoàn thành chức năng này so với các chức năng khác?
- Chức năng này sẽ được thực hiện ở đâu?
- Chức năng này được thực hiện như thế nào (quy trình là gì)?
- Tại sao chức năng này lại quan trọng hoặc then chốt đối với tổ chức?

Bằng cách trả lời những câu hỏi này, bạn có thể tạo ra bản nháp ban đầu về DRP của tổ chức của mình. Tên gọi thường được sử dụng để mô tả một tài liệu được tạo ra bằng cách giải quyết những câu hỏi này là *đánh giá tác động kinh doanh (business impact analysis - BIA)*. Tất nhiên, cả kế hoạch khắc phục hậu quả thiên tai và đánh giá tác động kinh doanh đều cần được ban lãnh đạo phê duyệt, và điều quan trọng là họ phải tín nhiệm vào kế hoạch - nếu không, nỗ lực của chúng ta rất có thể sẽ thất bại.

Câu ngạn ngữ cổ “những người không lập kế hoạch là đang lập kế hoạch thất bại” chắc chắn có hiệu lực trong tình huống này.

Một DRP tốt phải bao gồm các quy trình và thủ tục cần thiết để tổ chức của bạn hoạt động bình thường và đảm bảo hoạt động liên tục. Những bước cụ thể sẽ được yêu cầu để khôi phục hoạt động? Các quy trình này phải được lập thành văn bản và nếu có thể và khả thi, được xem xét và kiểm tra trên cơ sở định kỳ. Việc có một kế hoạch với các thủ tục từng bước mà không ai biết cách làm theo sẽ không có tác dụng gì để đảm bảo tổ chức vẫn tiếp tục hoạt động. Thực hiện DRP và các quy trình của bạn trước khi thảm họa xảy ra giúp bạn có cơ hội phát hiện ra những sai sót hoặc những điểm yếu trong kế hoạch khi vẫn còn thời gian để điều chỉnh và sửa chữa chúng. Nó cũng sẽ tạo ra cơ hội cho những nhân vật chủ chốt trong kế hoạch thực hành những gì họ sẽ đạt được.



### LƯU Ý

Việc xác định các chức năng nghiệp vụ khác nhau của bạn thuộc loại nào thường sẽ đem lại nhiều kiến thức. Bạn có thể thấy rằng một số chức năng nhất định hiện đang được tiến hành không phải là thiết yếu cho hoạt động của bạn và có thể bị loại bỏ. Bằng cách này, việc chuẩn bị cho một sự kiện bảo mật có thể thực sự giúp bạn hợp lý hóa các quy trình hoạt động của mình.

### Kế hoạch Liên tục Kinh doanh

Như trong hầu hết các vấn đề về vận hành, lập kế hoạch là một yếu tố nền tảng để thành công. Điều này cũng đúng trong liên tục kinh doanh và *kế hoạch liên tục kinh doanh* (*business continuity plan - BCP*) đại diện cho việc lập kế hoạch và các quyết định chính sách tiên tiến để đảm bảo đạt được các mục tiêu liên tục kinh doanh trong một thời kỳ hỗn loạn rõ ràng. Bạn có thể tự hỏi sự khác biệt giữa một kế hoạch khôi phục sau

thảm họa và kế hoạch liên tục kinh doanh là gì. Rốt cuộc, mục đích của việc khắc phục hậu quả không phải là mục đích tiếp tục hoạt động của tổ chức hoặc doanh nghiệp trong thời gian gián đoạn sao? Nhiều lần, hai thuật ngữ này được sử dụng đồng nghĩa và đối với nhiều tổ chức có thể không có sự khác biệt lớn giữa chúng. Tuy nhiên, có sự khác biệt thực sự giữa BCP và DRP, một trong số đó là trọng tâm.

Trọng tâm của BCP là hoạt động liên tục của các thành phần thiết yếu của doanh nghiệp hoặc tổ chức. Liên tục kinh doanh không phải là về các hoạt động như bình thường mà chỉ là về các hoạt động thiết yếu và đã được cắt giảm. Trong BCP, bạn sẽ thấy sự nhấn mạnh đáng kể hơn vào số lượng giới hạn các hệ thống tối quan trọng mà tổ chức cần vận hành. BCP mô tả các chức năng quan trọng nhất, dựa trên quá trình phân tích tác động kinh doanh đã được tiến hành trước đó và sẽ mô tả thứ tự mà theo đó, các chức năng cần được quay trở lại hoạt động. BCP mô tả những gì cần thiết để doanh nghiệp tiếp tục hoạt động trong ngắn hạn, thậm chí ngay cả khi tất cả các yêu cầu không được đáp ứng và hồ sơ rủi ro được thay đổi.

Trọng tâm của DRP là khôi phục và xây dựng lại tổ chức sau khi thảm họa đã xảy ra. Mục tiêu của khôi phục là hoạt động hoàn chỉnh của tất cả các yếu tố của doanh nghiệp. DRP là một phần của bức tranh lớn hơn, trong khi BCP là một nhu cầu chiến thuật cần thiết cho đến khi các hoạt động có thể được khôi phục. Trọng tâm chính của DRP là bảo vệ cuộc sống con người, có nghĩa là các kế hoạch sơ tán và quy trình tắt hệ thống phải được xác định. Trên thực tế, sự an toàn của nhân viên phải là một chủ đề xuyên suốt DRP.



**MÁCH NƯỚC CHO KỲ THI** Mặc dù các thuật ngữ DRP và BCP có thể được sử dụng đồng nghĩa trong các doanh nghiệp nhỏ, nhưng trong các doanh nghiệp lớn, sẽ có sự khác biệt về trọng tâm giữa hai kế hoạch. Trọng tâm của BCP là tiếp tục hoạt động của một doanh nghiệp, mặc dù ở mức độ sụt giảm hoặc thông qua các phương tiện khác nhau trong một khoảng thời gian nào đó. DRP đặc biệt tập trung vào việc khôi phục sau thảm họa. Trong nhiều trường hợp, cả hai chức năng này xảy ra cùng một lúc, và do đó chúng thường được kết hợp trong các công ty nhỏ và trong nhiều cuộc thảo luận. DRP là một phần của quy trình BCP lớn hơn.

### **Liên tục Hoạch định Vận hành (COOP)**

Việc đảm bảo tính liên tục của các hoạt động là một yêu cầu cấp thiết của doanh nghiệp, vì nó đã được chứng minh rằng các doanh nghiệp không thể phục hồi một cách nhanh chóng thực sự có khả năng không bao giờ khôi phục sau tình trạng gián đoạn và sẽ phải ngừng kinh doanh. Mục tiêu tổng thể của *tính liên tục của việc hoạch định vận hành (COOP)* là xác định xem tập hợp con nào của các hoạt động bình thường cần được tiếp tục trong khoảng thời gian gián đoạn. Tính liên tục của hoạch định vận hành liên quan đến việc phát triển một kế hoạch toàn diện để ban hành trong tình huống mà các hoạt động bình thường đã bị gián đoạn. Điều này bao gồm việc xác định các tài sản quan trọng (bao gồm nhân sự chủ chốt), các hệ thống quan trọng và sự phụ thuộc lẫn nhau cũng như đảm bảo tính sẵn sàng của chúng trong thời gian gián đoạn.

Việc phát triển một kế hoạch hoạt động liên tục là một nỗ lực chung giữa doanh nghiệp và nhóm CNTT. Doanh nghiệp hiểu những chức năng nào là tối quan trọng đối với sự liên tục của hoạt động và những chức năng nào có thể được tạm dừng. Nhóm CNTT hiểu cách điều này chuyển thành thiết

bị, dữ liệu và các dịch vụ và có thể thiết lập các chức năng CNTT chính xác. Quản lý cấp điều hành sẽ phải đưa ra các quyết định quan trọng liên quan đến việc cân bằng rủi ro so với chi phí và tính trọng yếu khi xem xét các chiến lược địa điểm nóng, ấm hoặc lạnh.



**MÁCH NƯỚC CHO KỲ THI** COOP tập trung vào liên tục hoạt động kinh doanh, trong khi BCP tập trung vào việc đưa một doanh nghiệp trở lại hoạt động có lãi, thậm chí ngay cả ở mức độ hoặc công suất bị sụt giảm. Các cơ quan chính phủ, nơi các dịch vụ là thiết yếu và chi phí có thể được xử lý sau đó, đặt trọng tâm vào COOP, trong khi rất nhiều doanh nghiệp tập trung vào DRP và BCP.

### Nhóm Ứng phó Sự cố

*Nhóm ứng phó sự cố mạng (cyber incident response team - CIRT)* bao gồm các nhân sự được chỉ định để ứng phó với một sự cố. Kế hoạch ứng phó sự cố nên xác định các thành viên [chính thức] và các thành viên dự phòng, trước khi sự cố xảy ra. Một khi ứng phó sự cố bắt đầu, việc cỗ găng tìm kiếm nhân sự để thực hiện nhiệm vụ chỉ làm chậm chức năng [ứng phó sự cố] và trong nhiều trường hợp sẽ khiến nó trở nên không thể quản lý được. Cho dù là một nhóm chuyên trách hay một nhóm tình nguyện viên theo tình huống, khía cạnh lập kế hoạch ứng phó sự cố cần phải giải quyết chủ đề ai là thành viên của nhóm và nhiệm vụ của họ là gì.

Cấp quản lý cần bổ nhiệm các thành viên trong nhóm và đảm bảo rằng họ có đủ thời gian chuẩn bị cho việc phục vụ. Trưởng nhóm thường là một thành viên của cấp quản lý, người hiểu đầy đủ về cả môi trường CNTT của doanh nghiệp lẫn quy trình IR vì nhiệm vụ của họ là lãnh đạo nhóm về mặt có liên quan đến quy trình. Các chuyên gia về vấn đề chủ

đề (SME) trên các hệ thống khác nhau có liên quan sẽ cung cấp phần làm việc thực tế của nhóm, thường kết hợp với các nhân viên CNTT vận hành cho mỗi hệ thống. Nhóm chịu trách nhiệm cho mọi giai đoạn của quá trình ứng phó sự cố, đã được đề cập trước đó trong chương.

Một bước quan trọng trong quá trình hoạch định ứng phó sự cố là xác định vai trò và trách nhiệm của các thành viên trong nhóm ứng phó sự cố. Các vai trò và trách nhiệm này có thể thay đổi một chút dựa trên các thể loại sự cố đã được xác định, nhưng việc xác định chúng trước khi sự cố xảy ra sẽ cho phép nhóm thực hiện các nhiệm vụ cần thiết trong suốt những khía cạnh nhạy-cảm-về-thời-gian của sự cố. Quyền ngắt kết nối, thay đổi các máy chủ và khởi động/dừng dịch vụ là những ví dụ phổ biến về các hành động đã được xác định trước tốt nhất để tránh tiêu-tốn-thời-gian cho việc phê duyệt trong một sự cố thực tế.

Có một số vai trò cụ thể dành riêng cho tất cả các nhóm IR: trưởng nhóm, người truyền thông trong nhóm và một nhóm các chuyên gia về chủ đề phù hợp (SME). Trưởng nhóm quản lý quy trình IR tổng thể, vì vậy họ cần phải là thành viên của cấp quản lý để có thể điều hướng chuỗi mệnh lệnh của công ty. Người truyền thông của nhóm là người phát ngôn của nhóm cho tất cả các nhóm khác, bên trong và bên ngoài công ty. Các thành viên trong nhóm IR thường là các SME, và thời gian của họ là rất quý giá và cần phải được dành cho công việc. Người truyền thông trong nhóm bảo vệ những thành viên này khỏi phần trả lời phỏng vấn của báo chí tiêu-tốn-thời-gian càng nhiều càng tốt.

### **Chính sách Lưu giữ**

*Lưu giữ dữ liệu* là lưu trữ các bản ghi dữ liệu. Một trong những bước đầu tiên trong việc tìm hiểu về việc lưu giữ dữ liệu trong một tổ chức là xác định xem hồ sơ nào cần lưu trữ và trong khoảng thời gian bao lâu. Trong số rất nhiều lý do để giữ lại dữ liệu, một số lý do phổ biến nhất là vì mục

đích lập hóa đơn và kê toán, nghĩa vụ hợp đồng, lịch sử bảo hành và tuân thủ các quy định của chính phủ địa phương, tiểu bang và quốc gia, chẳng hạn như các quy tắc IRS. Việc duy trì kho lưu trữ dữ liệu lâu hơn mức cần thiết là một nguồn rủi ro, cũng như việc không lưu trữ thông tin đủ lâu. Một số thông tin tuân theo các quy định yêu cầu lưu giữ dữ liệu dài, chẳng hạn như PHI cho những người lao động đã từng tiếp xúc với các mối nguy hiểm cụ thể. Một số phần tử dữ liệu, chẳng hạn như phần tử mã xác minh thẻ (CVC/CV2) trong giao dịch thẻ tín dụng, không bao giờ được lưu trữ như một phần của hồ sơ giao dịch. Chúng được sử dụng để phê duyệt và tiêu hủy nhằm tránh mất mát [dữ liệu] sau khi giao dịch được kết thúc.

Thất bại trong việc duy trì dữ liệu ở trạng thái an toàn cũng có thể là một vấn đề về lưu giữ, cũng như việc không lưu giữ lại dữ liệu đó. Trong một số trường hợp, việc tiêu hủy dữ liệu, đặc biệt là dữ liệu là đối tượng của lưu giữ pháp lý trong một vấn đề pháp lý, có thể dẫn đến các kết luận bất lợi của tòa án và các biện pháp trừng phạt. Ngay cả khi việc phá hủy dữ liệu là vô tình hay cố ý, nó vẫn bị xử phạt, bởi vì công ty có trách nhiệm bảo vệ nó. Lưu giữ pháp lý có thể gia tăng thêm sự phức tạp đáng kể cho các nỗ lực lưu giữ dữ liệu, vì nó [lưu giữ pháp lý] buộc phải đảm bảo lưu trữ dữ liệu riêng biệt cho đến khi các vấn đề pháp lý đã được giải quyết xong. Khi dữ liệu đang nằm trong quy trình lưu giữ pháp lý, đồng hồ lưu giữ của dữ liệu sẽ không bị hết hạn cho đến khi lệnh lưu giữ được dỡ bỏ. Điều này khiến cho việc xác định, gán nhãn và duy trì dữ liệu là đối tượng của lưu giữ pháp lý trở thành một khía cạnh bổ sung cho các cân nhắc lưu trữ thông thường.



**MÁCH NƯỚC CHO KỲ THI** Các chính sách ưu giữ dữ liệu khác nhau tùy theo mỗi tổ chức. Tuy nhiên, một số thông tin chẳng hạn như PHI có thể phải tuân theo các quy định yêu cầu những quy tắc lưu giữ dữ liệu cụ thể.

## Tóm tắt Chương

Trong chương này, đầu tiên, bạn làm quen với các kế hoạch và quy trình ứng phó sự cố. Theo quy trình ứng phó sự cố, mô hình chuẩn bị, xác định, ngăn chặn, loại bỏ, khôi phục và bài học kinh nghiệm đã được trình bày. Chủ đề chính tiếp theo là các bài tập. Trong phần thảo luận này, các dạng bài tập khác nhau (diễn tập trên bàn, diễn tập và mô phỏng) đã được trình bày.

Phần chính tiếp theo xem xét các khuôn khổ tấn công. Khuôn khổ MITRE ATT&CK được trình bày, tiếp theo là Mô hình Kim cương về Phân tích Xâm nhập và mô hình Cyber Kill Chain. Việc quản lý các bên liên quan đã được đề cập cũng như các kế hoạch truyền thông khi xảy ra sự cố.

Chương này kết thúc bằng việc xem xét các kế hoạch khôi phục sau thảm họa, kế hoạch liên tục kinh doanh và tính liên tục của kế hoạch hoạt động. Thành phần của nhóm ứng phó sự cố cũng đã được đề cập và các chính sách lưu giữ liên quan đến dữ liệu ứng phó sự cố cũng đã được trình bày.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Giai đoạn nào của quy trình ứng phó sự cố diễn ra trước một sự cố thực tế?

  - A. Chuẩn bị
  - B. Xác định
  - C. Ngăn chặn
  - D. Phòng ngừa.
2. Giai đoạn nào của quá trình ứng phó sự cố đề cập đến việc loại bỏ sự cố?

  - A. Nhận dạng
  - B. Diệt trừ
  - C. Khôi phục
  - D. Giảm nhẹ.
3. Thuật ngữ nào được sử dụng để mô tả các bước mà một tổ chức thực hiện sau bất kỳ tình huống nào được xác định là bất thường trong hoạt động của một hệ thống máy tính?

  - A. Kế hoạch sự cố xâm nhập mạng/máy tính
  - B. Kế hoạch ứng phó sự cố
  - C. Khôi phục sao lưu và cấu hình lại
  - D. Ứng phó với sự kiện mạng.
4. Thuật ngữ nào chỉ tập hợp các bước cần thiết để phát triển một kế hoạch toàn diện nhằm ban hành trong một tình huống các hoạt động bình thường bị gián đoạn là gì?

  - A. Khôi phục sau thảm họa
  - B. Lập kế hoạch hoạt động liên tục

- C.** Lập kế hoạch ứng phó sự cố
- D.** Lập kế hoạch khôi phục các chức năng kinh doanh.
- 5.** Trong giai đoạn nào của quá trình ứng phó sự cố, các hành động được thực hiện để hạn chế sự cố ở số lượng máy tối thiểu?
- A.** Diệt trừ
- B.** Nhận dạng
- C.** Ngăn chặn
- D.** Khôi phục.
- 6.** Điều gì dưới đây không thuộc về Mô hình Kim cương về Phân tích Xâm nhập?
- A.** Nạn nhân
- B.** Cơ sở hạ tầng
- C.** Đối thủ
- D.** Lỗi hổng.
- 7.** Đối với các tổ chức đưa ra sự khác biệt giữa BCP và DRP, phát biểu nào sau đây là đúng?
- A.** BCP nêu chi tiết các chức năng quan trọng nhất và vạch ra thứ tự mà theo đó, các chức năng quan trọng cần được đưa trở lại hoạt động để duy trì hoạt động kinh doanh.
- B.** BCP là một tập con của DRP.
- C.** DRP phác thảo bộ chức năng nghiệp vụ tối thiểu cần thiết để tổ chức tiếp tục hoạt động.
- D.** DRP luôn được phát triển trước, và BCP thường là phần đính kèm của tài liệu này.
- 8.** Điều nào dưới đây là một phần của Cyber Kill Chain? (Chọn tất cả các đáp án đúng).
- A.** Do thám
- B.** Vũ khí hóa
- C.** Chống-diều-tra-pháp-y

**D. Cài đặt.**

- 9.** Có hai yếu tố chính đóng vai trò quyết định mức độ ứng phó với sự cố. Tính trọng yếu của thông tin là yếu tố quyết định chủ yếu. Yếu tố còn lại là gì?
- A.** Độ nhạy cảm thông tin hoặc phân loại dữ liệu
  - B.** Giá trị của bất kỳ dữ liệu nào bị mất trong sự cố
  - C.** Sự cố có thể ảnh hưởng đến hoạt động của tổ chức như thế nào
  - D.** Liệu tổ chức có muốn theo đuổi một giải pháp pháp lý chống lại (những) kẻ tấn công hay không.
- 10.** Cách tốt nhất để xử lý các hệ thống lớn, phức tạp có các yếu tố quy trình rất tốn kém và dài dòng trong một bài tập là gì?
- A.** Diễn tập trên bàn (tabletop)
  - B.** Diễn tập
  - C.** Mô phỏng
  - D.** Bỏ qua yếu tố này.

## Đáp án

- A.** Chuẩn bị là giai đoạn ứng phó sự cố xảy ra trước một sự cố cụ thể. Chuẩn bị bao gồm tất cả các nhiệm vụ cần thiết để được tổ chức và sẵn sàng để ứng phó với một sự cố. Hành động xác định đi đến quyết định rằng thông tin liên quan đến sự cố đáng được điều tra thêm bởi nhóm IR. Ngăn chặn là tập hợp các hành động được thực hiện để hạn chế sự cố ở số lượng máy tối thiểu. Phòng ngừa không phải là một giai đoạn của quá trình ứng phó sự cố.
- B.** Loại bỏ liên quan đến việc loại bỏ vấn đề và trong môi trường hệ thống phức tạp ngày nay, điều này có thể có nghĩa là xây dựng lại một máy tính hoàn toàn sạch. Hành động xác định đi đến quyết định rằng thông tin liên quan đến vụ việc đáng được điều tra thêm bởi nhóm IR. Quá trình khôi phục bao gồm các bước cần thiết để đưa hệ thống và ứng dụng trở về trạng thái hoạt động. Giảm nhẹ không phải là một giai đoạn trong quy trình ứng phó sự cố.
- B.** Kế hoạch ứng phó sự cố là thuật ngữ được sử dụng để mô tả các bước mà một tổ chức sẽ thực hiện để ứng phó với bất kỳ tình huống nào được xác định là bất thường trong hoạt động của hệ thống máy tính.
- B.** Lập kế hoạch liên tục hoạt động là tập hợp các bước cần thiết để phát triển một kế hoạch toàn diện để ban hành trong một tình huống khi các hoạt động bình thường bị gián đoạn. Khôi phục sau thảm họa là quá trình mà một tổ chức sử dụng để khôi phục sau các sự kiện gây gián đoạn hoạt động bình thường. Kế hoạch ứng phó sự cố mô tả các bước mà tổ chức thực hiện để ứng phó với bất kỳ tình huống nào được xác định là bất thường trong hoạt động của hệ thống máy tính. Lập kế hoạch khôi phục các chức năng nghiệp vụ không phải là một thuật ngữ tiêu chuẩn được sử dụng trong lập kế hoạch khôi phục.

5. **C.** Ngăn chặn là tập hợp các hành động được thực hiện để hạn chế sự cố chỉ nằm trong số lượng máy tối thiểu. Loại bỏ liên quan đến việc loại bỏ vấn đề và trong môi trường hệ thống phức tạp ngày nay, điều này có thể có nghĩa là xây dựng lại một máy tính hoàn toàn sạch. Hành động xác định đi đến quyết định rằng thông tin liên quan đến vụ việc đáng được điều tra thêm bởi nhóm IR. Quá trình khôi phục bao gồm các bước cần thiết để đưa hệ thống và ứng dụng trở về trạng thái hoạt động.
6. **D.** Lỗ hổng bảo mật không phải là một nút chính thức của Mô hình kim cương để phân tích xâm nhập. Nút thứ tư là năng lực.
7. **A.** Rất nhiều tổ chức, đặc biệt là những tổ chức nhỏ hơn, coi hai thuật ngữ BCP và DRP là đồng nghĩa, nhưng đối với những tổ chức khác, BCP phác thảo các chức năng nghiệp vụ cần thiết để tiếp tục hoạt động và có thể mô tả thứ tự các chức năng sẽ được khôi phục. DRP phác thảo tất cả các quy trình và cách chúng có thể được khôi phục như thế nào, BCP hoạt động như một tài liệu đồng hành mô tả chức năng nào cần được khôi phục và theo thứ tự nào.
8. **A, B và D.** Do thám, vũ khí hóa và cài đặt là các bước trong Cyber Kill Chain. Chống-điều-tra-pháp-y: không, mặc dù những hành động này có thể xảy ra nhưng chúng được nhúng trong các bước khác.
9. **C.** Yếu tố thứ hai liên quan đến một quyết định kinh doanh về cách thức mà một sự cố ảnh hưởng đến hoạt động kinh doanh hiện tại. Một loạt các vi phạm, dù nhỏ hay lớn, đều cho thấy một mô hình có thể có các vấn đề về quan hệ công chúng và quy định.
10. **C.** Mô phỏng là một công cụ rất có giá trị để bắt chước các bộ phận của một quy trình không thể đưa được vào bài tập vì chi phí, thời gian, nguồn lực hoặc các ràng buộc khác.

## Chương 28    Điều tra

---

### Điều tra

Trong chương này bạn sẽ

- Tìm hiểu về các nguồn thông tin khác nhau được sử dụng để hỗ trợ cho một cuộc điều tra,
  - Tìm hiểu về cách để kết hợp các nguồn dữ liệu thích hợp để hỗ trợ cho một cuộc điều tra.
- 

Các cuộc điều tra được sử dụng để xác định xem điều gì đã xảy ra, ai đã làm gì và những yếu tố nào của hệ thống thông tin đã bị ảnh hưởng bởi một số sự kiện hoặc chuỗi sự kiện cụ thể. Các yếu tố cần phải được điều tra về hoạt động và sự thay đổi trái phép bao gồm cả các phần tử dữ liệu trong hệ thống và bản thân hệ thống. Có thể có nhiều dữ liệu chẩn đoán và điều tra đã được thu thập như một phần của hoạt động bảo mật đang diễn ra hoặc được phát triển để ứng phó với một sự cố. Chương này xem xét cách sử dụng các nguồn dữ liệu này để hỗ trợ cho một cuộc điều tra và làm sáng tỏ những gì đã thực sự xảy ra với cả hệ thống và dữ liệu mà nó xử lý.

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 4.3 của kỳ thi CompTIA Security+: Khi xảy ra sự cố, hãy sử dụng các nguồn dữ liệu thích hợp để hỗ trợ điều tra.

## Kết quả đầu ra từ việc Quét Lỗ hổng

*Kết quả đầu ra từ việc quét lỗ hổng bảo mật cung cấp thông tin về hệ thống đang hoạt động, về bất kỳ dịch vụ bổ sung nào đang lắng nghe trên mạng và các lỗ hổng bảo mật đã biết chống lại từng hệ thống hoặc dịch vụ này. Thông tin này quan trọng theo nhiều cách. Đầu tiên, nó cho phép xác minh rằng các hệ thống được ủy quyền đã được vá lỗi một cách đầy đủ. Các hệ thống có lỗ hổng đóng vai trò như là điểm xâm nhập cho những kẻ tấn công và việc đảm bảo các điểm xâm nhập này được đóng lại là điều quan trọng. Thứ hai, và thậm chí quan trọng hơn, là việc xác định các dịch vụ bổ sung. Những dịch vụ này có thể được vá hoặc có thể không và chúng cũng đại diện cho một tuyến đường dẫn vào hệ thống cho kẻ tấn công. Việc có các dịch vụ bổ sung đang hoạt động một cách không cần thiết chỉ làm gia tăng diện tích bề mặt tấn công, khiến cho kẻ tấn công dễ dàng xâm nhập vào hệ thống hơn. Điểm mấu chốt: một báo cáo lỗ hổng bảo mật cung cấp cho bạn thông tin về những gì đang diễn trên mạng của bạn, dù là hợp pháp hay không.*

## Thông tin tổng quan SIEM

*Bảng thông tin tổng quan SIEM (security information and event management - quản lý thông tin bảo mật và sự kiện) là các cửa sổ vào kho dữ liệu SIEM, một bộ sưu tập thông tin có thể cho bạn biết nơi các cuộc tấn công đang diễn ra và cung cấp một dấu vết để cho biết cách thức kẻ tấn công đã xâm nhập vào mạng và di chuyển đến vị trí hiện tại của chúng. Hệ thống SIEM hoạt động như một kho lưu trữ thông tin dành cho những thông tin xung quanh các cuộc xâm nhập tiềm năng và thực tế. Trong quá trình điều tra, hệ thống SIEM có thể cung cấp một loạt thông tin liên quan đến người dùng, những gì họ đã thực hiện, v.v... Mục đích cơ bản của hệ thống SIEM là cung cấp cảnh báo và thông tin liên quan cho các đội ứng phó sự cố đang tiến hành điều tra về sự cố. Nếu điều gì đó xảy ra đã khởi đầu một cuộc điều tra và hệ thống SIEM không*

có những thông tin liên quan thì điều này cho thấy rằng SIEM và các yếu tố cấu thành của nó cần được điều chỉnh tốt hơn để mang lại sự giám sát có ý nghĩa của hệ thống đối với các vấn đề tiềm ẩn.



**MÁCH NƯỚC CHO KỲ THI** Các SIEM cho phép bạn xác định, trực quan hóa, và giám sát các xu hướng thông qua các cảnh báo và một trang thông tin tổng quan.

### Cảm biến

Các *cảm biến* là những thiết bị cung cấp dữ liệu bảo mật cho kho dữ liệu bảo mật. Bất kể kho dữ liệu đó được đặt ở đâu, thông tin bảo mật vẫn là điều quan trọng đối với các nhà điều tra. Các cảm biến không chỉ xảy ra, chúng phải được đặt đúng vị trí để thu thập được thông tin. Vị trí đặt cảm biến bắt đầu với việc xác định các mục tiêu thu thập. Nghiên cứu về vị trí của luồng dữ liệu, thông tin có giá trị đang ở đâu trong mạng và nơi mà các đối thủ có thể tiếp cận, cùng với thông tin bạn muốn thu thập, chỉ là một trong số các yếu tố được đưa vào quá trình thiết kế vị trí đặt cảm biến. Giống như nhật ký có thể cung cấp một loạt các thông tin hữu ích nhưng đồng thời chúng cũng có thể tạo ra nhiều dữ liệu vô nghĩa. Cảm biến cũng không khác. Các cảm biến bắt những gói tin có thể ghi lại những thông tin quan trọng cho một cuộc điều tra, nhưng chúng phải ở đúng vị trí (nghĩa là có tính minh bạch liên quan đến các gói tin được mong đợi) đồng thời tránh các khu vực lưu lượng chung, nơi có nhiều tiếng ồn. Để được chuẩn bị một cách thích hợp cho các cuộc điều tra trong tương lai, bạn cần thiết kế và đặt các cảm biến của mình một cách hợp lý.

## Độ nhạy

*Độ nhạy* là chất lượng của việc nhanh chóng phát hiện hoặc phản ứng với những thay đổi, tín hiệu hoặc những ảnh hưởng nhỏ. Do mục đích của hệ thống SIEM là cảnh báo cho người vận hành về những thay đổi chỉ ra các sự kiện quan trọng nên độ nhạy đối với những sự kiện đó là điều rất quan trọng. Vấn đề lớn nhất với SIEM và độ nhạy là sự đánh đổi giữa dương tính giả và âm tính giả. Nếu bạn cảnh báo về quá nhiều những điều kiện có thể xảy ra, bạn sẽ làm gia tăng kết quả dương tính giả và gây ra sự mệt mỏi cho nhân viên vận hành. Chờ đợi quá nhiều dữ liệu và bạn bỏ sót một số dữ liệu, tạo ra một kết quả âm tính giả và ẩn tượng rằng hệ thống SIEM không hoạt động. Việc điều chỉnh độ nhạy cho đến khi bạn có được sự cân bằng phù hợp là một nhiệm vụ khó khăn nhưng rất quan trọng.

## Khuynh hướng

Các *khuynh hướng* là một chuỗi các điểm dữ liệu chỉ ra sự thay đổi theo thời gian. Các khuynh hướng có thể tăng, giảm, theo chu kỳ hoặc liên quan đến sự thay đổi. Điều quan trọng là các xu hướng chỉ ra một số hình thức thay đổi. Không phải tất cả các hình thức thay đổi đều phù hợp với sứ mệnh của hệ thống SIEM và yếu tố quan trọng là hiểu được những thay đổi nào thực sự là thay đổi và thay đổi nào không. Một số thay đổi quan trọng theo cách trực tiếp, chẳng hạn như những lần đăng nhập không thành công. Nếu số lần đăng nhập thất bại trung bình là 20 lần mỗi ngày và đột nhiên bạn nhận được 10.000 lần trong một giờ, điều ngày cho thấy đã có điều gì đó bị thay đổi. Một kẻ tấn công? Một tập lệnh kịch bản có lỗi? Sẽ cần có một số cuộc điều tra để tìm ra. Điều gì sẽ xảy ra nếu những lỗi tương tự đó xảy ra với bốn người dùng, với mọi quản trị viên hệ thống? Khuynh hướng là quan trọng, nhưng thông tin đăng sau chúng cũng vậy. Điều này khiến cho việc cảnh báo về nhiều

hạng mục có báo cáo toàn diện tốt sẽ hữu ích hơn chỉ là một cảnh báo cho biết “con số này quá cao”. Bối cảnh mới là vấn đề.

## Cảnh báo

Các *cảnh báo* là phương pháp chủ yếu để giao tiếp giữa hệ thống SIEM và nhân viên vận hành. Khi các điều kiện thỏa những yêu cầu quy tắc, hệ thống SIEM có thể gửi một cảnh báo. Càng có nhiều thông tin hơn có thể được cung cấp trong cảnh báo (những thông tin có liên quan khác, bối cảnh của sự kiện, v.v...) thì cảnh báo càng tốt hơn. Điều quan trọng không phải là nói cho một kỹ sư bảo mật biết rằng “một điều gì đó đã diễn ra, hãy đi tìm hiểu xem đó là gì”, thay vào đó, để hướng dẫn cho kỹ sư bảo mật định hướng đúng đắn với những thông tin bổ sung mà nhân viên vận hành có thể diễn giải và sau đó đặt ra một kế hoạch để điều tra một cách hiệu quả.

## Tương quan

*Tương quan* là quá trình thiết lập một mối quan hệ giữa hai biến số. Tuy nhiên, như một nhà khoa học khôn ngoan đã từng tuyên bố, mỗi tương quan không phải là quan hệ nhân quả, có nghĩa là chỉ vì các phép đo có xu hướng cùng nhau không có nghĩa là cái này gây ra cái kia. Thường xuyên có một yếu tố khác đang diễn ra, một số biến số nào đó đã không được đo lường. Hãy nghĩ về một loạt các lần đăng nhập không thành công đến từ một địa chỉ IP cũng đã bị từ chối tại tường lửa cho hoạt động quét. Hoặc một số các lỗi kiểm soát truy cập, và hoạt động chẳng hạn như đăng nhập thành công với tên người dùng khác từ cùng một địa chỉ IP trong một khoảng thời gian ngắn thì sao? Hoặc một gói UDP có cổng đích là 67, nhưng địa chỉ đích không phải là một trong các máy chủ DHCP của bạn? Tương quan chính là phương tiện để hệ thống SIEM áp dụng các quy tắc kết hợp các nguồn dữ liệu để phát hiện sự kiện tinh chỉnh.



**MÁCH NƯỚC CHO KỲ THI** Các nhật ký tương quan sự kiện SIEM là cực kỳ hữu ích bởi vì chúng có thể được sử dụng để xác định những hoạt động độc hại trên một loạt các thiết bị và chương trình. Đây có thể là những dữ liệu đã không được chú ý.

### Tập tin Nhật ký

Các *tập tin nhật ký* là một nguồn thông tin chính trong quá trình điều tra. Phần mềm có thể ghi lại trong các tập tin nhật ký một loạt thông tin trong khi nó (phần mềm) đang hoạt động. Từ kiểm tra sức-khỏe-bản-thân đến dữ liệu liên-quan-đến-lỗi, đến siêu dữ liệu vận hành hỗ trợ cho các sự kiện đang diễn ra trên một hệ thống, tất cả những dữ liệu này cuối cùng đều nằm trong các tập tin nhật ký. Những tập tin nhật ký này đóng vai trò như một hồ sơ lịch sử về những gì đã từng xảy ra trên một hệ thống. Các tập tin nhật ký yêu cầu việc thiết lập cấu hình bởi vì nếu bạn không ghi nhật ký lại một sự kiện khi nó diễn ra, bạn không thể quay ngược lại thời điểm đó để nắm bắt nó (sự kiện). Tương tự, việc ghi nhật ký lại mọi thứ sẽ tạo ra quá nhiều dữ liệu - dữ liệu phải được xem qua trong quá trình điều tra. Chìa khóa là sự cân bằng: ghi lại những gì bạn cần biết để đưa ra quyết định — không hơn, không kém.

### Mạng

Các mạng chứa đầy các thiết bị có thể cung cấp những thông tin nhật ký vô giá. Các tường lửa, bộ định tuyến, bộ cân bằng tải và bộ chuyển mạch có thể cung cấp rất nhiều thông tin về những gì đang xảy ra trên mạng. Các *nhật ký mạng* có xu hướng trùng lặp các vấn đề vì các gói tin có thể đi qua một số thiết bị, tạo ra nhiều bản ghi gần như giống nhau. Việc loại bỏ dữ liệu trùng lặp cũng như không có liên quan là một thách thức đối với việc ghi nhật ký mạng, nhưng lợi ích có thể rất lớn vì việc ghi nhật ký thích hợp có thể giúp truy tìm ra kẻ tấn công dễ dàng hơn.

## Hệ thống

Hầu như mọi hệ điều hành đều tạo ra các *nhật ký hệ thống*. Những nhật ký này có thể cung cấp một lịch sử rất chi tiết về những hành động đã được thực hiện trên một hệ thống. Các hồ sơ đăng nhập cho biết những lần đăng nhập không thành công có thể quan trọng, nhưng các mục hiển thị sự đăng nhập thành công cũng vậy. Nhiều lần thất bại sau một lần thành công có thể là điều đáng ngờ, đặc biệt là khi số lần thất bại và thời gian loại trừ thao tác nhập của nhân viên vận hành. Còn về lỗi quyền truy cập thì sao? Những điều này có thể chỉ ra nỗ lực thực hiện hoạt động trái phép. Truy cập thành công thì sao? Việc ghi nhật ký lại những điều này sẽ làm cơ sở dữ liệu tràn ngập bằng một số lượng lớn các bản ghi không liên quan. Đây là một trong những thách thức khi ghi nhật ký lại mọi thứ trên hệ thống - nhật ký nào tạo ra những câu trả lời có ý nghĩa và nhật ký nào chỉ tạo ra tiếng ồn? Ngoài ra, hãy nhận thức được rằng quyết định ghi nhật ký phải xảy ra trước khi một sự kiện xảy ra, hay nói cách khác, bạn không thể quay lại và làm-lại nếu bạn đã không ghi lại được nhật ký về một phần bằng chứng quan trọng.

## Ứng dụng

Các *nhật ký ứng dụng* được tạo ra bởi chính ứng dụng khi chúng hoạt động. Một số ứng dụng cung cấp ghi nhật ký với phạm vi rộng rãi, những ứng dụng khác ghi nhật ký tối thiểu hoặc thậm chí không ghi nhật ký. Một số ứng dụng cho phép cấu hình những gì được ghi lại, những ứng dụng khác thì không. Rất nhiều ứng dụng máy chủ - máy chủ web, máy chủ thư và máy chủ cơ sở dữ liệu - có khả năng ghi nhật ký bao quát, bao gồm người dùng đã thực hiện hành động nào và vào khi nào. Các hệ thống khác chỉ ghi nhật ký khi chúng bắt đầu và dừng hoạt động và có thể ghi lại các lỗi.

## Bảo mật

Các *nhật ký bảo mật* là những nhật ký được lưu giữ bởi Hệ điều hành về siêu dữ liệu có liên quan đến hoạt động bảo mật. Trong Microsoft Windows, hàng trăm sự kiện khác nhau có thể được định cấu hình để ghi vào Nhật ký bảo mật - khởi động hệ thống, tắt hệ thống, lỗi về quyền, đăng nhập, đăng nhập không thành công, thay đổi thời gian hệ thống, tạo tiến trình mới, thay đổi tác vụ đã được lập lịch trình, v.v... Những nhật ký này có thể rất quan trọng, nhưng để trở nên quan trọng, chúng cần phải được điều chỉnh để thu thập được những thông tin cần thiết. Trong Windows, điều này thường được thực hiện thông qua các đối tượng chính sách nhóm. Động lực thúc đẩy những gì cần được ghi lại là chính sách kiểm toán của hệ thống, một tuyên bố về những hồ sơ nào cần được lưu giữ lại.



### MÁCH NƯỚC CHO KỲ THI

Windows Event Viewer được sử dụng để xem các nhật ký của Windows. Nhật ký Hệ thống hiển thị thông tin liên quan đến hệ điều hành. Nhật ký Ứng dụng cung cấp dữ liệu liên quan đến các ứng dụng đang chạy trên hệ thống. Nhật ký Bảo mật cung cấp thông tin về sự thành công và thất bại của các lần đăng nhập đã cố gắng cũng như các sự kiện kiểm toán liên-quan-đến-bảo-mật. Hãy sẵn sàng để xác định kết quả đầu ra của tập tin nhật ký cụ thể trong kỳ thi!

## Web

Các máy chủ web hồi đáp lại các yêu cầu về tài nguyên đã được định dạng và cụ thể bằng các phản hồi, cho dù ở dạng trang web hay một lỗi. Và mọi hoạt động này đều có thể được ghi lại. Các máy chủ web được triển khai một cách cụ thể để thực hiện nhiệm vụ này nhưng chúng cũng là mục tiêu của các cuộc tấn công - các cuộc tấn công cố gắng chạy các lệnh kịch bản độc hại, thực hiện các cuộc tấn công DDoS, thực hiện

các cuộc tấn công chèn (lệnh) và kịch bản chéo-trang, v.v... Các tập tin nhật ký web có thể giúp xác định khi nào các hoạt động này đang diễn ra.

## DNS

Các *nhật ký DNS*, khi đã được bật, có thể chứa một bản ghi cho mọi truy vấn và phản hồi (DNS). Đây có thể là một kho tàng thông tin cho chuyên viên điều tra vì nó có thể tiết lộ phần mềm độc hại đang gọi đến máy chủ điều-khiển-và-kiểm-soát của nó hoặc chuyển dữ liệu đến các địa điểm không-phải-của-công-ty. Phân tích nhật ký DNS có thể hiển thị các địa chỉ IP và tên miền mà những hệ thống của bạn nên giao tiếp cũng như những địa chỉ mà chúng không nên giao tiếp. Trong trường hợp kẻ tấn công hoặc phần mềm độc hại đang thực hiện giao tiếp, những kênh giao tiếp này có thể gần như bị ẩn trên mạng nhưng hệ thống DNS, là một phần của kiến trúc mạng, có thể ghi lại các hoạt động. Đây là một trong những lý do tại sao nhật ký DNS là một trong số các nhật ký có giá trị nhất để đưa vào hệ thống SIEM.

## Xác thực

*Nhật ký xác thực* chứa những thông tin về các lần xác thực thành công và thất bại. Nguồn thông tin nhật ký xác thực phổ biến nhất đến từ các nhật ký bảo mật của hệ thống, nhưng cũng tồn tại các nguồn bổ sung khác. Với sự mở rộng của các dịch vụ xác thực đa yếu tố, các ứng dụng quản lý các yếu tố (xác thực) thứ hai cũng có các nhật ký. Những nhật ký này rất quan trọng vì chúng có thể hiển thị những điều bất thường chẳng hạn như dữ liệu đăng nhập chính xác nhưng dữ liệu yếu-tố-thứ-hai thất bại, cho thấy rằng thông tin xác thực chính có thể đã bị tiết lộ.

## Các Tập tin Kết xuất

*Các tập tin kết xuất* là bản sao của những gì đã từng có trong bộ nhớ tại một thời điểm - thường là một thời điểm khi một số lỗi xảy ra. Các tập tin kết xuất có thể được tạo ra bởi hệ điều hành (OS) khi hệ điều hành gặp sự cố, và những tập tin này có thể được phân tích để xác định được nguyên nhân của sự cố. Các tập tin kết xuất cũng có thể được tạo ra bởi một số tiện ích và sau đó được chuyển đến bên thứ ba để phân tích khi ứng dụng hoạt động không chính xác. Tập tin kết xuất có thể chứa rất nhiều loại thông tin nhạy cảm, bao gồm cả mật khẩu, khóa mật mã, v.v... Nên cẩn trọng khi xử lý các tập tin kết xuất và đặc biệt là khi chia sẻ chúng để phân tích. Một số nhà cung cấp bảo mật có các công cụ hỗ trợ bảo mật thông tin nhạy cảm trong các tập tin kết xuất, nhưng nguy cơ lộ bí mật vẫn hiện hữu. Do quy mô và độ phức tạp liên quan đến việc diễn giải các tập tin kết xuất nên chúng không phải là một công cụ điều tra phổ biến, ngoại trừ các cuộc điều tra ở phạm vi hẹp chẳng hạn như lý do tại sao hệ thống gặp sự cố.

Mặt khác, những kẻ tấn công thích lấy các tập tin kết xuất và đọc trộm chúng, do đó, việc thiết lập hệ thống để không tồn tại các tập tin kết xuất nhằm ngăn chặn tin tặc làm hỏng máy chủ và sau đó quay lại để lấy tập tin kết xuất tiếp theo.

## VoIP và Quản lý Cuộc gọi

Các giải pháp *thoại qua IP (VoIP)* và các ứng dụng *quản lý cuộc gọi* cho phép một loạt các dịch vụ giao tiếp bằng âm thanh và hình ảnh qua Internet. Các hệ thống này có thể ghi lại nhật ký về nhiều loại dữ liệu, bao gồm thông tin cuộc gọi như số được gọi (gọi đến và đi), thời gian của cuộc gọi và thời lượng của cuộc gọi. Các bản ghi này được gọi là bản ghi chi tiết cuộc gọi (call detail records - CDR). Khi được kết hợp với hệ thống video và âm thanh sử dụng VoIP, các nhật ký này có thể được tăng

cường thông tin về cách thông tin được mã hóa, bao gồm các codec liên quan và độ phân giải.

### **Lưu Lượng Giao thức Khởi đầu Phiên (SIP)**

Giao thức Khởi tạo Phiên (Session Initiation Protocol - SIP) là một giao thức dựa-trên-văn-bản được sử dụng để tạo tín hiệu các ứng dụng thoại, video và nhắn tin thông qua IP. SIP cung cấp thông tin để khởi đầu, duy trì và kết thúc các phiên thời-gian-thực. *Nhật ký lưu lượng SIP* thường ở Định dạng Nhật ký Chung SIP (Common Log Format - CLF), bắt chước nhật ký của máy chủ web và nắm bắt các chi tiết liên quan đến giao tiếp (chẳng hạn như đến và đi).

### **Syslog/Rsyslog/Syslog-ng**

*Syslog* là viết tắt của System Logging Protocol và là một giao thức tiêu chuẩn được sử dụng trong hệ thống Linux để gửi nhật ký hệ thống hoặc thông điệp về sự kiện đến một máy chủ cụ thể, được gọi là máy chủ nhật ký hệ thống. *Rsyslog* là một biến thể mã nguồn mở của syslog, tuân theo các đặc tả thông số kỹ thuật nhật ký hệ thống nhưng cũng cung cấp các tính năng bổ sung như lọc dựa-trên-nội-dung. *Syslog-ng* là một triển khai mã nguồn mở khác của tiêu chuẩn syslog. Syslog-ng cũng mở rộng mô hình nhật ký hệ thống nguyên thủy bằng các yếu tố như lọc nội dung. Một ưu điểm chính của syslog-ng so với syslog và rsyslog là nó có thể gắn thẻ, phân loại và tương quan theo thời gian thực, và điều này có thể cải thiện hiệu suất SIEM. Đối với các hệ thống dựa-trên-Linux, những triển khai này là tiêu chuẩn thực tế để quản lý các tập tin nhật ký. Vì tập tin nhật ký là một trong những nguồn hiện vật chính, các cuộc điều tra sử dụng đáng kể các tập tin nhật ký và dữ liệu được ghi-lại-nhật-ký-hệ-thống để xây dựng lịch sử về những gì đã thực sự xảy ra trên một hệ thống.



**MÁCH NƯỚC CHO KỲ THI** Systlog, rsyslog và syslog-ng, tất cả đều chuyển dữ liệu thành các tập tin nhật ký trên một máy chủ nhật ký. Rsyslog và syslog-ng đều mở rộng tiêu chuẩn syslog nguyên thủy bằng cách bổ sung thêm những năng lực như lọc nội dung, làm giàu nhật ký, và tương quan các phần tử dữ liệu thành các sự kiện ở cấp-degree-cao-hơn.

### **Journalctl**

Trên hệ thống Linux, daemon ban đầu khởi chạy hệ thống được gọi là systemd. Khi systemd tạo tập tin nhật ký, nó sẽ thực hiện việc này thông qua dịch vụ systemd-journald. Journalctl là câu lệnh được sử dụng để xem các nhật ký này. Để xem các tùy chọn lệnh khác nhau cho journalctl, bạn nên tham khảo các trang chủ trên hệ thống. Dưới đây là một ví dụ về lệnh journalctl để xem các nhật ký cho một dịch vụ hệ thống nhất định:

```
journalctl -u ssh
```



**MÁCH NƯỚC CHO KỲ THI** Hãy tìm hiểu sự khác biệt giữa Journalctl và syslog. Journalctl là câu lệnh để kiểm tra nhật ký trên máy chủ. Syslog (và các biến thể rsyslog và syslog-ng) được sử dụng để di chuyển các nhật ký đến một máy chủ nhật ký và đôi khi để thao tác các mục nhập tập tin nhật ký trong khi chuyển tiếp.

### **NXLog**

*NXlog* là một công cụ quản lý nhật ký đa nền tảng được thiết kế để hỗ trợ việc sử dụng dữ liệu nhật ký trong quá trình điều tra. Bộ công cụ này có khả năng xử lý dữ liệu kiểu-nhật-ký-hệ-thống cũng như các định dạng nhật ký khác, bao gồm cả Microsoft Windows. Nó có các khả năng nâng

cao để làm phong phú các tập tin nhật ký thông qua tra cứu dựa-trên-ngữ-cảnh, các mối tương quan và làm giàu dựa-trên-quy-tắc. NXLog có các bộ kết nối với hầu hết các ứng dụng chính và có thể hoạt động như một công cụ thu thập nhật ký, bộ chuyển tiếp, tổng hợp và điều tra để tìm kiếm thông qua dữ liệu nhật ký. Do nhật ký là một trong những nguồn dữ liệu được sử dụng nhiều nhất trong các cuộc điều tra, các công cụ như NXLog có thể cho phép các chuyên viên điều tra xác định các vấn đề về bảo mật, vi phạm chính sách và các vấn đề hoạt động trong hệ thống.

### **Giám sát băng thông**

*Giám sát băng thông* là những tiện ích được thiết kế để đo lường việc sử dụng băng thông mạng theo thời gian. Giám sát băng thông có thể cung cấp những thông tin về lượng băng thông đang được sử dụng, theo loại dịch vụ và lượng băng thông còn lại. Giám sát băng thông có thể ghi lại thông tin này theo thời gian và cung cấp một hồ sơ lịch sử về các vấn đề tắc nghẽn mạng, bao gồm theo loại lưu lượng truy cập trong chất lượng của các mạng được-dịch-vụ-thực-thi.

### **Siêu Dữ liệu**

*Siêu dữ liệu* là dữ liệu về dữ liệu. Một mục nhập tập tin trên hệ thống lưu trữ có nội dung tập tin cộng với siêu dữ liệu, bao gồm tên tập tin, sự khởi tạo, truy cập và dấu thời gian cập nhật, kích thước, v.v... Tập tin Microsoft Word có nội dung tài liệu và các trường bổ sung về siêu dữ liệu tương ứng. Các tập tin hình ảnh JPEG có các trường siêu dữ liệu giống nhau, bao gồm vị trí chụp và thiết bị được sử dụng để tạo ra hình ảnh. Hàng tấn siêu dữ liệu tồn tại trên một hệ thống và trong rất nhiều trường hợp, các phần tử riêng lẻ của siêu dữ liệu cần được tương quan với các siêu dữ liệu khác để xác định được các hoạt động. Lấy ví dụ, khi một USB được cắm vào hệ thống. Điều này tạo ra siêu dữ liệu, nhưng dành cho người dùng nào? Siêu dữ liệu riêng biệt có thể cho bạn biết rằng ai đã

đăng nhập vào thời điểm đó. Việc thu thập, phân tích và tương quan siêu dữ liệu đều là một phần của hầu hết mọi cuộc điều tra.



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng tất cả những thứ gì là kỹ thuật số đều có chứa siêu dữ liệu, và việc tương quan siêu dữ liệu là một phần của hầu hết mọi cuộc điều tra.

### Email

Email có một nửa là siêu dữ liệu, một nửa là thông điệp. Đối với thông điệp ngắn, siêu dữ liệu có thể lớn hơn chính bản thân của thư. Siêu dữ liệu email nằm trong tiêu đề của email và bao gồm thông tin định tuyến, người gửi, người nhận, dấu thời gian, chủ đề và các thông tin khác liên quan đến việc gửi thư. Tiêu đề của email bao gồm thông tin về việc xử lý email giữa tác nhân người dùng thư (mail user agents - MUA), tác nhân chuyển thư (mail transfer agents - MTA) và đại lý gửi thư (mail delivery agents - MDA), cũng như một loạt các chi tiết khác. Toàn bộ thông điệp được gửi thông qua văn bản ASCII thuận túy, với các tập tin đính kèm được bao gồm bằng cách sử dụng mã hóa Base64. Tiêu đề email cung cấp tất cả những thông tin liên quan đến email khi nó di chuyển từ người gửi sang người nhận. Sau đây là một mẫu tiêu đề email:

Received: from smtp4.cc.uh.edu (129.7.234.211) by xFENode3B.mail.example.net (129.7.40.150) with Microsoft SMTP Server id 8.2.255.0; Sat, 11 Apr 2020 18:54:42 -0500  
Received: from smtp4.cc.uh.edu (smtp4.example.net [127.0.0.1]) by localhost (Postfix) with SMTP id BC4DA1E004A for <waconklin@example.com>; Sat, 11 Apr 2020 18:53:55 -0500 (CDT)  
Received: from nm22.bullet.mail.ne1.yahoo.com (nm22.bullet.mail.ne1.yahoo.com [98.138.90.85]) by smtp4.example.net (Postfix) with ESMTP id 538C31E0034 for <waconklin@example.com>; Sat, 11 Apr 2020 18:53:55 -0500 (CDT)  
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed;  
d=yahoo.com; s=s2048;  
t=1428796434; bh=esKcEn6Pe1DHaDx/5lqarnNbc5vZAFO5+z93Xt/06S0=;  
h=Date:From:Reply-To:To:In-Reply-To:References:Subject:From:Subject;  
b=OQTvNETmW6KKGn/cWXsQd43khTwbsGpRFhpwB0iCopROLVxabwPryOB/6Rpsb37JC5IYTxYrDj  
rslDhaSBj1381Y8ior9CS83YyV3JnRzk6F+YrDQDUXAuG5vbhDo91KUX0pNa/R4rdvK47T6uO9  
2k7wf1+egSLATDeId5ccUFUZLBQpxBjX6WtLjb16eValGPQLgLCNdhedkgGBEuP+yFfc0xDr97  
5eUYFsxwLDS36pi88etIkMso0FDbQLsGfk3SneIkm+o5wSDq71AsWk3NX4p+yFjW16V  
7OjQSG2XF6KnNt9gUh9v98U+WW/Crwlq110xUHL1FjiP6oNsGkw==  
Received: from [98.138.100.112] by nm22.bullet.mail.ne1.yahoo.com  
with NNFMPP;  
11 Apr 2020 23:53:54 -0000  
Received: from [98.138.89.173] by tm103.bullet.mail.ne1.yahoo.com  
with NNFMPP;  
11 Apr 2020 23:53:53 -0000  
  
Received: from [127.0.0.1] by omp1029.mail.ne1.yahoo.com with NNFMPP;  
11 Apr 2020 23:53:53 -0000  
X-Yahoo-Newman-Property: ymail-5  
X-Yahoo-Newman-Id: 880223.99814.bm@omp1029.mail.ne1.yahoo.com  
X-YMail-OSG: NKvYQJKVM1kWuLmyDvNnFXECaMumy9LBgfZhcKRiubzkoq9\_NVdEUqlT7hMlkOv  
1oWFqcbcbyJwpOTgEmUZIsGX2ZpKSfNrUUzmQ3.ksRewbg9xRVVDqnQbdJksIfreePVCUGNJ26elD  
Ts4mEjfKzWPgKiXkxmy8iNhDzs zw0RmJpDOrDymsdTE3ObnKA83ZXsj9w0CwXnkJ\_UtmVSWtylo  
NLdv8KRSP10TaW8APZeaAmmTKPO06z.8jJg.GOGWAZbonqsm\_zXvMjcfmmQ8wd8PB0h2pFqzvwn  
  
cfwHL3.iDmOzcNBYrF5mNfbmdaoHAztYxA8edB2kFqN3vje3VJPkoPOCiOhq\_c\_wFIss8E6W02Vjk  
0gCJRLAPEwo30kyz\_QDyGgfpfv4GAXrz9bQet8sy\_e2ztRyVnj9GDu.DHSYnU5TaTLzvRhMQO3p  
082zOb2Qm\_4Miilk36RzypHRAEWh\_G1Txr3sRloz1RhsioTgMYqksk0E\_7P2bBJOJb3HsTyG2o\_i  
swOuz7CIt8U67Fe1IlDoPsU5hJj8DXH1SK\_pGU13j  
  
Received: by 98.138.105.206; Sat, 11 Apr 2020 23:53:53 +0000  
Date: Sat, 11 Apr 2020 23:53:52 +0000  
From: Sender Name <SenderName@yahoo.com>  
Reply-To: Sender Name <SenderName@yahoo.com>  
To: "Conklin, Wm. Arthur" <waconklin@example.com>  
Message-ID: 517184424.1041513.1428796432644.JavaMail.yahoo@mail.yahoo.com  
In-Reply-To: 9AF24FE2BE34BC42A10F1DE75C05D8871652896780@EXSERVER3.example.com  
References: 9AF24FE2BE34BC42A10F1DE75C05D8871652896780@EXSERVER3.example.com  
Subject: Re: Homework Lab 2  
MIME-Version: 1.0  
Content-Type: multipart/mixed;  
boundary="----=\_Part\_1041512\_683422731.1428796432643"  
X-PMX-Version: 6.0.3.2322014, Antispam-Engine: 2.7.2.2107409, Antispam-Data: 2015.4.11.234523  
X-PerlMx-Spam: Gauge=IIIIIIII, Probability=8%, Report='  
HTML\_50\_70 0.1, HTML\_NO\_HTTP 0.1, BODYTEXTH\_SIZE\_10000\_LESS 0,  
BODYTEXTP\_SIZE\_3000\_LESS 0, BODY\_SIZE\_10000\_PLUS 0, DKIM\_SIGNATURE 0,  
ECARD\_KNOWN\_DOMAINS 0, REFERENCES 0, WEBMAIL\_SOURCE 0, ANY\_URI 0,  
BOUNCE\_CHALLENGE\_SUBJ 0, BOUNCE\_NDR\_SUBJ\_EXEMPT 0, C230066\_P1\_5 0,  
Return-Path: <SenderName@yahoo.com>

Dữ liệu tiêu đề tập tin có thể rất quan trọng trong quá trình điều tra bởi vì nó có thể hiển thị những chi tiết như dưới đây:

- **Từ (From)** Chứa những thông tin về nơi mà thông điệp được gửi đi (có thể bị giả mạo một cách dễ dàng).
- **Đến (To)** Đầu nhận cuối cùng của email (không nhất thiết phải là địa chỉ email của người nhận).
- **Chủ đề (Subject)** Hãy nghĩ về điều này như là “tiêu đề” hoặc chủ đề mà người gửi đã thiết lập cho email của họ.
- **Ngày (Date)** Đây là ngày giờ khi email được viết ra.
- **Đường-Trả-về (Return-Path)** Còn được gọi là Trả-lời-Cho (Reply-To), trường này bao gồm địa chỉ nơi mà thư trả lời sẽ được gửi đến.
- **Ngày Phát (Delivery Date)** Đây là dấu thời gian khi một phần mềm email nhận được email.
- **Đã nhận (Received)** Dòng này hiển thị các máy chủ mà một email đã đi qua để đến được hộp thư của người nhận. Để đọc nó theo thứ tự thời gian, bạn phải bắt đầu từ cuối (nơi gửi email ban đầu) và đọc lên đến đỉnh (đích cuối cùng của email).
- **DKIM Signature và Domain Key Signature** DKIM là viết tắt của DomainKeys Identified Mail. Cùng với chữ ký khóa miền (domain key signature), nó là một phần của hệ thống nhận dạng chữ ký email.
- **Mã-nhận-diện-Thông-điệp (Message-ID)** Đây là sự kết hợp của các chữ cái và số duy nhất được tạo ra khi email được viết lần đầu (cũng có thể giả mạo được).
- **Phiên-bản-MIME (MIME-version)** MIME là một tiêu chuẩn Internet mở rộng định dạng và chức năng của email. Bạn có thể đính kèm video, hình ảnh và các tập tin khác bằng MIME. Tập tin đính kèm có trong Base64.

- **Kiểu-nội-dung (Content-type)** Cho bạn biết liệu email được viết dưới dạng văn bản rõ ràng (plaintext) hay HTML.
- **Trạng thái X-Spam (X-Spam status)** Cho bạn biết điểm số của một email. Nếu nó vượt quá ngưỡng, email sẽ bị coi là thư rác.
- **Cấp độ X-Spam (X-Spam level)** Cấp độ này phụ thuộc vào điểm số của trạng thái XSpam của email. Đối với mỗi điểm mà nó đạt được, cấp độ X-Spam sẽ hiển thị một dấu hoa thị.
- **Nội dung thông điệp (Message body)** Thông điệp thực tế đã được gửi đi.

Như bạn có thể thấy, một e-mail có thể chủ yếu bao gồm siêu dữ liệu.

## Di động

Các thiết bị di động tạo ra, lưu trữ và truyền tải siêu dữ liệu. Các trường phổ biến bao gồm thời điểm khi một cuộc gọi hoặc tin nhắn được thực hiện, cho dù đó là cuộc gọi đến hay đi, thời lượng cuộc gọi hoặc độ dài của tin nhắn văn bản (được tính bằng ký tự) và số điện thoại của người gửi và người nhận. Hãy lưu ý rằng tin nhắn hoặc tín hiệu âm thanh không phải là một phần của siêu dữ liệu, nhưng bạn có thể nhận được lượng thông tin là bao nhiêu chỉ từ siêu dữ liệu? Nhiều hơn những gì bạn trông thấy. Ví dụ: các số có thể được tra cứu, cung cấp danh tính của người gửi và người nhận (chẳng hạn như một cuộc trò chuyện với văn phòng bác sĩ, tiếp theo sau đó là cuộc gọi từ hiệu thuốc).

Các nguồn siêu dữ liệu khác bao gồm những thứ như điểm truy cập Wi-Fi được kết nối tới, dữ liệu GPS trong các nhật ký ứng dụng, bất kể thiết bị có camera hay không và dữ liệu EXIF (sẽ được thảo luận sau trong phần "Tập tin").

## Web

Web cung cấp một phương tiện di chuyển thông tin giữa các trình duyệt và máy chủ. Có rất nhiều loại giao thức liên quan và nhiều nguồn siêu dữ

liệu khác nhau. Bản thân các trang web chứa đầy siêu dữ liệu và các trình duyệt lưu trữ những siêu dữ liệu khác nhau bao gồm những trang nào đã được truy cập và vào khi nào. Siêu dữ liệu trình duyệt là nguồn thông tin điều tra pháp y được sử dụng một cách thường xuyên, vì các mục nhập về nội dung và thời điểm trình duyệt đã truy cập dữ liệu có thể sẽ rất quan trọng. Có phải người dùng đã truy cập vào một trang web cụ thể? Họ có sử dụng ứng dụng email dựa-trên-web, tiết lộ thông tin email thực tế cũng như thực tế là họ đã sử dụng email không? Họ đã ở trên một trang web trong thời gian bao lâu? Nếu người dùng truy cập vào một trang web hiển thị hình ảnh đã được gắn thẻ bởi một trong các thiết bị bảo mật, họ ở lại trang đó hay ngay lập tức truy cập vào một trang khác? Có thể có vô số thông tin về hành vi của người dùng liên quan đến việc duyệt web.

## Tập tin

Siêu dữ liệu tập tin có hai loại: hệ thống và ứng dụng. Hệ thống tập tin sử dụng siêu dữ liệu để theo dõi tên tập tin cũng như dấu thời gian liên quan đến lần truy cập cuối cùng, tạo và ghi lần cuối. Siêu dữ liệu hệ thống sẽ bao gồm các mục mà Hệ điều hành cần, chẳng hạn như thông tin về quyền sở hữu, đối tượng mẹ, quyền và các mô tả bảo mật.

Siêu dữ liệu ứng dụng trong tập tin là một phần của trường dữ liệu tập tin và được sử dụng bởi ứng dụng. Ví dụ: một tài liệu Microsoft Word chứa rất nhiều siêu dữ liệu, bao gồm các trường về tác giả, công ty, số lần được chỉnh sửa, thời gian in gần đây nhất, v.v... Hiện tại, Word đã có hơn 90 trường siêu dữ liệu có thể được sử dụng/điều chỉnh bởi người dùng. Mặt khác, một tập tin JPEG có siêu dữ liệu thường được thể hiện dưới dạng dữ liệu EXIF. Định dạng tập tin hình ảnh có thể trao đổi (exchangeable image file - EXIF) là một tiêu chuẩn xác định các định dạng của các thẻ hình ảnh, âm thanh và siêu dữ liệu được sử dụng bởi

các máy ảnh, điện thoại và các thiết bị ghi kỹ thuật số khác. Siêu dữ liệu EXIF phổ biến có thể bao gồm những điều dưới đây:

- Tên tập tin gốc,
- Ngày và dấu thời gian chụp và chỉnh sửa cuối cùng (với độ chính xác khác nhau),
- Tọa độ vị trí GPS (độ vĩ độ và kinh độ),
- Một hình ảnh thu nhỏ kích thước nhỏ của hình ảnh gốc,
- Tên tác giả và chi tiết bản quyền,
- Tiêu đề la bàn,
- Thông tin thiết bị, bao gồm nhà sản xuất và kiểu máy,
- Thông tin chụp, bao gồm loại ống kính, dài tiêu cự, khẩu độ, tốc độ cửa trập và cài đặt đèn flash.

Dữ liệu EXIF tồn tại để hỗ trợ các ứng dụng sử dụng những tập tin này và có thể được sửa đổi một cách độc lập với nội dung tập tin.



**MÁCH NƯỚC CHO KỲ THI** Siêu dữ liệu là một nguồn thông tin cực kỳ có giá trị trong một cuộc điều tra. Việc hiểu được kiểu thông tin và các chi tiết được trình bày trong từng thể loại chính là điều quan trọng.

### **NetFlow/sFlow**

*NetFlow* và *sFlow* là các giao thức được thiết kế để nắm bắt thông tin về các luồng gói tin (nghĩa là, một chuỗi các gói tin có liên quan) khi chúng đi qua một mạng. *NetFlow* là một tiêu chuẩn độc quyền của Cisco. Dữ liệu luồng được tạo ra bởi chính các thiết bị mạng, bao gồm cả bộ định tuyến và bộ chuyển mạch. Dữ liệu được thu thập và chuyển đến bộ thu thập dữ liệu là một tập hợp siêu dữ liệu đơn giản - địa chỉ IP nguồn và đích, cổng nguồn và cổng đích, nếu có (ví dụ, ICMP không sử dụng cổng)

và giao thức. NetFlow thực hiện điều này cho tất cả các gói tin, trong khi sFlow (luồng được lấy mẫu) thực hiện việc lấy mẫu thống kê. Trên các mạng có thông-lượng-cao, NetFlow có thể tạo ra một lượng lớn dữ liệu - dữ liệu yêu cầu khử-trùng-lặp (de-duplication). Tuy nhiên, việc có được tất cả dữ liệu đó sẽ bắt được các gói sự kiện bảo mật hiếm hoi. sFlow phù hợp hơn để giám sát lưu lượng mang tính thống kê. Cisco đã bổ sung thêm tính năng giám sát thống kê cho NetFlow trên các bộ định tuyến cơ sở hạ tầng công-nghệ-cao của mình để xử lý lưu lượng truy cập.

---



## MÁCH NƯỚC CHO KỲ THI

Cả NetFlow và sFlow đều thu thập các gói tin từ các bộ định tuyến và bộ chuyển mạch. Dữ liệu NetFlow có thể rất hữu ích trong các cuộc điều tra xâm nhập. sFlow chủ yếu được sử dụng để quản lý lưu lượng, mặc dù nó sẽ giúp chống lại các cuộc tấn công DDoS.

## IPFIX

*Xuất Thông tin Luồng Giao thức Internet (Internet Protocol Flow Information Export - IPFIX)* là một giao thức IETF là câu trả lời cho tiêu chuẩn độc quyền NetFlow của Cisco. IPFIX dựa trên NetFlow phiên bản 9 và có thể cấu hình cao bằng cách sử dụng một loạt các biểu mẫu. Mục đích chính của IPFIX là cung cấp thông tin về trạng thái của mạng cho một trạm giám sát trung tâm. IPFIX là một giao thức dựa-trên-đẩy, trong đó người gửi gửi báo cáo đi và không nhận được phản hồi từ người nhận.

## Kết quả đầu ra từ Bộ phân tích Giao thức

Một bộ phân tích giao thức (còn được gọi là một *bộ dò gói tin (packet sniffer)*, *bộ phân tích mạng (network analyzer)* hoặc *bộ dò tìm mạng (network sniffer)*) là một phần của phần mềm hoặc một hệ thống phần mềm/phần cứng được tích hợp có thể nắm bắt và giải mã lưu lượng mạng.

Bộ phân tích giao thức đã rất phổ biến với các quản trị viên hệ thống và các chuyên gia bảo mật trong nhiều thập kỷ vì chúng là những công cụ linh hoạt và hữu ích cho môi trường mạng. Từ góc độ bảo mật, bộ phân tích giao thức có thể được sử dụng cho một số các hoạt động, chẳng hạn như:

- Phát hiện xâm nhập hoặc lưu lượng không mong muốn. (Một IDS/IPS phải có một số loại khả năng nắm bắt và giải mã để có thể tìm kiếm lưu lượng đáng ngờ/độc hại).
- Nắm bắt lưu lượng trong quá trình ứng phó sự cố hoặc xử lý sự cố.
- Tìm kiếm bằng chứng về các botnet, Trojan và các hệ thống đã bị lây nhiễm.
- Tìm kiếm lưu lượng truy cập bất thường hoặc lưu lượng vượt quá ngưỡng nhất định.
- Kiểm tra mã hóa giữa các hệ thống hoặc ứng dụng.

Từ góc độ quản trị mạng, bộ phân tích giao thức có thể được sử dụng cho các hoạt động chăng hạn như:

- Phân tích các vấn đề về mạng,
- Phát hiện các ứng dụng được định cấu hình sai hoặc các ứng dụng hoạt động sai,
- Thu thập và báo cáo việc sử dụng mạng và thống kê lưu lượng,
- Gỡ lỗi giao tiếp máy khách / máy chủ

Bất kể mục đích sử dụng là gì, một bộ phân tích giao thức phải có khả năng xem xét lưu lượng mạng để nắm bắt và giải mã nó. Kết quả đầu ra của bộ phân tích giao thức là một định dạng mà con-người-có-thể-đọc-được của thông tin đang được chuyển vào hệ thống. Thông tin này có thể cung cấp thông tin chi tiết một cách chính xác về những gì đang xảy ra hoặc không xảy ra. Các công cụ có thể được sử dụng để quét kết quả đầu



ra cho các hạng mục cụ thể được quan tâm, các hình mẫu, hoạt động cụ thể và các thành phần giao tiếp khác có thể được quan tâm.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các yếu tố bảo mật liên quan đến các cuộc điều tra. Chương này được mở đầu bằng một phần về kết quả quét lỗ hổng bảo mật, tiếp theo là một phần về bảng thông tin tổng quan SIEM. Trong phần thứ hai, các chủ đề phụ về cảm biến, độ nhạy, xu hướng, cảnh báo và mối tương quan đã được đề cập. Phần tiếp theo đã đề cập đến các tập tin nhật ký và các chủ đề về mạng, hệ thống, ứng dụng, bảo mật, Web, DNS và xác thực đã được trình bày. Tiếp theo là các tập tin kết xuất, VoIP và trình quản lý cuộc gọi, và nhật ký lưu lượng SIP.

Tiếp theo, các chủ đề về syslog/rsyslog/syslog-ng, journalctl, NXLog, lưu giữ và giám sát băng thông cũng đã được trình bày. Phần chính tiếp theo là về siêu dữ liệu, mô tả các dạng siêu dữ liệu của email, di động, web và tập tin.

Chương này đã kết thúc với một phần về NetFlow/sFlow, nơi IPFIX được trình bày, và sau đó là một xem xét về các kết quả đầu ra của bộ phân tích giao thức.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

- 1.** Nhật ký có giá trị nhất để tìm kiếm phần mềm độc hại trong một hệ thống là gì?
  - A.** Mạng.
  - B.** Web.
  - C.** DNS.
  - D.** IPFIX.
- 2.** Để hiểu rõ nhất những máy nào đang nói chuyện với nhau, cách nào sau đây nên được sử dụng?
  - A.** Nhật ký DNS
  - B.** NetFlow
  - C.** Nhật ký mạng
  - D.** Cảnh báo SIEM.
- 3.** Để ghi nhật ký từ xa bằng một máy chủ nhật ký tập trung, giao thức nào sau đây nên được sử dụng?
  - A.** DNS
  - B.** NetFlow
  - C.** Syslog
  - D.** IPFIX.
- 4.** IPFIX được sử dụng cho mục đích gì?
  - A.** Chụp lại những máy nào đang giao tiếp với nhau
  - B.** Quản lý các giải pháp nhẫn tin di động
  - C.** Đọc tập tin nhật ký hệ thống
  - D.** Nhật ký DNS.

5. Bạn có thể tìm siêu dữ liệu cho thấy nơi một hình ảnh đã được chụp ở đâu?
  - A. Dữ liệu EXIF
  - B. Dữ liệu IPFIX
  - C. Siêu dữ liệu email
  - D. SIP CTL
6. Điều gì trong số này không được liên kết với tập tin nhật ký hệ thống?
  - A. Journalctl
  - B. NXLog
  - C. SIP CTL
  - D. IPFIX.
7. Tương quan làm gì với dữ liệu SIEM?
  - A. Xác định nguyên nhân
  - B. Cung cấp thông tin bối cảnh nền
  - C. Cho phép diễn giải dữ liệu dựa-trên-quy-tắc
  - D. Tất cả những điều trên.
8. Một trong những thách thức của dữ liệu NetFlow là gì?
  - A. Định dạng độc quyền
  - B. Các trường dữ liệu dư thừa
  - C. Ghi kích thước
  - D. Loại bỏ các bản ghi trùng lặp dọc theo một đường dẫn.
9. Công cụ nào có thể được sử dụng để đọc dữ liệu nhật ký hệ thống trong các hệ thống Linux?
  - A. Bất kỳ trình soạn thảo văn bản nào
  - B. Journalctl
  - C. Trình duyệt web
  - D. Máy phân tích giao thức.

**10.** Nội dung nào dưới đây là các vấn đề cần được xác định trong quá trình thiết lập giải pháp SIEM? (Chọn tất cả các đáp án đúng).

- A.** Vị trí của cảm biến
- B.** Tập tin nhật ký và các trường liên quan
- C.** Các điều kiện cảnh báo mong muốn
- D.** Ghi nhật ký DNS.

## Đáp án

1. **C.** Nhật ký DNS có thể nhìn thấy các yêu cầu giao tiếp với máy chủ điều-khiển-và-kiểm-soát phần mềm độc hại (C2).
2. **B.** Dữ liệu NetFlow mô tả máy nào đang nói chuyện với máy nào.
3. **C.** Syslog là giao thức được sử dụng để di chuyển các tập tin nhật ký đến các máy chủ từ xa.
4. **A.** IPFIX hoạt động giống như NetFlow, xác định những máy nào đang giao tiếp với nhau.
5. **A.** EXIF là siêu dữ liệu được liên kết với các tập tin hình ảnh và video.
6. **D.** IPFIX không được liên kết với các tập tin nhật ký hệ thống.
7. **C.** Sự tương quan cho phép các sự kiện khác nhau được kết hợp để cung cấp mức độ đặc trưng cao hơn trong việc xác định phát hiện sự kiện dựa-trên-SIEM. Tương quan là một phương tiện để hệ thống SIEM áp dụng các quy tắc kết hợp các nguồn dữ liệu để tinh-chỉnh việc phát hiện sự kiện.
8. **D.** Mặc dù NetFlow là một tiêu chuẩn độc quyền, nhưng định dạng của nó đã được công bố. Nó có kích thước bản ghi nhỏ và dữ liệu có thể được lặp lại từ nhiều thiết bị đọc theo đường dẫn của gói tin. Việc oại bỏ các bản sao (bản ghi) trong hệ thống phân tán có thể là một thách thức.
9. **B.** Journalctl có thể đọc nhật ký hệ thống trên hệ thống Linux.
10. **A, B, C và D.** Việc thiết lập một SIEM yêu cầu nhiều bước, bao gồm xác định nguồn dữ liệu, điều kiện cảnh báo, nhật ký và trường sẽ sử dụng, v.v...

## Chương 29 Các Kỹ thuật và Biện pháp Giảm nhẹ

---

### Các Kỹ thuật và Biện pháp Kiểm soát Giảm nhẹ

Trong chương này bạn sẽ

- Tìm hiểu về những biện pháp giảm nhẹ khác nhau có thể được áp dụng cho các hệ thống,
  - Tìm hiểu về các biện pháp kiểm soát khác nhau có thể được sử dụng để bảo vệ các hệ thống.
- 

Các hệ thống không thể được bảo mật một cách hoàn toàn theo thiết kế hoặc theo sử dụng, nhưng tuy nhiên, một loạt các yếu tố có thể được sử dụng để gia tăng vị thế bảo mật của hệ thống. Các biện pháp kiểm soát và giảm nhẹ này có tác dụng làm giảm thiểu rủi ro trong hệ thống. Chương này sẽ khám phá các biện pháp kiểm soát và giảm nhẹ khác nhau được đề cập trong bài kiểm tra Security+.

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 4.4 của kỳ thi CompTIA Security+: Khi xảy ra sự cố, hãy áp dụng các biện pháp hoặc kỹ thuật giảm nhẹ để bảo vệ môi trường.

## Tái lập cấu hình Các giải pháp Bảo mật Đầu cuối

Các *giải pháp bảo mật điểm đầu cuối* là những biện pháp kiểm soát có thể giảm thiểu rủi ro tại điểm đầu cuối. Các giải pháp điểm đầu cuối phải nhận thức được mối đe dọa và sau đó kích hoạt một hành động cụ thể để giảm thiểu rủi ro. Các giải pháp chống vi-rút/phần mềm chống phần mềm độc hại là biện pháp bảo vệ điểm đầu cuối điển hình mà hầu hết người dùng đều nghĩ đến, cũng như các thành phần như tường lửa và các phần tử bảo vệ chống xâm nhập.

Các phần tử điểm đầu cuối được tích hợp hơn có thể là một phần của hệ điều hành, hoặc chúng có thể làm việc với hệ điều hành (OS) để thay đổi hành vi nhằm thực thi các quy tắc. Microsoft có hai cơ chế là một phần Hệ điều hành Windows để quản lý những ứng dụng nào có thể hoạt động trên máy của họ:

- **Chính sách hạn chế phần mềm** Được sử dụng thông qua chính sách nhóm, các chính sách hạn chế phần mềm cho phép kiểm soát đáng kể các ứng dụng, tập lệnh kịch bản và tập tin thực thi. Chế độ chính là theo máy chứ không phải theo tài khoản người dùng.
- **Kiểm soát cấp độ tài khoản người dùng** Được thực thi thông qua AppLocker, một dịch vụ cho phép kiểm soát chi tiết việc người dùng có thể thực thi chương trình nào. Thông qua việc sử dụng các quy tắc, doanh nghiệp có thể kiểm soát đáng kể việc ai có thể truy cập và sử dụng phần mềm đã cài đặt.

Trên nền tảng Linux, những khả năng tương tự được cung cấp từ các ứng dụng của nhà cung cấp bên-thứ-ba.

Câu hỏi cuối cùng là, bạn sẽ làm gì khi phát hiện ra thứ gì đó nằm ngoài những đặc tả thông số kỹ thuật mong muốn? Phản ứng điển hình là cách ly, sẽ được mô tả sau cũng trong chương này.

## Danh sách Ứng dụng được Phê duyệt

Các ứng dụng có thể được kiểm soát tại Hệ điều hành tại thời điểm bắt đầu thông qua việc xác minh ứng dụng dựa trên danh sách các ứng dụng đã được phê duyệt (danh sách trắng) và danh sách các ứng dụng bị chặn hoặc bị từ chối (danh sách đen). *Danh sách ứng dụng đã được phê duyệt* bao gồm một danh sách các ứng dụng được chấp thuận. Nếu một ứng dụng không có trong danh sách được phép, nó sẽ bị chặn. Cả danh sách trắng và danh sách đen đều có những ưu điểm và nhược điểm. Việc sử dụng một danh sách ứng dụng được phê duyệt sẽ dễ sử dụng hơn nếu xét từ khía cạnh xác định các ứng dụng được phép chạy và các giá trị băm có thể được sử dụng để đảm bảo các tập tin thực thi đã không bị hư hỏng. Thách thức trong cách tiếp cận này là số lượng ứng dụng tiềm năng được chạy trên một máy điển hình. Đối với một máy chỉ có một mục đích duy nhất, chẳng hạn như một máy chủ cơ sở dữ liệu, điều này có thể tương đối dễ sử dụng. Đối với các máy đa năng, nó có thể phức tạp hơn, vì các ứng dụng có thể bị bỏ sót, dẫn đến lỗi.

## Danh sách Ứng dụng bị Khóa/Danh sách Từ chối

Việc sử dụng một *danh sách ứng dụng bị chặn* hoặc *từ chối* về cơ bản là việc lưu ý những ứng dụng nào không được phép chạy trên máy. Về cơ bản, đây là loại khả năng “bỏ qua” hoặc “chặn cuộc gọi” vĩnh viễn. Theo lịch sử, điều này còn được gọi là danh sách đen, rất khó, nếu không muốn nói là không thể, sử dụng để chống lại các mối đe dọa động vì việc xác định một ứng dụng cụ thể có thể dễ dàng tránh được thông qua những thay đổi nhỏ.



## MÁCH NƯỚC CHO KỲ THI

Danh sách trắng, hoặc việc sử dụng danh sách ứng dụng được phép, là việc sử dụng danh sách các ứng dụng đã được phê duyệt. Nếu một ứng dụng không có trong danh sách trắng,

**CompTIA Security+ - All in One - Exam Guide**

1011 | Page

quyền truy cập sẽ bị từ chối và ứng dụng đó sẽ không được cài đặt hoặc chạy. Danh sách đen, hoặc sử dụng danh sách chặn/từ chối ứng dụng, là danh sách các ứng dụng được coi là không mong muốn. Nếu một ứng dụng nằm trong danh sách đen, ứng dụng đó sẽ không được cài đặt hoặc không được phép chạy.

## Cách ly

Khi một hệ thống phát hiện được một điều kiện đáp ứng một bộ quy tắc cụ thể và xác định rằng một hành động là bắt buộc thì một trong những quyết định quan trọng là hành động sau cùng của hành động đó. Trong trường hợp có tường lửa, việc chặn kết nối là điều cuối cùng, kết quả không thể được hoàn tác. Nhưng trong trường hợp một tập tin đáng ngờ, thay đổi tập tin hoặc thay đổi cấu hình, sẽ có khả năng xảy ra sai sót trong quyết định và có thể mong muốn có được khả năng “hoàn tác” ảo. Đây là nơi mà khái niệm *cách ly* đi vào phương trình. Cách ly một đề mục là khiến cho nó bị vô hiệu hóa nhưng không bị xóa vĩnh viễn khỏi hệ thống. Có nhiều cơ chế khác nhau để thực hiện việc này, nhưng kết quả cuối cùng là giống nhau: tùy chọn cách ly cho người dùng cơ hội hoàn tác việc vô hiệu hóa. Nếu đề mục đã bị xóa vĩnh viễn, tùy chọn này sẽ không khả dụng. Các công cụ bảo mật cung cấp các tùy chọn cách ly có cơ chế vô hiệu hóa một đề mục và kích hoạt lại đề mục đó nếu được chỉ thị bởi người dùng.

## Những thay đổi Cấu hình

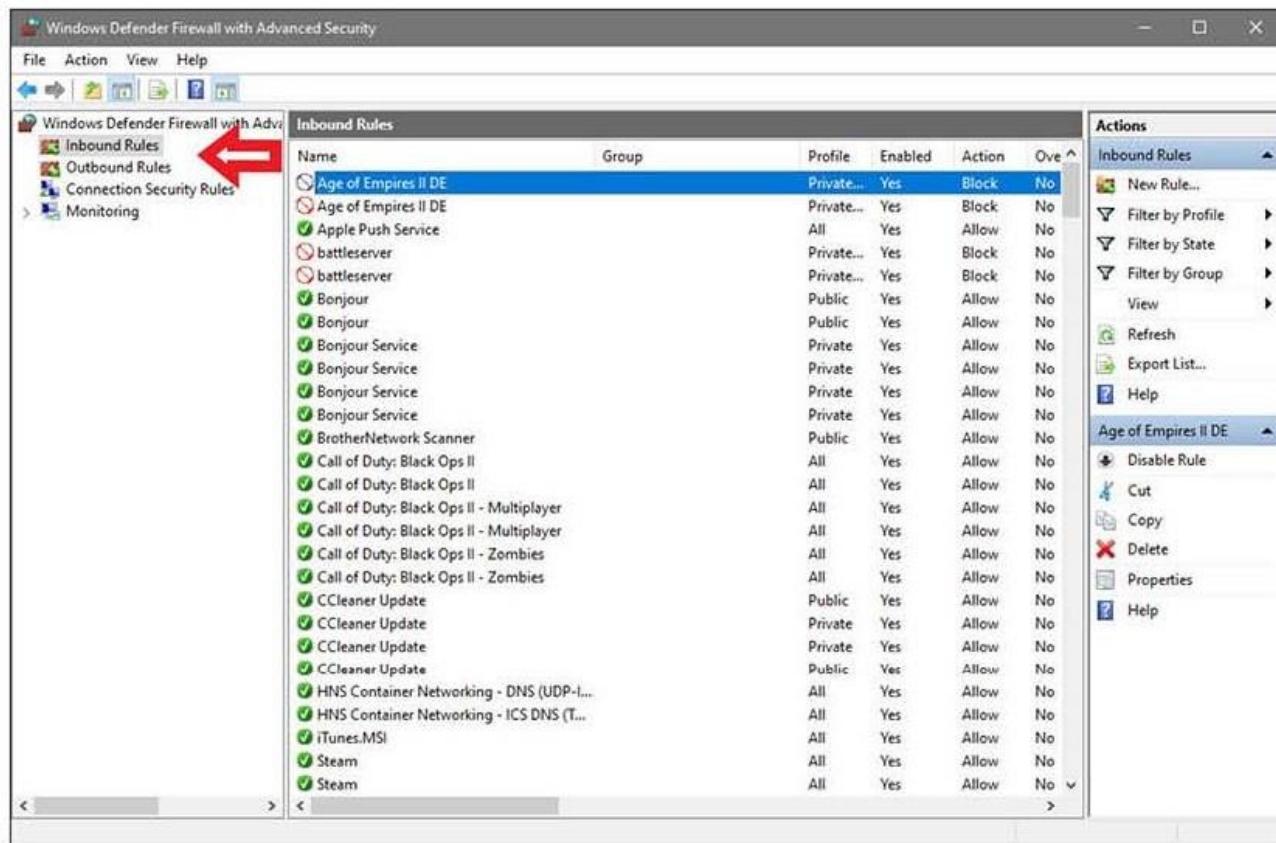
Các cấu hình là mạch máu của một hệ thống. Việc bảo vệ hệ thống khỏi *những thay đổi cấu hình* là điều cần thiết để bảo vệ hệ thống trong cấu hình cụ thể mà việc triển khai đã dự định. Việc thay đổi cấu hình có thể thêm chức năng, xóa chức năng, thậm chí thay đổi hoàn toàn chức năng của hệ thống bằng cách thay đổi các phần tử của chương trình để bao

gồm mã (phần mềm) bên ngoài. Việc bảo vệ hệ thống khỏi những thay đổi cấu hình trái phép là điều quan trọng đối với bảo mật.

### Các Quy tắc Tường lửa

Tường lửa hoạt động bằng cách thực thi một bộ quy tắc đối với lưu lượng đang cố gắng vượt qua nó. Bộ *quy tắc tường lửa* này, còn được gọi là bộ quy tắc tường lửa (firewall ruleset), là bản sao của những ràng buộc chính sách tại một điểm cụ thể trong mạng. Do đó, bộ quy tắc sẽ khác nhau giữa các tường lửa, bởi vì nó (bộ quy tắc tường lửa) là việc triển khai hoạt động của các ràng buộc lưu lượng mong muốn tại từng điểm. Các quy tắc tường lửa nêu rõ liệu tường lửa có cho phép lưu lượng truy cập cụ thể đi qua hay chặn nó (lưu lượng) lại. Cấu trúc của quy tắc tường lửa có thể từ đơn giản đến rất phức tạp, tùy thuộc vào loại tường lửa và kiểu lưu lượng truy cập. Một tường lửa lọc gói có thể hoạt động trên các địa chỉ IP và cổng, cho phép hoặc chặn lưu lượng dựa trên thông tin này.

Các quy tắc tường lửa có tính định hướng, có các quy tắc gửi đến và gửi đi. Các quy tắc gửi đến bảo vệ máy khỏi lưu lượng đến (inbound). Các quy tắc gửi đi (outbound) cũng có thể bảo vệ chống lại việc gửi dữ liệu (bao gồm cả các yêu cầu) đến những nơi trái phép hoặc nguy hiểm. Ví dụ về các quy tắc này và các hạng mục gửi đến và gửi đi được minh họa trong Hình 29-1.



**Hình 29-1** Các quy tắc tường lửa trong Microsoft Defender, một giải pháp máy khách của Windows



**MÁCH NƯỚC CHO KỲ THI** Các quy tắc tường lửa đặt ra những câu hỏi tuyệt vời dựa-trên-hiệu-suất - những quy tắc nào thuộc về tường lửa nào? Việc hiểu được cách một quy tắc ngăn chặn hoặc cho phép lưu lượng là điều cần thiết, nhưng cũng cần xem xét bức tranh tổng thể của luồng lưu lượng mạng được quy định như thế nào bởi các quy tắc. Hãy có khả năng đưa các quy tắc vào sơ đồ mạng để đáp ứng được các mục tiêu.

## MDM

Kiến thức về khái niệm *quản lý thiết bị di động* (*mobile device management* - MDM) là điều thiết yếu trong môi trường các thiết bị được

CompTIA Security+ - All in One - Exam Guide

1014 | Page

kết nối ngày nay. MDM bắt đầu như một thuật ngữ tiếp thị về một tập hợp các yếu tố bảo vệ thường được sử dụng liên quan đến thiết bị di động. Khi được coi là một tập hợp các tùy chọn bảo mật toàn diện dành cho thiết bị di động, mọi công ty nên có và thực thi chính sách MDM. Chính sách phải yêu cầu những điều sau:

- Khóa thiết bị bằng một mật khẩu mạnh mẽ,
- Mã hóa dữ liệu trên thiết bị,
- Tự động khóa thiết bị sau một khoảng thời gian không hoạt động nhất định,
- Khả năng khóa thiết bị từ xa nếu nó bị mất hoặc bị đánh cắp,
- Khả năng tự động xóa thiết bị sau một số lần đăng nhập thất bại nhất định,
- Khả năng xóa thiết bị từ xa nếu thiết bị bị mất hoặc bị đánh cắp.

Các chính sách mật khẩu nên mở rộng cho các thiết bị di động, bao gồm cả việc khóa (lockout) và, nếu có thể, tự động xóa dữ liệu. Chính sách của công ty về mã hóa dữ liệu trên thiết bị di động cũng nên quan trọng với chính sách mã hóa dữ liệu trên máy tính xách tay. Nói cách khác, nếu bạn không yêu cầu mã hóa máy tính xách tay thì bạn có nên yêu cầu mã hóa cho thiết bị di động không? Không có câu trả lời thống nhất cho câu hỏi này vì trên thực tế, thiết bị di động sẽ di động nhiều hơn so với máy tính xách tay và dễ bị thất lạc hơn. Và đây là một câu hỏi tối hậu về rủi ro mà cấp quản lý phải giải quyết: rủi ro là gì và chi phí của các phương án được sử dụng là gì? Điều này cũng đặt ra một câu hỏi lớn hơn: thiết bị nào nên có mã hóa như một cơ chế bảo vệ an ninh cơ bản? Đó là theo loại thiết bị hay theo người dùng dựa trên việc dữ liệu nào sẽ có rủi ro? May mắn thay, các giải pháp MDM tồn tại, khiến cho các lựa chọn trở nên có thể quản lý được.



**MÁCH NƯỚC CHO KỲ THI** Quản lý thiết bị di động (MDM) là một thuật ngữ dành cho một tập hợp các phần tử bảo vệ được sử dụng một cách phổ biến có liên quan đến các thiết bị di động.

### DLP

*Ngăn ngừa mất mát dữ liệu (data loss prevention - DLP)* đề cập đến công nghệ được sử dụng để phát hiện và ngăn chặn việc truyền tải dữ liệu trong một doanh nghiệp. Được sử dụng tại những địa điểm quan trọng, công nghệ DLP có thể quét các gói tin để tìm kiếm các hình mẫu dữ liệu cụ thể. Công nghệ này có thể được điều chỉnh để phát hiện số tài khoản, các bí mật, điểm đánh dấu cụ thể hoặc các tập tin. Khi các phần tử dữ liệu cụ thể được phát hiện, hệ thống có thể chặn việc truyền tải dữ liệu lại. Thách thức chính trong việc sử dụng công nghệ DLP chính là vị trí của cảm biến. Cảm biến DLP cần có khả năng quan sát dữ liệu, vì vậy nếu kênh (truyền tải) đã được mã hóa, công nghệ DLP có thể bị cản trở.

DLP bắt đầu ra đời với tư cách là một thiết bị cấp-doanh-nghiệp, nhưng việc triển khai công nghệ này đã dần mở rộng đến các thiết bị đầu cuối, bao gồm cả hệ điều hành và các ứng dụng như Microsoft 365. Các giải pháp phân phối này sử dụng các chính sách DLP để phát hiện, giám sát và bảo vệ chống lại việc phát hành ngẫu nhiên hoặc tiết lộ những thông tin nhạy cảm.



**MÁCH NƯỚC CHO KỲ THI** DLP có thể được phân loại là các biện pháp kiểm soát kỹ thuật. Mục tiêu chính của nó là để phát hiện các vi phạm và ngăn chặn mất mát dữ liệu.

## Lọc Nội dung/Lọc URL

*Bộ lọc nội dung/bộ lọc URL* được sử dụng để giới hạn các kiểu nội dung cụ thể trên Web cho người dùng. Một ách sử dụng khá phổ biến là chặn các trang web không liên quan đến công việc và để hạn chế các mục như tìm kiếm trên Google và các phương pháp truy cập nội dung khác đã được xác định là không phù hợp. Cũng giống như tất cả các thiết bị thực thi chính sách khác, bộ lọc nội dung dựa trên một bộ các quy tắc và việc duy trì quy tắc là một vấn đề. Một trong những vấn đề phổ biến nhất với bộ lọc nội dung là phạm vi chặn quá rộng. Trong môi trường y tế, việc chặn từ "breast" sẽ không hoạt động, và cũng sẽ không hoạt động trong một nhà máy chế biến thịt gà. Cần phải có một cơ chế để chấm dứt việc chặn một cách dễ dàng và nhanh chóng nếu người dùng phản đối và dễ dàng xác định rằng họ nên có quyền truy cập.

## Cập nhật hoặc Thu hồi các Chứng nhận

Các chứng nhận được sử dụng để chuyển các khóa mật mã như một phần của rất nhiều quy trình - từ ký dữ liệu đến các dịch vụ xác thực, đến thiết lập các dịch vụ mật mã giữa các thiết bị. Hầu hết công việc với các chứng nhận đều được tự động hóa và xử lý ở hậu trường, nhưng nó vẫn phụ thuộc vào một bộ chứng chỉ hợp lệ và chuỗi chứng chỉ đã được phê duyệt. Để biết chi tiết về cách thức hoạt động, hãy đọc Chương 25, "Cơ sở hạ tầng Khóa Công khai". Một yếu tố cực kỳ quan trọng của chứng nhận là việc bảo vệ chuỗi chứng nhận trên máy. Các lỗi trong phần tử này có thể khiến cho chứng nhận bị từ chối. Việc không duy trì được các chứng nhận hợp lệ là một nguyên nhân khác gây ra lỗi. Nhiều lỗi trong số này có thể đã không được chú ý, như đã được chứng minh trong việc đếm số ca nhiễm COVID-19 được tự động hóa ở bang California. Một lỗi chứng nhận với một trong những nhà cung cấp phòng thí nghiệm của tiểu bang đã dẫn đến việc kết quả bị thiếu sót đáng kể và nguyên nhân là do chứng nhận đã hết hạn.



**MÁCH NƯỚC CHO KỲ THI** Các chứng nhận sẽ hợp lệ trong một khoảng thời gian cụ thể. Khi một chứng nhận gần hết hạn, nó nên được gia hạn nếu cần thiết. Tuy nhiên, đôi khi các chứng nhận bị thu hồi vì chủ sở hữu không còn đáng được tin cậy nữa, các khóa mã hóa đã bị xâm phạm, hoặc có những thay đổi hoặc lỗi khác với chứng nhận.

### Cách ly

*Cách ly* là việc sử dụng các giao thức mạng và kết nối kết quả để hạn chế quyền truy cập vào các phần khác nhau của mạng. Giới hạn này có thể là một phần hoặc có thể là toàn bộ, như được cung cấp bởi một khoảng trống không khí (air gap) và phương pháp phân tách này được sử dụng để thực thi các ranh giới tin cậy khác nhau. Thông tin chi tiết hơn về vai trò của mạng được trình bày trong phần “Phân đoạn”, ngay sau đây.

Cách ly cũng có thể được sử dụng như một phần của một chiến lược ứng phó sự cố, trong đó các hệ thống bị ảnh hưởng được cách ly khỏi phần còn lại của mạng. Điều này được thực hiện để hạn chế rủi ro gây ra bởi các hệ thống không còn hoạt động theo cách được mong muốn. Trong trường hợp lây nhiễm ransomware, đây là một yếu tố giảm thiểu then chốt nếu nó có thể được sử dụng sớm trong sự cố.

### Ngăn chặn

*Ngăn chặn* là một khái niệm then chốt trong ứng phó sự cố. *Ngăn chặn* là hành động thực hiện các hành động cụ thể nhằm hạn chế thiệt hại tiềm ẩn của sự cố, hạn chế thiệt hại và ngăn ngừa thiệt hại thêm nữa. Ngăn chặn có thể được thực hiện bằng nhiều cơ chế khác nhau, bao gồm phân đoạn mạng, cách ly các phần tử trái phép hoặc thay đổi cấu hình hệ thống. Mục tiêu đều giống nhau: hạn chế sự tiếp xúc của hệ thống với phần tử gây thiệt hại.

## Phân đoạn

Khi các mạng ngày càng trở nên phức tạp, với nhiều tầng lớp và kết nối với nhau, một vấn đề có thể phát sinh trong kết nối. Một trong những hạn chế của Giao thức Spanning Tree (STP) là không có khả năng quản lý lưu lượng lớp 2 một cách hiệu quả trên các mạng có độ phức tạp cao. STP được tạo ra để ngăn chặn các vòng lặp trong các mạng lớp 2 và đã được cải tiến trong phiên bản hiện tại của nó, được gọi là Rapid Spanning Tree Protocol (RSTP). RSTP tạo ra một cây bao trùm (spanning tree) trong mạng lưới bao gồm các thiết bị chuyển mạch lớp 2, vô hiệu hóa các liên kết không phải là một phần của cây bao trùm. RSTP, IEEE 802.1w, cung cấp sự hồi tụ nhanh hơn cho giải pháp cây bao trùm mới sau khi các thay đổi cấu trúc liên kết được phát hiện. Vấn đề với các thuật toán cây bao trùm là lưu lượng mạng bị gián đoạn trong khi hệ thống tính toán lại và thiết lập cấu hình lại. Những gián đoạn này có thể gây ra các vấn đề về hiệu quả mạng và dẫn đến việc thúc đẩy các thiết kế mạng phẳng, nhằm tránh các vấn đề lặp-gói-tin thông qua một kiến trúc không có các lớp (tier).

Một tên gọi liên quan đến cấu trúc liên kết mạng phẳng là *mạng kết cấu* (*network fabric*), một thuật ngữ dùng để mô tả một mạng phẳng và không có chiều sâu. Các loại mạng kết cấu ngày càng trở nên phổ biến trong các trung tâm dữ liệu và các khu vực khác có lưu-lượng-cao, vì chúng có thể cung cấp thông lượng tăng lên và mức độ chập chờn mạng và các gián đoạn khác thấp hơn. Mặc dù điều này khá tốt cho hiệu quả của các hoạt động mạng, nhưng ý tưởng “mọi người đều có thể nói chuyện với mọi người” này là một vấn đề liên quan đến bảo mật.

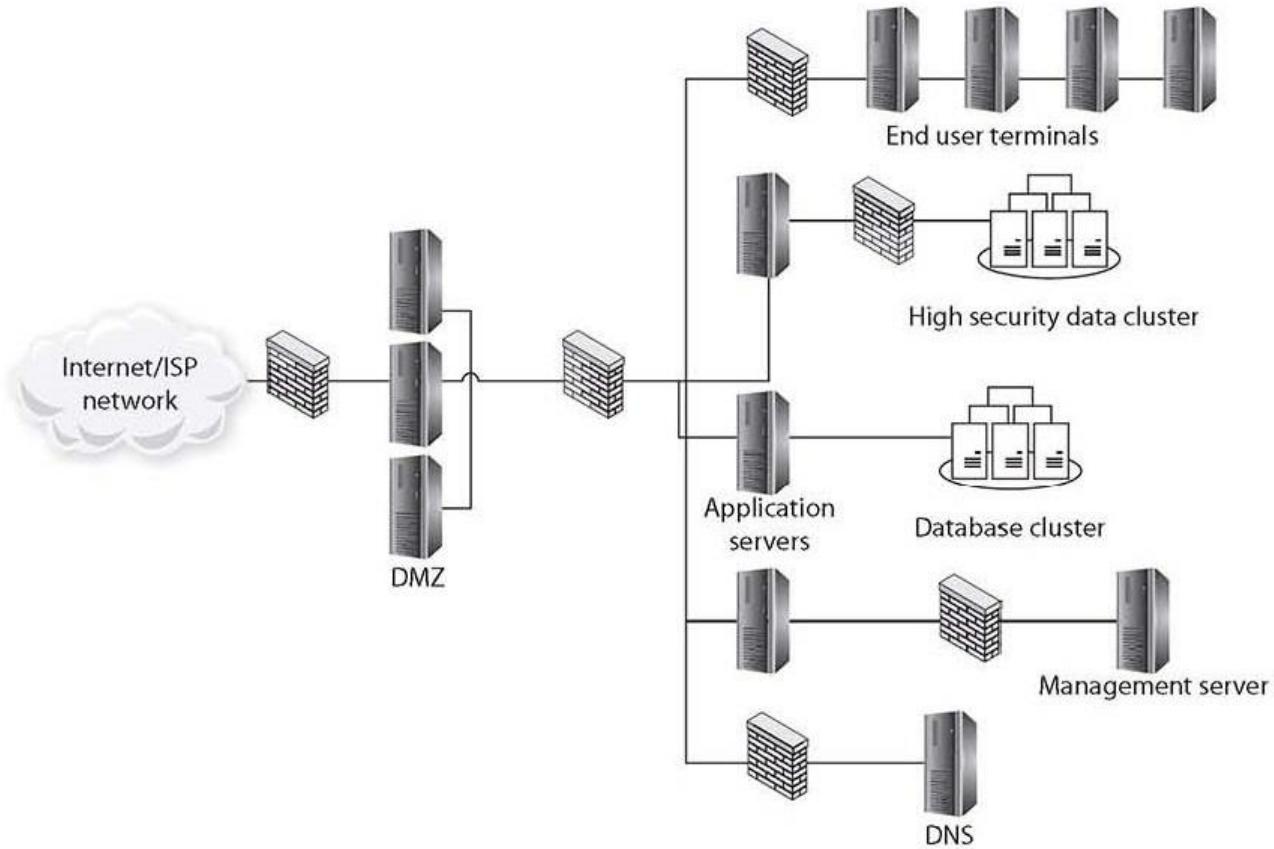
Các mạng hiện đại, với các kết nối ngày càng phức tạp của chúng, dẫn đến các hệ thống mà việc điều hướng có thể trở nên phức tạp giữa các nút. Cũng giống như kiến trúc dựa-trên-DMZ cho phép các mức độ tin cậy

khác nhau, việc cô lập các phần cụ thể của mạng bằng cách sử dụng các quy tắc bảo mật có thể cung cấp những môi trường tin cậy khác nhau. Có một số thuật ngữ được sử dụng để mô tả kiến trúc kết quả, bao gồm *phân đoạn (segmentation)* mạng, phân tách (segregation), cô lập (isolation) và vùng bao (enclave). Các vùng bao là thuật ngữ được sử dụng phổ biến nhất để mô tả các phần của mạng được cách ly về mặt logic bằng cách phân đoạn tại giao thức mạng. Khái niệm phân tách mạng thành các vùng bao có thể tạo ra những khu vực tin cậy nơi các biện pháp bảo vệ đặc biệt có thể được sử dụng và lưu lượng truy cập từ bên ngoài vùng bao bị hạn chế hoặc được sàng lọc một cách thích hợp trước khi nhập.

Các vùng bao không đối lập hoàn toàn với khái niệm cấu trúc mạng phẳng, chúng chỉ là những khu vực được chạm khắc, như các khu dân cư có kiểm soát, nơi người ta cần có thông tin xác thực đặc biệt để đi vào. Rất nhiều cơ chế bảo mật có thể được sử dụng để tạo ra một vùng bao bảo mật. Đánh địa chỉ lớp 2 (chia mạng con) có thể được sử dụng, khiến cho khả năng giải quyết trực tiếp trở thành một vấn đề. Các tường lửa, bộ định tuyến và proxy cấp ứng dụng có thể được sử dụng để sàng lọc các gói tin trước khi vào hoặc ra khỏi vùng bao. Ngay cả khía cạnh con người của hệ thống cũng có thể bị hạn chế bằng cách chỉ định một hoặc nhiều quản trị viên hệ thống để quản lý hệ thống.

Các vùng bao là một công cụ quan trọng trong thiết kế mạng an toàn hiện đại. Hình 29-2 minh họa cho một thiết kế mạng với việc triển khai hai-tường-lửa tiêu chuẩn của một DMZ. Ở phía bên trong của mạng, có thể nhìn thấy nhiều tường lửa, loại bỏ các vùng bao bảo mật riêng lẻ hoặc các vùng áp dụng các quy tắc bảo mật tương tự. Các vùng bao chung bao gồm các vùng dành cho cơ sở dữ liệu bảo-mật-cao, người dùng bảo-mật-thấp (trung tâm cuộc gọi), các ki-ốt công khai và các giao diện quản lý đối với máy chủ và thiết bị mạng. Việc có được mỗi thành phần này trong

khu vực riêng của nó mang lại sự kiểm soát bảo mật nhiều hơn. Trên lớp quản lý, việc sử dụng lược đồ địa chỉ IP không thể định tuyến cho tất cả các giao diện ngăn chúng được truy cập trực tiếp từ Internet.



**Hình 29-2** Các vùng bao bảo mật



### MÁCH NƯỚC CHO KỲ THI

Phân đoạn, vì nó áp dụng cho bảo mật mạng, là một thuật ngữ rất rộng. Các VLAN, tường lửa và thậm chí cả phân đoạn lưu trữ và phân vùng chứa đều có thể được sử dụng cho mục đích phân đoạn.

## **Điều phối, Tự động hóa và Ứng phó Bảo mật (SOAR)**

Hoạt động bảo mật trong môi trường doanh nghiệp có rất nhiều bộ phận di động. Từ quan điểm cấp-cao-nhất, bạn có quản lý lỗ hổng, thông tin tình báo về mối đe dọa, ứng phó sự cố và các hoạt động bảo mật được tự động hóa. Tất cả những thứ này đều hoạt động dựa trên dữ liệu – những dữ liệu đến từ vô số thiết bị mạng, hệ thống phát hiện xâm nhập, tường lửa và các thiết bị bảo mật khác. Dữ liệu này thường được đưa vào hệ thống quản lý sự kiện và thông tin bảo mật (SIEM) có thể thu thập, tổng hợp và áp dụng đối sánh mẫu cho khối lượng dữ liệu. Các cảnh báo sau đó có thể được xử lý bởi nhân viên bảo mật. Tuy nhiên, điều này còn lâu mới được xem là tích hợp hoàn toàn. Hệ thống điều phối, tự động hóa và ứng phó bảo mật (security orchestration, automation, and response - SOAR) lấy dữ liệu SIEM cũng như dữ liệu từ các nguồn khác và hỗ trợ cho việc tạo ra các runbook và playbook.

Quản trị viên bảo mật có thể tạo một loạt runbook và playbook có thể được sử dụng để ứng phó với một loạt các hoạt động ứng phó sự cố. Các phần tiếp theo sẽ đề cập đến các chi tiết về runbook và playbook. Các kết hợp runbook và playbook có thể được sử dụng để ghi lại các quy trình bảo mật khác nhau và có thể cung cấp cho người dùng các quy trình đã được phê duyệt để điều phối ngay cả những quy trình bảo mật phức tạp nhất. Phần mềm SOAR tích hợp tất cả các yếu tố này thành các giải pháp có thể quản lý được cho nhân viên của trung tâm vận hành bảo mật, tích hợp cả dữ liệu thô và dữ liệu đã được xử lý vào các bước có thể thực hiện dựa trên các quy trình đã được phê duyệt.



### **MÁCH NƯỚC CHO KỲ THI**

Các hệ thống SOAR cực kỳ có giá trị khi được đưa vào việc giảm thiểu sự cố đối với các mối đe dọa nghiêm trọng

vì chúng có thể tự động hóa việc thu thập dữ liệu và bắt đầu ứng phó với mối đe dọa.

### **Runbooks**

Một *runbook* (*sổ tay hướng dẫn*) bao gồm một loạt các bước có điều kiện dựa-trên-hành-động để thực hiện các hành động cụ thể liên quan đến tự động hóa bảo mật. Những hành động này có thể liên quan đến việc thu thập và làm giàu dữ liệu, ngăn chặn mối đe dọa, cảnh báo và thông báo cũng như các yếu tố có thể tự động hóa khác của quy trình vận hành bảo mật. Mục đích chính của runbook là đẩy nhanh quá trình ứng phó sự cố bằng cách tự động hóa một loạt các bước và quy trình đã được phê duyệt. Runbook thường tập trung vào các hệ thống và dịch vụ và cách chúng được quản lý một cách chủ động.

### **Playbooks**

Một *playbook* (*sổ tay hoạt động*) là một tập hợp các bước và hành động đã được phê duyệt cần thiết để ứng phó thành công với một sự cố hoặc một mối đe dọa cụ thể. Các playbook thường được tạo dưới dạng danh sách kiểm tra (checklist) được chia thành từng mục, với tất cả dữ liệu thích hợp đã được điền sẵn vào trước - hệ thống, thành viên nhóm, các hành động, v.v... Các playbook cung cấp một phương pháp tiếp cận đơn giản từng-bước từ-trên-xuống để điều phối các hoạt động của nhóm bảo mật. Chúng có thể bao gồm một loạt các yêu cầu - yêu cầu về kỹ thuật, yêu cầu nhân sự và yêu cầu pháp lý hoặc quy định - tất cả đều ở dạng đã được phê duyệt trước để giảm bớt sự tranh-giành-thời-điểm khi đồng hồ đang điểm vào một sự kiện đang hoạt động.



### **MÁCH NƯỚC CHO KỲ THI**

Một runbook thường tập trung vào các khía cạnh kỹ thuật của các hệ thống hoặc mạng máy tính. Một playbook



ADMINISTRATION & SECURITY  
VIETNAM

thường toàn diện hơn và đặt trọng tâm nhiều hơn vào con người/việc kinh doanh nói chung.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các kỹ thuật giảm thiểu và các biện pháp kiểm soát bảo mật được sử dụng để bảo vệ môi trường. Chương được mở đầu bằng một cuộc thảo luận về cấu hình các giải pháp bảo mật điểm đầu cuối. Cụ thể, các chủ đề về danh sách trắng ứng dụng, danh sách đen ứng dụng và cách ly đã được trình bày. Phần chính tiếp theo bao gồm những thay đổi cấu hình. Các phần phụ trong lĩnh vực này bao gồm các quy tắc tường lửa, quản lý thiết bị di động, ngăn chặn mất dữ liệu, bộ lọc nội dung/bộ lọc URL và cập nhật hoặc thu hồi chứng nhận.

Sau đó, chương này đề cập đến các chủ đề về cô lập, ngăn chặn và phân đoạn. Chương kết thúc với chủ đề về điều phối, tự động hóa và ứng phó bảo mật (SOAR), cùng với các chủ đề phụ về runbook và playbook.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Bạn được chỉ đạo từ quản lý cấp trên để ngăn chặn việc nhân viên truy cập vào Facebook từ máy tính của công ty. Cách dễ nhất để thực hiện biện pháp kiểm soát này là gì?

  - A. Danh sách chấp thuận ứng dụng
  - B. Danh sách chặn ứng dụng
  - C. DLP
  - D. Lọc nội dung.
2. Việc có một chứng nhận đã bị hết hạn là một ví dụ về loại lỗi nào?

  - A. Quản lý thiết bị di động
  - B. Cấu hình
  - C. Danh sách ứng dụng cho phép
  - D. Bộ lọc nội dung/bộ lọc URL.
3. Một tập hợp các bước tự động hóa đã được xác định trước tập-trung-vào-hệ-thống là một ví dụ về điều gì?

  - A. Cô lập
  - B. Runbook
  - C. Playbook
  - D. Các quy tắc tường lửa.
4. Một máy chủ ứng dụng nghiệp vụ của bạn đang gửi dữ liệu đến các đối tác bằng cách sử dụng các thông điệp đã được mã hóa (đã ký). Bạn nghe thấy từ một trong những đối tác rằng thông điệp của họ đã không còn được gửi đến. Bạn nên điều tra về những gì?

  - A. Danh sách ứng dụng được phép
  - B. Danh sách ứng dụng bị chặn

- C. Playbook cho hệ thống**
- D. Thiết lập cấu hình của quy trình.**
- 5.** Bạn có các máy ki-ốt ở sảnh đợi và rải rác khắp cơ sở. Chúng không đòi hỏi khách phải đăng nhập để truy cập các mục nhất định. Cách tốt nhất để bảo vệ những máy này khỏi bị người dùng đưa trojan vào máy là gì?
- A. Danh sách ứng dụng được phép**
- B. Danh sách ứng dụng bị chặn**
- C. Ngăn ngừa mất mát dữ liệu**
- D. Thiết lập cấu hình của quy trình**
- 6.** Để điều phối các hoạt động của nhóm trong một sự kiện ứng phó sự cố, cách tốt nhất để truyền đạt các hướng dẫn đã được phê duyệt là gì?
- A. Runbook**
- B. Giải pháp MDM**
- C. Quy tắc cách ly**
- D. Playbook.**
- 7.** Hệ thống bảo mật của bạn đã xác định rằng một tập tin thực thi cụ thể là có thể nguy hiểm. Cách tốt nhất để xử lý mục cụ thể đã được xác định là gì?
- A. Phân đoạn**
- B. Cách ly**
- C. Quy tắc tường lửa**
- D. Playbook.**
- 8.** Công ty của bạn đã hợp nhất với một công ty khác và công ty này sử dụng một phiên bản phần mềm kế toán khác với công ty của bạn. Làm thế nào bạn có thể cung cấp cho người dùng máy tính trong bộ phận kế toán để họ không vô tình chạy phiên bản không chính xác?

- A. Danh sách ứng dụng được phép**
- B. Cô lập**
- C. Các cấu hình liên quan đến ứng dụng**
- D. Danh sách ứng dụng bị chặn.**
- 9.** Bạn muốn ngăn chặn việc mọi người sử dụng mạng di động nội bộ để chơi trò chơi trên điện thoại cá nhân của họ. Phương pháp tốt nhất để quản lý việc này là gì?
- A. MDM**
- B. Danh sách ứng dụng bị chặn**
- C. Bộ lọc nội dung**
- D. Phân đoạn.**
- 10.** Mục đích chính của giải pháp SOAR là gì?
- A. Để thu thập và tổng hợp dữ liệu bảo mật đa dạng**
- B. Để phân tích dữ liệu về sự bất thường và tạo ra các cảnh báo**
- C. Để đưa ra các kế hoạch ứng phó chi tiết, đã được phê duyệt đối với các tình huống ứng phó sự cố**
- D. Để quản lý các thay đổi cấu hình trên hệ thống.**

## Đáp án

1. **D.** Facebook được truy cập thông qua trình duyệt, vì vậy bạn sẽ cần phải cài đặt tính năng lọc nội dung.
2. **B.** Lỗi chứng nhận thường do lỗi cấu hình liên quan đến chứng nhận.
3. **B.** Từ ngữ “tập-trung-vào-hệ-thống” trở đến một playbook. Một playbook tập trung vào quy trình nghiệp vụ.
4. **D.** Chứng nhận có khả năng đã bị thu hồi hoặc bị loại bỏ khỏi danh tính của người dùng đó và không còn hợp lệ bởi tổ chức phát hành chứng nhận. Đây là một lỗi cấu hình.
5. **A.** Danh sách ứng dụng được phép nghiêm ngặt sẽ giới hạn những gì chạy trên hệ thống chỉ trong phạm nhũng ứng dụng được cho phép.
6. **D.** Các playbook tập trung vào phản hồi của nhóm giao tiếp dưới dạng các yếu tố tập trung vào kinh doanh thay vì các yếu tố máy móc kỹ thuật.
7. **B.** Vì hạng mục là một đối tượng nên biện pháp kiểm dịch được áp dụng. Các phương pháp cô lập khác thuộc về mạng và hệ thống.
8. **D.** Danh sách ứng dụng bị chặn liệt kê các ứng dụng theo số phiên bản sẽ ngăn không cho các phiên bản cụ thể được thực thi trên các máy đã chọn.
9. **A.** Việc bắt buộc người dùng cài đặt giải pháp MDM trước khi kết nối điện thoại của họ với mạng nội bộ giải quyết rất nhiều vấn đề bảo mật, bao gồm cả vấn đề kiểm soát truy cập.
10. **C.** SOAR được biết đến với việc sản tạo ra các runbook và playbook để đáp ứng các điều kiện cụ thể.

## Chương 30    Điều tra pháp y Kỹ thuật số

---

### Điều tra pháp y Kỹ thuật số

Trong chương này bạn sẽ

- Tìm hiểu về những khía cạnh then chốt của điều tra pháp y kỹ thuật số,
  - Tìm hiểu về cơ sở pháp lý đằng sau các quy trình điều tra pháp y,
  - Tìm hiểu về các bước của các quy trình điều tra pháp y.
- 

Điều tra pháp y máy tính chắc chắn là một từ thông dụng phổ biến trong bảo mật máy tính. Thuật ngữ *điều tra pháp y (pháp y)* liên quan đến việc áp dụng những kiến thức khoa học vào các vấn đề pháp lý. Cụ thể, pháp y máy tính liên quan đến việc bảo quản, nhận dạng, lập tài liệu và diễn giải dữ liệu máy tính. Trong nhiều trường hợp, pháp y kỹ thuật số là khía cạnh kỹ thuật của việc phát triển bằng chứng về những gì đã xảy ra hoặc đã không xảy ra như một phần của nỗ lực ứng phó sự cố. Pháp y kỹ thuật số đặc biệt sử dụng các nguyên tắc khoa học để cung cấp sự đảm bảo trong việc giải thích về việc bằng chứng kỹ thuật số nào cho bạn biết về những gì đã xảy ra hoặc chưa xảy ra với một hệ thống máy tính.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 4.5 của kỳ thi CompTIA Security+: Giải thích các khía cạnh chính của pháp y kỹ thuật số.

## Tài liệu/Bằng chứng

Tất cả mọi bằng chứng đều không được tạo ra theo những cách thức giống nhau. Một số bằng chứng mạnh hơn và tốt hơn những bằng chứng khác, yếu hơn. Một số loại bằng chứng có thể thích hợp, bao gồm:

- **Bằng chứng trực tiếp** Lời khai bằng miệng chứng minh cho một sự việc cụ thể (chẳng hạn như lời khai của nhân chứng). Kiến thức về các sự kiện có được thông qua năm giác quan của nhân chứng, không có suy luận hoặc giả định.
- **Bằng chứng thực** Còn được gọi là bằng chứng liên kết hoặc bằng chứng vật chất, điều này bao gồm các đối tượng hữu hình chứng minh hoặc bác bỏ một thực tế. Bằng chứng vật chất liên kết phạm với hiện trường vụ án.
- **Bằng chứng tài liệu** Bằng chứng dưới dạng hồ sơ kinh doanh, bản in, sách hướng dẫn, và những thứ tương tự. Phần lớn bằng chứng liên quan đến tội phạm máy tính là bằng chứng tài liệu.
- **Bằng chứng chứng minh** Được sử dụng để hỗ trợ cho bồi thẩm đoàn và có thể ở dạng mô hình, thí nghiệm, biểu đồ, v.v..., được cung cấp để chứng minh rằng một sự kiện đã xảy ra.

Một loạt các hạng mục có thể được coi là tài liệu và bằng chứng trong một cuộc điều tra. Chương này xem xét một số loại phổ biến mà người ta sẽ gặp trong cuộc kiểm tra pháp y và các vấn đề tương ứng với từng loại.

## Lưu giữ Pháp lý

Trong hệ thống pháp luật của Hoa Kỳ, tiền lệ pháp lý yêu cầu rằng thông tin liên quan tiềm năng phải được lưu giữ ngay lập tức mà một bên "lường trước một cách hợp lý" về vụ kiện tụng hoặc một loại tranh chấp chính thức khác. Mặc dù điều này nghe có vẻ mang tính kỹ thuật, nhưng nó khá dễ hiểu: một khi một tổ chức nhận thức được rằng họ cần phải lưu giữ bằng chứng cho một vụ kiện, thì tổ chức đó phải làm như vậy. Cơ chế

cũng khá đơn giản: một khi bạn nhận thấy tổ chức của mình cần phải lưu giữ bằng chứng, bạn phải sử dụng *lưu giữ pháp lý (legal hold)* hoặc lưu giữ kiện tụng (litigation hold), là quy trình mà bạn bảo quản đúng cách bất kỳ và tất cả bằng chứng kỹ thuật số liên quan đến một vụ việc tiềm ẩn. Sự kiện này thường được kích hoạt bởi một tổ chức đưa ra yêu cầu lưu giữ kiện tụng cho tổ chức khác. Sau khi một tổ chức nhận được thông báo này, tổ chức đó phải duy trì một bộ dữ liệu hoàn chỉnh không thay đổi, bao gồm siêu dữ liệu, của bất kỳ và tất cả thông tin liên quan đến vấn đề gây ra vụ kiện tụng. Điều này có nghĩa là các chính sách lưu giữ dữ liệu thông thường không còn đủ nữa và ngay cả những thay đổi đối với siêu dữ liệu cũng có thể bị coi là vi phạm yêu cầu lưu giữ. Nếu thẩm phán xác định rằng việc vi phạm yêu cầu tạm giữ có thể ảnh hưởng nghiêm trọng đến khả năng đưa ra quyết định của bồi thẩm đoàn thì thẩm phán có thể hướng dẫn bồi thẩm đoàn coi hành vi đó là che giấu bằng chứng. Các quyết định chính của bồi thẩm đoàn đã được quyết định dựa trên việc không lưu giữ thông tin, vì việc không tuân thủ có thể được coi là sơ suất.

Những thông tin là đối tượng của lưu giữ pháp lý nằm ở đâu? Ở mọi nơi, bao gồm email, tài liệu văn phòng (điện tử và giấy), mạng chia sẻ, điện thoại di động, máy tính bảng, cơ sở dữ liệu - ở mọi nơi mà thông tin được chia sẻ, tất cả các bản sao cần được tạo ra theo cách không được thay đổi, ngay cả khi các tài liệu liên quan đã được tạo ra từ nhiều năm trước. Việc tìm kiếm và quản lý tất cả thông tin này thuộc một nhánh của pháp y kỹ thuật số được gọi là khám-phá-điện-tử (e-discovery), liên quan đến việc xác định, quản lý và lưu giữ thông tin kỹ thuật số là đối tượng của lưu giữ pháp lý. Thời gian để chuẩn bị cho tình huống lưu giữ pháp lý là trước khi sự kiện xảy ra vì sẽ mất thời gian để tạo ra các chính sách và

thủ tục cần thiết và khiến cho chúng có hiệu quả thông qua đào tạo nâng cao nhận thức phù hợp.

---



**MÁCH NƯỚC CHO KỲ THI** Việc hiểu được những hệ quả của việc lưu giữ pháp lý và việc lưu giữ hồ sơ hợp pháp thay thế cho bất kỳ chính sách hoặc thủ tục tiêu chuẩn nào của công ty.

### Video

Một phương pháp thuận tiện để nắm bắt thông tin quan trọng tại thời điểm thu thập là quay phim. Các video cho phép thu thập dữ liệu băng-thông-cao có thể hiển thị cái gì được kết nối với những gì, cách mọi thứ được bố trí, máy tính để bàn, v.v... Một bức tranh có thể có giá trị bằng hàng nghìn từ ngữ, vì vậy hãy dành thời gian để ghi lại mọi thứ bằng hình ảnh. Hình ảnh về sổ sê-ri và các kết nối mạng và USB sau này có thể chứng minh là vô giá trong quá trình điều tra pháp y. Tài liệu hoàn chỉnh là điều bắt buộc trong mọi quy trình điều tra pháp y và các bức ảnh có thể hỗ trợ rất nhiều trong việc nắm bắt các chi tiết mà nếu không, sẽ mất rất nhiều thời gian và dễ bị lỗi sao chép.

Một nguồn dữ liệu video khác là trong các camera truyền hình mạch-kín (closed-circuit television - CCTV) được sử dụng cho mục đích an ninh, cả trong công nghiệp và gia đình ngày càng tăng. Giống như tất cả các thông tin kỹ thuật số khác, video CCTV có thể được sao chép và thao tác và cần được bảo quản giống như các thông tin kỹ thuật số khác.

---



**MÁCH NƯỚC CHO KỲ THI** Một camera kỹ thuật số rất thích hợp để ghi lại quang cảnh và thông tin. Ảnh chụp màn hình của hình ảnh màn

hình đang hoạt động cũng có thể được chụp. Các hình ảnh có thể nêu chi tiết các yếu tố như biển số sê-ri, máy móc, ổ đĩa, các kết nối cáp, v.v... Một bức ảnh thực sự đáng giá bằng hàng nghìn ngàn từ ngữ.

Một khía cạnh khác liên quan đến các video trong thế giới được thống-trị-bởi-diện-thoại-thông-minh ngày nay - nơi hàng triệu video được ghi lại mỗi ngày và tải lên các trang web truyền thông xã hội như Twitter, Facebook, YouTube, v.v..., là sự phân chia hợp pháp của các luồng bằng chứng như vậy. Cộng thêm khả năng làm giả tinh vi do AI tạo ra, và nhu cầu xác thực các nguồn "bằng chứng" này đã trở thành điều thực tế trong điều tra pháp y kỹ thuật số.

### **Tính có thể chấp nhận được (Admissibility)**

Để bằng chứng trở nên đáng tin cậy, đặc biệt nếu như nó sẽ được sử dụng trong các thủ tục tố tụng tại tòa án hoặc trong các hành động kỷ luật của công ty mà có thể gặp phải thách thức về mặt pháp lý, nó phải đáp ứng ba tiêu chuẩn dưới đây:

- **Bằng chứng đầy đủ** Bằng chứng phải thuyết phục hoặc được đo lường mà không bị nghi ngờ.
- **Bằng chứng phải thích hợp** Bằng chứng phải đủ tiêu chuẩn và đáng tin cậy về mặt pháp lý.
- **Bằng chứng phải có liên quan** Bằng chứng phải là điều quan trọng của vụ án hoặc có liên quan đến vấn đề.

Đối với các tài liệu đáp ứng các tiêu chuẩn này để *có thể được chấp nhận*, điều quan trọng là các thủ tục thích hợp phải được tuân thủ ở tất cả các giai đoạn trong quá trình thu thập, xử lý và phân tích. Một vật phẩm chính thức trở thành bằng chứng trong quá trình tố tụng pháp lý khi thẩm phán xác định rằng vật phẩm đó được chấp nhận. Ba quy tắc định hướng

việc xác định của thẩm phán về việc có thừa nhận một vật phẩm làm bằng chứng hay không bao gồm:

- **Quy tắc bằng chứng tốt nhất (Best evidence rule)** Tòa án thích bằng chứng nguyên thủy hơn là bản sao, để đảm bảo rằng đã không có sự thay đổi bằng chứng (dù cố ý hay vô ý) xảy ra. Trong một số trường hợp, bản sao bằng chứng có thể được chấp nhận, chẳng hạn như khi bản gốc bị mất hoặc bị phá hủy do thiên tai hoặc trong quá trình kinh doanh bình thường. Bản sao cũng được chấp nhận khi một bên-thứ-ba nắm ngoài quyền hạn của trát đòi hầu tòa của tòa án đang sở hữu bản gốc. Trong nhiều trường hợp, các bản sao của hồ sơ kỹ thuật số, nơi cung cấp bằng chứng về tính toàn vẹn, có thể được sử dụng tại tòa án.



#### LƯU Ý

Các quy tắc về bằng chứng tồn tại ở cấp liên bang và tiểu bang và sẽ khác nhau. Các bằng chứng kỹ thuật số không phải lúc nào cũng được coi là "văn bản" và không phải lúc nào cũng tuân theo quy tắc bằng chứng tốt nhất.

- **Quy tắc loại trừ (Exclusionary rule)** Tu chính án thứ tư đối với Hiến pháp Hoa Kỳ loại trừ việc khám xét và thu giữ bất hợp lý. Do đó, bất kỳ bằng chứng nào được thu thập đã vi phạm Tu chính án thứ tư đều không được chấp nhận là bằng chứng. Ngoài ra, nếu bằng chứng được thu thập vi phạm Đạo luật về Quyền riêng tư của Giao tiếp Điện tử (ECPA) hoặc các vi phạm có liên quan khác của Bộ luật Hoa Kỳ hoặc các đạo luật khác thì có thể sẽ không được tòa án chấp nhận. Ví dụ, nếu không có chính sách nào tồn tại liên quan

đến ý định của công ty là giám sát lưu lượng mạng hoặc hệ thống băng điện tử, hoặc nếu chính sách đó có tồn tại nhưng nhân viên không được yêu cầu thừa nhận bằng cách ký vào thỏa thuận, việc thu thập lưu lượng mạng của nhân viên có thể là vi phạm ECPA.

- **Quy tắc tin đồn (Hearsay rule)** Tin đồn là bằng chứng gián tiếp - bằng chứng được cung cấp bởi nhân chứng không dựa trên kiến thức cá nhân của nhân chứng nhưng được cung cấp để chứng minh sự thật của vấn đề đã được khẳng định. Tin đồn là không thể chấp nhận được trừ khi nó thuộc một trong nhiều trường hợp ngoại lệ đã được công nhận (chẳng hạn như những trường hợp được mô tả trong FRE 803). Thông thường, bằng chứng do máy tính tạo ra được coi là bằng chứng tin đồn, vì người tạo ra bằng chứng (máy tính) không thể bị thẩm vấn. Các trường hợp ngoại lệ đang được đưa ra khi các vật phẩm như các nhật ký và tiêu đề (tài liệu được tạo ra bởi máy tính) đang được chấp nhận tại tòa án. Bằng chứng máy tính thường được đưa vào một vụ án bởi một nhân chứng chuyên môn, người có thể nói về dữ liệu và ý nghĩa của nó.



## LƯU Ý

Những luật lệ được đề cập ở đây là các luật lệ của Hoa Kỳ. Những quốc gia và khu vực tài phán khác có thể có những đạo luật tương tự cần được xem xét theo cách thức tương tự.

## Chuỗi Bảo quản bằng chứng (Chain of Custody)

Sau khi bằng chứng đã được thu thập, nó phải được kiểm soát một cách thích hợp để ngăn chặn sự giả mạo. Chuỗi hành trình quản lý bằng chứng sẽ tính đến tất cả những người đã xử lý hoặc có quyền truy cập vào bằng chứng. Cụ thể hơn, chuỗi bảo quản bằng chứng cho thấy ai đã thu được

bằng chứng, khi nào và ở đâu, vị trí lưu trữ, và ai có quyền kiểm soát hoặc sở hữu bằng chứng trong toàn bộ thời gian kể từ khi thu thập được bằng chứng. Bất kỳ quyền truy cập và mọi truy cập vào bằng chứng sẽ phải được ghi lại.

Dưới đây là các bước quan trọng trong chuỗi bảo quản bằng chứng:

1. Ghi lại từng vật phẩm đã được thu thập để làm bằng chứng.
2. Ghi lại người đã thu thập bằng chứng cùng với ngày và giờ nó được thu thập hoặc được ghi lại.
3. Viết một mô tả về bằng chứng trong tài liệu.
4. Bỏ bằng chứng vào thùng chứa và gắn thẻ số vụ án, tên người đã thu thập, ngày giờ thu thập hoặc ngày giờ bằng chứng được bỏ vào thùng.
5. Ghi lại tất cả các giá trị phân loại (băm) thông điệp trong tài liệu.
6. Vận chuyển một cách an toàn các bằng chứng đến cơ sở lưu trữ được bảo vệ.
7. Có được chữ ký của người chấp nhận chứng cứ tại cơ sở lưu trữ này.
8. Cung cấp các biện pháp kiểm soát để ngăn chặn việc truy cập và xâm phạm bằng chứng trong khi bằng chứng đang được lưu trữ.
9. Vận chuyển một cách an toàn các bằng chứng đến tòa án để tiến hành tố tụng.



**MÁCH NƯỚC CHO KỲ THI**      Đừng bao giờ phân tích trực tiếp các bằng chứng đã thu giữ được. Bằng chứng nguyên thủy phải được bảo mật và bảo vệ bằng một chuỗi bảo quản bằng chứng. Nó không bao giờ nên được giám định pháp y vì bản chất mong manh của bằng chứng kỹ thuật số. Tuy nhiên, một bản sao pháp y có thể được kiểm tra và nếu có vấn đề gì xảy ra, sẽ bị loại bỏ và quá trình sao chép có thể được lặp lại. Một

quy trình điều tra pháp y tốt sẽ chứng minh được rằng bản sao pháp y giống hệt với bản gốc khi bắt đầu và khi kết thúc quá trình kiểm tra. Từ quan điểm thực tế, các nhà điều tra thường tạo ra nhiều bản sao pháp y và thực hiện phân tích của họ song song trên nhiều bản sao.

### **Thời hạn của Chuỗi trình tự của các Sự kiện**

Các cuộc điều tra pháp y kỹ thuật số bắt đầu với một phạm vi, một trách nhiệm về những gì quan tâm được điều tra. Trong một môi trường máy tính hiện đại, việc yêu cầu mọi thứ đã xảy ra là một phạm vi không thể thực hiện được, vì chỉ cần khởi động một máy tính đã có thể dẫn đến hàng trăm sự kiện, theo đúng nghĩa đen. Một khi phạm vi được xác định, nó chắc chắn sẽ bao gồm yếu tố thời gian, thường là thứ gì đó theo trình tự như sau: năm giữa ngày và giờ bắt đầu và ngày và giờ kết thúc, đối với người dùng XYZ, hãy kiểm tra đối với (chèn bất kỳ điều gì được quan tâm ở đây, có thể là từ khóa, các loại hành động cụ thể, v.v...). Với thông tin này là ranh giới, thường sẽ tạo ra một *dòng thời gian của các sự kiện cụ thể* nằm trong phạm vi và ranh giới thời gian. Dòng thời gian này sẽ có các chi tiết cụ thể, bao gồm siêu dữ liệu để ghi nhận lại nó, thể hiện chuỗi các sự kiện như được ghi nhận lại bởi máy tính. Trình tự có thể rất quan trọng vì nó cung cấp những manh mối chính về những gì đã thực sự xảy ra, ngay cả khi không có hiện vật trực tiếp. Ví dụ, nếu lần đầu tiên một ổ USB được gắn vào là sau khi tập tin được chạm vào lần cuối và siêu dữ liệu có sẵn trong sổ đăng ký, thì tập tin đó có thể không được chuyển trên USB. Thông tin đăng nhập và đăng xuất của người dùng cũng giúp xác định trình tự và hoạt động. Nếu người dùng bị buộc tội thực hiện giao dịch X trên một tài nguyên mạng vào một ngày và giờ cụ thể, nhưng máy tính cá nhân của họ cho thấy họ chưa đăng nhập, nghĩa là họ đã sử dụng một máy tính khác hoặc có điều gì đó khác đang xảy ra, chẳng hạn như một tài khoản bị xâm nhập. Việc xây dựng một dòng thời gian của các hoạt động từ nhiều khía cạnh có thể cung cấp nhiều thông tin

hữu ích về điều gì đã xảy ra, điều gì có thể đã xảy ra và điều gì không có ý nghĩa (sẽ cần thêm dữ liệu).

## Dấu thời gian (Timestamps)

*Dấu thời gian* là các mục nhập siêu dữ liệu được liên kết với các tạo tác trong hệ thống máy tính. Mặc dù một mục nhập trong nhật ký có thể có dấu thời gian, nhưng một số mục có thể có rất nhiều dấu thời gian, được lưu trữ ở nhiều vị trí. Trong NTFS, có ba thời gian tập tin phổ biến (thời gian Tạo ra, Sửa đổi, Đã truy cập) và một thời gian siêu dữ liệu (Thay đổi MFT). Bốn dấu thời gian này được lưu trữ ở hai nơi: một có thuộc tính \$File\_Name và một có thuộc tính \$Standard\_Info. Và nếu đó vẫn chưa đủ gây bối rối thì hai thuộc tính khác nhau sẽ được cập nhật một cách khác nhau, nghĩa là chúng có thể khác nhau. Điều này rất quan trọng đối với các cuộc điều tra pháp y vì dấu thời gian có thể được thay đổi trên các hệ thống và điều này có thể dẫn đến những kết luận sai lầm. Việc giả mạo dấu thời gian là một thách thức vì hầu hết các công cụ không xử lý tất cả các dấu thời gian theo cùng một cách thức, điều này vốn có thể dẫn đến bằng chứng về việc giả mạo.

Thời gian được đo một cách khác nhau trong Linux và Windows. Linux sử dụng khái niệm Epoch time - số giây đã trôi qua kể từ ngày 1 tháng 1 năm 1970 (nửa đêm giờ UTC/GMT), không tính giây nhuận. Nó được lưu trữ dưới dạng số 32-bit có chữ ký, hỗ trợ cho thời gian trước ngày 1 tháng 1 năm 1970, cũng như sau đó. Đồng hồ hệ thống có độ phân giải một giây, mặc dù có các phần tử hẹn giờ cho phép đo thời gian xuống đến nano giây. Microsoft Windows sử dụng giá trị 64-bit đại diện cho thời gian đã trôi qua kể từ 12:00AM ngày 1 tháng 1 năm 1601 Giờ Phối hợp Quốc tế (Coordinated Universal Time - UTC), với độ phân giải vào khoảng 100 nano giây. Hãy lưu ý rằng cả hai hệ thống đều sử dụng UTC làm cơ

sở và hầu hết việc lưu trữ các phần tử thời gian đều được thực hiện trong UTC, với việc chuyển đổi sang giờ địa phương xảy ra khi đọc một giá trị.

Một trong những thách thức đối với tất cả việc sử dụng dấu thời gian là sự không nhất quán trong hệ điều hành trong việc giữ cho các giá trị luôn được cập nhật. Mặc dù Microsoft Windows có rất nhiều dấu thời gian khác nhau để xem xét, nhưng có sự mâu thuẫn lớn về nhiều giá trị trong số các dấu thời gian này đang được cập nhật bởi hệ điều hành hoặc một ứng dụng. Lý do chính cho điều này xoay quanh hiệu suất, vì hầu hết các dấu thời gian chỉ là hiện vật và không quan trọng trong nhiều chức năng của hệ điều hành tiêu chuẩn. Việc không duy trì dấu thời gian hoặc không duy trì tất cả các bản sao của dấu thời gian có thể cải thiện hiệu suất của một số hoạt động.

### **Độ lệch thời gian (Time Offset)**

Bản ghi *Độ lệch thời gian* là sự chênh lệch về thời gian giữa đồng hồ hệ thống và thời gian thực. Máy tính giữ thời gian nội bộ của riêng chúng, nhưng để giảm thiểu bản ghi độ lệch thời gian, hầu hết các máy tính đồng bộ thời gian của chúng qua Internet với một nguồn thời gian chính thức. Các tập tin và sự kiện được ghi lại trên máy tính sẽ có dấu thời gian dựa trên thời gian trên chính máy đó. Thật sai lầm khi cho rằng chiếc đồng hồ này là chính xác. Để cho phép mối tương quan của dữ liệu dấu thời gian từ các bản ghi bên trong máy tính với bất kỳ sự kiện bên ngoài nào, cần biết được bất kỳ khoảng chênh lệch thời gian nào giữa đồng hồ máy và thời gian thực. Khi thu thập dữ liệu điều tra pháp y, điều tối quan trọng là phải thu thập bản ghi độ lệch thời gian để những biến đổi cục bộ về thời gian có thể được khắc phục.

Một dạng chênh lệch thời gian khác là chênh lệch giữa múi giờ địa phương và UTC. Như đã thảo luận trước đó, với hầu hết các bản ghi thời gian ở

UTC, việc chuyển đổi sang múi giờ địa phương có thể cần thiết để hiểu được một số bản ghi.

---



**LƯU Ý** Bất cứ khi nào ai đó sử dụng thời gian, dù là dấu thời gian, thời gian nhật ký hay so sánh với lịch thực tế, điều quan trọng là phải đồng bộ hóa tất cả các bản ghi vào cùng một khoảng chênh lệch. Rất nhiều bản ghi sử dụng giờ địa phương. Việc so sánh giờ địa phương và giờ UTC sẽ dẫn đến sai số, ngoại trừ múi giờ GMT, trong đó giờ địa phương là UTC. Hãy tìm hiểu thời gian của bạn đối với các khu vực trước khi sử dụng.

---



**MÁCH NƯỚC CHO KỲ THI** Việc hiểu được các thành phần thời gian đối với điều tra pháp y là điều rất quan trọng. Hãy chú ý đến múi giờ và các chi tiết cụ thể trong câu hỏi.

### Các Thẻ

Như đã thảo luận trước đây, một tài liệu chuỗi-bảo-quản-băng-chứng ghi lại mọi truy cập vào băng chứng tính từ thời điểm thu thập cho đến khi tiêu hủy. Nhưng làm thế nào để người ta đề cập đến một phần băng chứng cụ thể, đặc biệt nếu nó là phần cứng có chứa dữ liệu, chẳng hạn như ổ USB? Điều này được thực hiện thông qua các thẻ. Các *thẻ* được đánh số sê-ri vật lý được gắn vào mỗi vật phẩm và số thẻ được sử dụng để xác định một vật phẩm cụ thể. Thông thường, các vật phẩm sau đó được cất giữ trong các túi chống tĩnh điện để bảo vệ chúng khỏi bị hư hỏng.

## Báo cáo

Các *báo cáo* là những mô tả chính thức về dữ liệu điều tra pháp y. Báo cáo có thể có nhiều thành phần khác nhau - từ thông tin mang tính mô tả thuần túy, chẳng hạn như mã số nhận dạng máy/thiết bị (ngày sản xuất, kiểu máy và số sê-ri), đến thông tin về dữ liệu, bao gồm cả kích thước và giá trị băm. Các báo cáo cũng có thể có các thành phần cụ thể bắt nguồn từ thông tin này, chẳng hạn như dòng thời gian, phân tích các từ khóa, hiện vật cụ thể và các vật phẩm hiện hữu hoặc bị thiêu. Một chuyên gia có thể xem xét những yếu tố này có nghĩa là gì hoặc có thể có ý nghĩa gì đối với hệ thống. Ví dụ, nếu dấu thời gian khác nhau đáng kể, chuyên gia có thể lưu ý (phát biểu) rằng đang tồn tại sự khác biệt. Từ góc độ chuyên môn, điều quan trọng là điều tra viên pháp y chỉ bám vào những gì thông tin có thể hiển thị và không cố gắng bổ sung thêm bình luận. Ví dụ, nếu dữ liệu dấu thời gian đã bị giả mạo thì đây là một sự thật có thể chứng minh được. Tuy nhiên, việc xem xét ai đã làm điều đó mang tính suy đoán nhiều hơn và có thể dẫn đến việc chuyên gia bị đưa ra tòa về việc này. Các chuyên gia đi lạc khỏi điều có thể được chứng minh có thể bị loại bởi thẩm phán, và bị loại khỏi một vụ án là một vết đen sẽ gây ra thắc mắc về ý kiến bây giờ và trong tương lai của một ai đó. Do đó, các báo cáo có xu hướng được làm sạch và các luật sư sẽ thêm màu sắc của vụ việc vào sau đó.

## Nhật ký Sự kiện

Lý tưởng nhất, bạn nên giảm thiểu phạm vi ghi nhật ký để từ đó, khi phải tìm kiếm trong các nhật ký, sự kiện bạn quan tâm sẽ nổi bật lên mà không bị ẩn đi trong một biển các mục nhật ký không liên quan. Trước khi một sự cố xảy ra, nếu như là một phần của giai đoạn chuẩn bị, tổ chức đang giới hạn việc ghi nhật ký đối với những sự kiện cụ thể - chẳng hạn như sao chép các tập tin nhạy cảm - thì sau đó, nếu có câu hỏi về việc liệu sự kiện có xảy ra hay không thì một tập tin nhật ký sẽ tồn tại để cung

cấp thông tin. Khi bạn có ý tưởng về những thông tin nào bạn sẽ muốn có khả năng sẽ được kiểm tra, bạn có thể lập kế hoạch ghi nhật ký chủ động để đảm bảo thông tin được ghi lại khi nó xảy ra và nếu có thể ở một vị trí có thể ngăn ngừa sự thay đổi. Việc *ghi nhật ký chủ động* được xác định trong quá trình chuẩn bị, và khi đến thời điểm phục hồi, việc lập kế hoạch trước sẽ mang lại hiệu quả trong việc tạo ra bằng chứng. Thu thập thông tin tình báo chiến lược, được đề cập ở phần sau của chương, có thể cung cấp những thông tin cần thiết để xây dựng một kế hoạch ghi nhật ký chủ động có hiệu quả.

### **Phỏng vấn**

Hãy nhớ rằng độ tin cậy của nhân chứng là điều cực kỳ, cực kỳ quan trọng. Có thể dễ dàng hình dung mức độ uy tín có thể bị tổn hại một cách nhanh chóng như thế nào nếu nhân chứng không thể trả lời một cách chắc chắn khi được hỏi, "Bạn đã khóa hệ thống tập tin chưa?", hoặc khi được hỏi, "Khi bạn chụp ảnh ổ đĩa này, bạn có sử dụng hệ thống mới không?", nhân chứng không thể trả lời rằng đĩa đích là mới hay đã được định dạng hoàn toàn bằng định dạng cấp-thấp trước khi dữ liệu được sao chép sang nó. Việc chuẩn bị nhân chứng có thể rất quan trọng trong một vụ án, ngay cả đối với các chuyên gia kỹ thuật.

Vì trí nhớ của con người không lâu dài như các tập tin máy tính nên điều quan trọng là phải lấy được lời khai của nhân chứng và thu thập được dữ liệu đó càng sớm càng tốt. Hãy yêu cầu họ viết ra những gì họ nhớ ngay lập tức sẽ rất hữu ích trong việc bảo tồn trí nhớ.



**MÁCH NƯỚC CHO KỲ THI** Các thành phần khác nhau trong tài liệu/bằng chứng hoạt động cùng nhau, không phải là các thực thể riêng biệt. Hãy chắc chắn đã hiểu câu hỏi yêu cầu cụ thể về điều gì khi bạn

chọn câu trả lời, vì một số câu trả lời có thể được kết nối với một câu trả lời đúng, nhưng một câu trả lời sẽ là thành phần chính.

### **Thu thập (Acquisition)**

*Thu thập* đề cập đến việc thu thập thông tin có thể trở thành bằng chứng trong một cuộc điều tra. Bằng chứng bao gồm các tài liệu, lời tuyên bố bằng lời nói, và các hiện vật vật chất có thể được chấp nhận trước tòa án pháp luật. Bằng chứng là rất quan trọng để thuyết phục cấp quản lý, bồi thẩm đoàn, thẩm phán hoặc các cơ quan chức năng khác rằng một sự kiện cụ thể đã thực sự xảy ra. Điều tối quan trọng là phải ghi lại tất cả các bước đã được thực hiện trong quá trình thu thập bằng chứng, vì những bước này có thể bị thách thức trước tòa và các quá trình được theo sau như được chứng minh bằng tài liệu sẽ là tất cả những gì có thể được sử dụng để chứng minh tính xác thực của các quá trình. Các bước liên quan đến việc thu thập bằng chứng rất quan trọng, vì hậu quả của việc không tuân thủ các quy trình thích hợp có thể sẽ không rõ ràng ngay lập tức và có thể là không thể sửa chữa được sau khi thực tế diễn ra.

Việc thu thập, lưu trữ và đệ trình bằng chứng là một thách thức, nhưng càng khó hơn khi máy tính được sử dụng vì những người liên quan có thể đã không được đào tạo về kỹ thuật và do đó có thể không hiểu đầy đủ về những gì đã xảy ra. Hãy ghi nhớ những điểm này khi bạn thu thập bằng chứng:

- Ai đã thu thập bằng chứng?
- Nó [bằng chứng] đã được thu thập như thế nào?
- Nó đã được thu thập ở đâu?
- Ai đã từng sở hữu nó?
- Nó đã được bảo vệ và lưu trữ như thế nào?
- Khi nào thì nó đã bị xóa khỏi bộ nhớ? Tại sao? Ai đã nắm quyền sở hữu?

Bằng chứng máy tính đưa ra nhiều thách thức hơn, vì bản thân dữ liệu không thể được xác định bằng các giác quan vật lý - nghĩa là, bạn có thể nhìn thấy các ký tự được in, nhưng bạn không thể nhìn thấy [*theo nghĩa đen*] các bit nơi dữ liệu đó được lưu trữ. Các bit dữ liệu chỉ đơn thuần là các xung từ tính trên đĩa hoặc một số công nghệ lưu trữ khác. Do đó, dữ liệu phải luôn được đánh giá thông qua một số loại "bộ lọc" thay vì được cảm nhận một cách trực tiếp. Điều này thường là mối bận tâm của kiểm toán viên, bởi vì các kỹ thuật kiểm toán tốt khuyến nghị bạn nên truy cập vào dữ liệu gốc hoặc phiên bản càng gần với dữ liệu gốc càng tốt. Hơn nữa, bất kỳ quá trình lọc nào, nếu cần thiết, sẽ không thay đổi ý nghĩa của dữ liệu.

### **Thứ tự của Biến động (Order of Volatility)**

Có rất nhiều nguồn dữ liệu trong hệ thống máy tính, và nếu máy đang chạy, một số nguồn này sẽ rất dễ biến động. Các hạng mục như trạng thái của CPU và các thanh ghi của nó, RAM và thậm chí cả bộ lưu trữ luôn thay đổi, điều này có thể khiến cho việc thu thập dữ liệu điện tử trở thành một nhiệm vụ rất khó khăn và phức tạp. Các thành phần này có xu hướng thay đổi ở các tỷ lệ khác nhau và bạn nên chú ý *đến thứ tự biến động* hoặc thời gian tồn tại của dữ liệu, để bạn có thể ưu tiên các nỗ lực thu thập của mình sau một sự cố bảo mật để đảm bảo rằng bạn không bỏ mất bằng chứng pháp y có giá trị. Trong một số trường hợp, bạn có thể chỉ có một cơ hội để thu thập dữ liệu biến động, sau đó, dữ liệu đó sẽ bị mất đi vĩnh viễn.

Dưới đây là thứ tự biến động của thông tin kỹ thuật số trong một hệ thống:

1. CPU, bộ nhớ đệm, và các nội dung thanh ghi (thu thập đầu tiên)
2. Các bảng định tuyến, bộ đệm ARP, các bảng tiến trình, thống kê lỗi
3. Các kết nối mạng đang hoạt động và luồng dữ liệu

4. Bộ nhớ (RAM)
  5. Các hệ thống tập tin tạm thời/không gian hoán đổi
  6. Dữ liệu trên ổ cứng
  7. Dữ liệu đăng nhập từ xa
  8. Dữ liệu được lưu trữ trên các phương tiện cất giữ/sao lưu (thu thập sau cùng)
- 



**MÁCH NƯỚC CHO KỲ THI** Việc hiểu được thứ tự biến động của thông tin kỹ thuật số trong một hệ thống là một hạng mục có thể kiểm tra được – hãy ghi nhớ điều này.

Không lưu tâm đến thứ tự của biến động trong quá trình thu thập dữ liệu sẽ dẫn đến mất dữ liệu, và khi đã mất, rất nhiều thể loại dữ liệu sẽ biến mất mãi mãi.

---



**MÁCH NƯỚC CHO KỲ THI** Một thành phần dữ liệu sau này được cần đến trong quá trình điều tra pháp y là một thời gian hệ thống chính xác liên quan đến một nguồn thời gian bên ngoài chính xác. Một bản ghi sự chênh lệch thời gian được tính toán bằng cách đo lường thời gian của hệ thống với một đồng hồ bên ngoài như một máy chủ Giao thức Thời gian Mạng (Network Time Protocol – NTP). Sự chênh lệch giữa thời gian của hệ thống và thời gian chính xác có thể bị mất nếu như hệ thống bị tắt nguồn, do đó tốt nhất là thu thập nó khi hệ thống vẫn đang hoạt động.

## Ổ đĩa

Khi thu thập những bằng chứng kỹ thuật số, điều quan trọng là phải sử dụng những kỹ thuật và công cụ thích hợp. Một vài trong số các thành phần then chốt là việc sử dụng khóa chống ghi khi thực hiện sao chép các bản sao pháp y, băm và xác minh việc khớp băm, xử lý và lưu trữ tài liệu, và bảo vệ phương tiện khỏi các yếu tố thay đổi mang tính môi trường. Đặc biệt lưu ý rằng dữ liệu đang hiện diện trên một hệ thống có thể là một chức năng của cả hệ thống tập tin và phần cứng đang được sử dụng. Một ổ đĩa cứng vật lý (HDD) sẽ lưu trữ dữ liệu lâu hơn ổ đĩa thẻ rắn (SSD). Và các hệ thống tập tin mới hơn với các bản ghi nhật ký và bản sao dạng shadow có thể có thông tin tồn tại lâu hơn các hệ thống cũ hơn như hệ thống dựa-trên-Bảng-Phân-bổ-Tập-tin (File Allocation Table) (dựa-trên-FAT). Các khối đĩa thô có thể được khôi phục trong một số hệ thống tập tin sau khi dữ liệu đã bị ghi đè hoặc bị xóa, do bản chất của cách thức mà các hệ thống tập tin quản lý dữ liệu như thế nào.

## Bộ nhớ Truy-cập-Ngẫu-nhiên (RAM)

*Bộ nhớ truy-cập-ngẫu-nhiên (RAM)* là bộ nhớ hoạt động của máy tính để xử lý dữ liệu hiện hành và các chương trình đang được xử lý bởi CPU. Bộ nhớ này, từ chối bị giới hạn ở 1-megabyte đơn lẻ giờ đây bao gồm 4GB hoặc nhiều hơn. Bộ nhớ này lưu lại trạng thái hiện tại của hệ thống khi nó đang xử lý và liên tục thay đổi. Có những trường hợp mà phần mềm độc hại chỉ tồn tại trên RAM, và nếu không phân tích và điều tra pháp y bộ nhớ, bạn sẽ không bao giờ phát hiện ra nó. Nhưng thông tin này cũng sẽ biến mất vĩnh viễn khi hệ thống bị tắt nguồn.

## Tập tin hoán đổi/Phân trang (Swap/Pagefile)

*Hoán đổi* hoặc *tập tin phân trang* là một cấu trúc trên ổ đĩa của một hệ thống để cung cấp bộ lưu trữ tạm thời cho bộ nhớ cần thiết khi đã vượt quá dung lượng RAM của một hệ thống. Hệ điều hành có các quy định để quản lý RAM và tập tin phân trang, chỉ giữ trong RAM những gì cần thiết

ngay tức thời và chuyển phần thừa sang tập tin phân trang khi RAM đã đầy. Điều này gây ra sự ảnh hưởng đến hiệu suất và với chi phí hợp lý cho RAM, hầu hết các hệ thống tránh điều này bằng cách có đủ RAM. Việc ghi lại tập tin phân trang (pagefile.sys được lưu trữ theo mặc định trong C:\pagefile.sys) trong một cuộc điều tra pháp y là điều quan trọng bắt cứ khi nào RAM được kiểm tra vì nó là một phần mở rộng của RAM.

### **Hệ điều hành (OS)**

*OS* hay hệ điều hành là một chương trình cơ sở của máy tính hoạt động như một nhà quản lý mọi hoạt động trên một hệ thống. OS là nguồn gốc của rất nhiều vật phẩm điều tra pháp y, hầu hết trong số chúng được tạo ra để nâng cao khả năng phản hồi của hệ thống đối với các yêu cầu của người dùng. Hai hệ điều hành chính, Microsoft Windows và Linux, về cơ bản thực hiện các nhiệm vụ giống nhau: chúng cho phép các ứng dụng được thực hiện trên một hệ thống. Cách chúng hoạt động, vật phẩm nào được tạo ra, mọi chi tiết kỹ thuật liên quan đến một cuộc điều tra pháp y đều khác nhau và do đó đòi hỏi sự xử lý riêng biệt và chuyên biệt đối với Hệ điều hành.

### **Thiết bị**

Một trong những cách chiếm được *thiết bị* phổ biến nhất là các thiết bị lưu trữ USB. Những thiết bị này được sử dụng để truyền tải tập tin giữa các máy và thường sử dụng trong bất kỳ trường hợp nào có nghi vấn về việc xóa thông tin. Một số hiện vật có thể liên quan đến việc sử dụng thiết bị USB trên hệ thống, bao gồm thời điểm nó được kết nối, liên kết các tập tin và tìm nạp trước các mục trên ổ đĩa và ai đã đăng nhập vào máy tại thời điểm sử dụng.

### **Firmware**

*Firmware* là một tập hợp phần mềm tương ứng với một thiết bị vật lý. Firmware tồn tại trong hầu hết các thiết bị điện tử, không chỉ trong các

máy tính, ví dụ: firmware dành cho các thiết bị USB. Firmware có thể là một mối quan tâm trong một cuộc điều tra pháp y khi sự hoạt động sai lệch của một thiết bị là một vấn đề, khi malware nhắm mục tiêu đến firmware. Do đó, cần một bộ công cụ và thiết bị rất chuyên dụng để phân tích phần firmware, vì không dễ dàng truy cập được đối với người dùng bên ngoài.

### **Ảnh chụp nhanh**

*Ảnh chụp nhanh*, như bạn có thể dễ dàng đoán được, là hình ảnh của một thời điểm cụ thể. Ảnh chụp nhanh rất phổ biến trong máy ảo, cung cấp một thời điểm mà máy có thể được khôi phục về đó. Các hệ điều hành cũng đã áp dụng công nghệ này cho một số thông tin của họ, sử dụng khôi phục tại-thời-điểm (point-in-time) để hỗ trợ cho việc khắc phục các sự cố từ các bản cập nhật hoặc thay đổi đối với hệ thống. Việc nắm bắt các điểm-theo-thời-gian này có thể hữu ích đối với một chuyên gia điều tra pháp y vì nó cho phép một phương tiện xem xét nội dung cụ thể tại một thời điểm sớm hơn. Phạm vi của những gì được bao phủ bởi ảnh chụp nhanh có thể khác nhau giữa các hệ thống khác nhau và điều này có thể hạn chế tính hữu ích của nó.

### **Bộ nhớ đệm**

*Bộ nhớ đệm* là những vị trí lưu trữ tạm thời dành cho các hạng mục thường được sử dụng và được thiết kế để tăng tốc xử lý. Các bộ nhớ đệm tồn tại khắp nơi trong hệ thống máy tính và là các hạng mục nâng cao hiệu suất. Bộ nhớ đệm tồn tại đối với tập tin, đối với bộ nhớ, đối với hiện vật, chúng tồn tại để truy xuất nhanh các mục mà Hệ điều hành đang mong đợi. Như vậy, chúng vốn có liên quan đến một hoạt động cụ thể đã được thực hiện và có khả năng được thực hiện lại và có thể dùng làm bằng chứng về các hoạt động cụ thể đã được thực hiện. Ví dụ về điều

này sẽ là một hiện vật, chẳng hạn như bản ghi prefetch của một tập tin, cho biết rằng người dùng đã đăng nhập trước đó đã mở tập tin đó.

## Mạng

Một nguồn quan trọng của thông tin trong một cuộc điều tra có thể là hoạt động mạng tương ứng với một thiết bị. Có thể có rất nhiều thông tin hữu ích trong các tập tin nhật ký mạng được liên kết với cơ sở hạ tầng mạng. Mức độ và độ chính xác của thông tin này được xác định bởi phạm vi của cuộc điều tra. Mặc dù dữ liệu tốt nhất sẽ đến từ một quá trình thu thập thông tin điều tra pháp y của mạng đang hoạt động nhưng trong hầu hết các trường hợp, kiểu dữ liệu này sẽ không có sẵn. Có rất nhiều khác của dữ liệu điều tra pháp y mạng, bao gồm các tập tin nhật ký tường lửa và IDS, dữ liệu luồng lưu lượng mạng, và các nhật ký sự kiện về các máy chủ và dịch vụ chính.

## Hiện vật

*Hiện vật* là những thành phần then chốt trong các cuộc điều tra pháp y kỹ thuật số hiện đại. Hầu hết các vật phẩm được sử dụng để chứng minh cho một hành động cụ thể đang xảy ra thuộc về một trong hai loại: siêu dữ liệu hoặc hiện vật hệ điều hành. Ví dụ về siêu dữ liệu bao gồm các mục registry, dấu thời gian và kích thước. Hiện vật Hệ điều hành bao gồm các tập tin nạp trước (prefetch), các hiện vật danh sách nhảy (jump list) chẳng hạn như được sử dụng thường xuyên nhất (most frequently used - MFU) và được sử dụng gần đây nhất (most recently used - MRU), shell bags và tập tin liên kết. Hiện vật siêu dữ liệu là các mục mà Hệ điều hành sử dụng để thực hiện các nhiệm vụ của nó, trong khi hầu hết các hiện vật của Hệ điều hành có liên quan đến việc cải thiện hiệu suất. Việc giữ bộ nhớ đệm của các liên kết đến các tập tin được sử dụng gần đây nhất sẽ làm tăng tốc hoạt động nếu người dùng quay lại công việc trước đó, và đây là một nhiệm vụ rất phổ biến. Ngoài ra, việc xóa tác phẩm (một

tập tin) không xóa đi các hiện vật liên quan. Do đó, các hiện vật vẫn có thể tồn tại sau khi tập tin đã biến mất, để lại bằng chứng cho thấy tập tin đó có tồn tại.

---



**MÁCH NƯỚC CHO KỲ THI** Hiện vật là những phần tử dữ liệu quan trọng được sử dụng để trong các cuộc điều tra pháp y. Chúng được kết nối tới cách thức mà máy tính quản lý dữ liệu để thực hiện một tác vụ. Đảm bảo chọn đúng hiện vật có liên quan một cách cụ thể và trực tiếp đến câu hỏi, không phải nằm ở ngoại vi.

### Tại-chỗ so với Đám mây

Đám mây đã trở thành một nguồn tài nguyên cho các hệ thống CNTT của doanh nghiệp, và do đó, nó có liên quan mật thiết đến cả khám-phá-điện-tử và điều tra pháp y. Việc có dữ liệu có thể hoặc không thể truy cập được một cách trực tiếp bằng các công cụ khám phá điện tử và pháp y có thể làm phức tạp thêm các quy trình cần thiết. Một vấn đề phức tạp nữa là các vấn đề pháp lý liên quan đến các hợp đồng giữa tổ chức và nhà cung cấp đám mây. Vì cả điều tra pháp y và khám phá điện tử đều là các quy trình thứ cấp từ góc độ kinh doanh, nên chúng có thể hoặc không thể được xác định trong một thỏa thuận đám mây tiêu chuẩn. Bởi vì các quy trình này có thể trở nên quan trọng - và nếu đúng, có thể đã quá muộn để giải quyết chúng theo hợp đồng - nên tổ chức cần phải chuẩn bị bằng cách xác định chúng trong các thỏa thuận đám mây với bên thứ ba.

Các vấn đề liên quan đến *tại-chỗ so với đám mây* liên quan đến điều tra pháp y là một trong những vấn đề bị chỉ phơi bởi quyền truy cập. Khi quá trình lưu trữ hoặc điện toán đang diễn ra trên nền tảng điện toán của một bên khác, chẳng hạn như trong đám mây, cho dù thực tế tại một địa

điểm khác hay tại chỗ, quyền truy cập bị chi phối bởi các hợp đồng và thỏa thuận liên quan đến mối quan hệ.

### **Các Điều khoản về Quyền Kiểm toán**

Các cuộc kiểm toán là cơ chế được sử dụng để xác minh rằng các hệ thống đang hoạt động với các mức mục đích, bảo mật và hiệu quả đã được thiết kế của chúng. Khả năng kiểm toán liên quan đến quyền truy cập vào một hệ thống và dữ liệu. Khi thông tin được lưu trữ hoặc xử lý trên đám mây, người dùng cần có được khả năng kiểm toán nhà cung cấp đám mây. Mức độ và phạm vi kiểm toán có thể khác nhau tùy theo bản chất động của cả đám mây và môi trường các quy định, nhưng có một điều sẽ không thay đổi. Chỉ có các quyền mà khách hàng có sẽ được nêu chi tiết trong các thỏa thuận/hợp đồng cấp dịch vụ với nhà cung cấp dịch vụ đám mây. Điều này khiến cho *điều khoản Quyền Kiểm toán* trở thành yêu cầu quan trọng của bất kỳ thỏa thuận mức dịch vụ nào và tính cụ thể của nó cần phải phù hợp với phạm vi hoạt động và quy định của tương tác đám mây.

### **Quy định/Quyền tài phán**

Dù là tại chỗ hay trên mây, sẽ có những trường hợp khi các hành động thực thi pháp luật hoặc quy định làm phát sinh những vấn đề về quyền tài phán. Nếu bạn có dữ liệu phát triển phần mềm của bạn trên đám mây, và các máy chủ/thành phần lưu trữ đang đặt ở một quốc gia nước ngoài, luật của ai sẽ được áp dụng? Điều quan trọng là phải tham vấn ý kiến cố vấn pháp lý của công ty để tìm hiểu sự phân nhánh của vị trí [lưu trữ] dữ liệu liên quan đến điều tra pháp y và việc sử dụng dữ liệu sau này.

### **Luật Thông báo Vi phạm Dữ liệu**

Những *luật thông báo về sự vi phạm dữ liệu* được đề cập chi tiết trong Chương 35, "Quyền riêng tư", nhưng đáng được đề cập đến trong cuộc thảo luận của chúng ta về điều tra pháp y vì việc phát hiện ra sự vi phạm

có thể xảy ra trong quá trình khám nghiệm pháp y. Rất nhiều cuộc điều tra pháp y liên quan đến hành vi trộm cắp tài sản trí tuệ, và cũng rất nhiều lần vi phạm dữ liệu được bảo vệ theo luật bảo mật quyền riêng tư.

## Tính toàn vẹn

*Tính toàn vẹn* là một khái niệm cực kỳ quan trọng trong bảo mật bởi vì nó đề cập đến tính xác thực của một phần tử dữ liệu. Đã có sự thay đổi trái phép đối với một phần tử hay người ta có thể tin tưởng vào giá trị hiện tại của phần tử đó không? Điều này hoạt động tốt như một khái niệm, nhưng làm thế nào để điều này thực sự được khởi tạo trong một hệ thống? Nó được thực hiện thông qua việc sử dụng các hàm băm mật mã, tổng kiểm tra và nguồn gốc xuất xứ của dữ liệu. Việc quản lý các phần tử này dựa vào các chức năng khác của hệ thống, nhưng nếu người ta có thể xác thực được một phần tử dữ liệu đến từ đâu (xuất xứ) và nó không bị thay đổi (giá trị băm) thì người ta có thể cho rằng tính toàn vẹn của nó là nguyên vẹn.

## Băm

Nếu các tập tin, nhật ký và thông tin khác sẽ được thu thập và sử dụng làm bằng chứng, bạn cần đảm bảo rằng dữ liệu đã không bị sửa đổi. Trong hầu hết các trường hợp, một công cụ để triển khai thuật toán băm để tạo ra các tóm tắt thông điệp sẽ được sử dụng.

Một *thuật toán băm* thực hiện một chức năng tương tự như các bit chẵn lẻ quen thuộc, kiểm tra tổng hoặc kiểm tra dư thừa theo chu kỳ (cyclic redundancy check - CRC). Nó áp dụng các phép toán cho một dòng dữ liệu (hoặc tập tin) để tính toán một số con số là duy nhất dựa trên thông tin có trong dòng dữ liệu (hoặc tập tin). Nếu một hàm băm tiếp theo được tạo trên cùng một dòng dữ liệu dẫn đến một giá trị băm khác thì điều đó thường có nghĩa là dòng dữ liệu đã bị thay đổi.

Toán học đứng sau các thuật toán băm đã được nghiên cứu một cách rộng rãi, và mặc dù có thể hai luồng dữ liệu khác nhau có thể tạo ra cùng một bản tóm tắt thông điệp, nhưng điều đó rất không chắc chắn sẽ có thể xảy ra. Đây là một lĩnh vực mật mã đã được xem xét một cách nghiêm ngặt và các yếu tố toán học đứng sau Tóm tắt Thông điệp 5 (Message Digest 5 - MD5) và Thuật toán Băm An toàn (Secure Hash Algorithm - SHA) là rất tốt. Vào năm 2005, những điểm yếu đã được phát hiện trong thuật toán MD5 và SHA, khiến Viện Tiêu chuẩn và Công nghệ Quốc gia Hoa Kỳ (NIST) đã thông báo về một cuộc thi để tìm ra một thuật toán băm mật mã mới, được đặt tên là SHA-3. SHA-3 đã được NIST thông qua vào năm 2015 và có cấu trúc bên trong khác với các phiên bản tiền nhiệm, khiến nó trở nên mạnh mẽ hơn. Mặc dù MD5 vẫn được sử dụng, thực tiễn tốt nhất là sử dụng dòng SHA-2 và SHA-3 khi nó được tích hợp vào các công cụ.

Công cụ băm được áp dụng cho từng tập tin hoặc nhật ký và giá trị tóm tắt thông điệp được lưu ý trong tài liệu điều tra. Thực tế tốt là bạn nên ghi nhật ký vào các phương tiện ghi một lần như CD-ROM. Nếu vụ án thực sự được đưa ra xét xử, các điều tra viên có thể cần chạy lại công cụ trên các tập tin hoặc nhật ký để cho thấy rằng chúng đã không bị thay đổi theo bất kỳ cách nào.



**LƯU Ý** Số lượng các tập tin được lưu trữ trên các ổ cứng ngày nay có thể rất lớn - hàng trăm nghìn tập tin, theo đúng nghĩa đen. Rõ ràng, số lượng này là quá nhiều để các điều tra viên phân tích. Tuy nhiên, bằng cách đổi chiều các tóm tắt thông điệp đối với các tập tin được cài đặt bởi các sản phẩm phần mềm phổ biến nhất với các tóm tắt thông điệp của các tập tin trên ổ đĩa đang được phân tích, các điều tra viên có thể

tránh được việc phân tích khoảng 90% các tập tin vì anh ta có thể cho rằng chúng chưa được sửa đổi. Thư viện Tham chiếu Phần mềm Quốc gia Hoa Kỳ (National Software Reference Library - NSRL) thu thập phần mềm từ nhiều nguồn khác nhau và kết hợp các cấu hình tập tin thành Bộ Dữ liệu Tham chiếu (Reference Data Set - RDS) có sẵn để tải xuống dưới dạng dịch vụ (xem [www.nsrl.nist.gov](http://www.nsrl.nist.gov)).

---



**LƯU Ý** Băm được sử dụng trong toàn bộ quá trình điều tra pháp y để đo lường tính toàn vẹn giữa các bản sao của dữ liệu. Kiểm tra tổng không có nét đặc trưng của các hàm băm, do đó các hàm băm là công cụ chính.

### **Checksums**

Kiểm tra tổng là những thuật toán toán học để tạo ra một con số kiểm tra dựa trên một luồng đi vào. Được thiết kế để kiểm tra các lỗi trong các tập dữ liệu nhỏ, chúng có cả những ưu và nhược điểm. Một ưu điểm là đối với việc kiểm tra lỗi, chúng khá nhanh và có thể phát hiện phân tích chiến lược một lỗi bit-đơn. Một nhược điểm là chúng bỏ sót một lượng lớn các lỗi vì một lỗi thứ hai có thể hủy bỏ tác động của lỗi thứ nhất trên một kiểm tra tổng. Do đó, các kiểm tra tổng không có mục đích thực tế trong các cuộc điều tra pháp y kỹ thuật số. Nếu hai kiểm tra tổng khác nhau, các luồng dữ liệu đi vào là khác nhau. Nếu các kiểm tra tổng là giống nhau, bạn vẫn có thể có các luồng dữ liệu khác nhau.

### **Nguồn gốc**

Nguồn gốc là một tham chiếu đến xuất xứ của dữ liệu. Trong trường hợp điều tra pháp y kỹ thuật số, sẽ là không đủ khi trình bày một phần tử dữ liệu cụ thể như là "bằng chứng, người ta cũng phải thể hiện nguồn gốc của nó. Nguồn gốc phải cụ thể, như ở đâu trên cấu trúc tập tin và vị trí

trên thiết bị, trong hầu hết các trường hợp, sẽ có nhiều cách trình bày, như trong cấu trúc tập tin liên quan đến nơi tập tin đang lưu trú và liên quan đến Hệ điều hành (logic) và vị trí của nó trên ổ đĩa vật lý trong các sector (vật lý). Nguồn gốc liên quan đến siêu dữ liệu, có thể bao gồm dấu thời gian, thông tin kiểm soát truy cập và một loạt những dữ liệu khác để có thể hỗ trợ cho việc xác định người dùng đã thực hiện hành động nào vào thời điểm nào có liên quan đến đối tượng. Trong hầu hết các trường hợp, không có một vị trí duy nhất cho bằng chứng này, giống như dòng thời gian, nó phải được xây dựng từ một số hiện vật khác nhau.

## Bảo quản

Khi thông tin hoặc đối tượng được trình bày cho ban quản lý hoặc được đệ trình cho tòa án để hỗ trợ cho một yêu cầu bồi thường thì thông tin hoặc các đối tượng đó có thể được coi là bằng chứng hoặc tài liệu hỗ trợ cho những nỗ lực điều tra của bạn. Quản lý cấp cao sẽ luôn hỏi rất nhiều câu hỏi – những câu hỏi bậc hai và bậc ba mà bạn cần có thể trả lời nhanh chóng. Tương tự như vậy, trong phiên tòa, sự tín nhiệm là rất quan trọng. Do đó, bằng chứng phải được thu thập, xác định, và bảo vệ một cách thích hợp để chống lại sự giả mạo, vận chuyển và lưu trữ.

Một trong những yếu tố quan trọng trong việc bảo quản [bằng chứng] là đảm bảo không có gì bị thay đổi do kết quả của việc thu thập dữ liệu. Nếu máy đang tắt, dừng bật máy lên - các ổ đĩa có thể được chụp ảnh khi máy đang tắt. Việc bật máy lên khiến cho rất nhiều tiến trình sẽ hoạt động và các phần tử dữ liệu bị thay đổi. Khi tạo bản sao pháp y của một đĩa cứng, hãy luôn sử dụng một trình chặn ghi, vì điều này sẽ ngăn chặn mọi sự thay đổi trên phương tiện đang được ghi lại. Việc sao chép thông thường sẽ để lại dấu vết và thay đổi tương ứng, và trình chặn ghi sẽ ngăn chặn những thay đổi này.

Bằng chứng kỹ thuật số có một vấn đề rất lớn và rõ ràng: nó có thể thay đổi và không để lại hồ sơ về sự thay đổi. Thực tế là kết quả của một vụ án có thể phụ thuộc vào thông tin có thể đã được thực hiện không tinh (bị thay đổi) khiến cho hành vi bảo quản trở thành một yếu tố quan trọng trong việc xác định tính xác thực của bằng chứng. Từ bước đầu tiên trong quy trình điều tra pháp y, vấn đề quan trọng nhất luôn phải là  *bảo quản* dữ liệu. Không có sự phục hồi nào từ dữ liệu đã bị thay đổi, vì vậy ngay từ khởi đầu của quá trình thu thập, các biện pháp bảo vệ phải được thực hiện. Có một số bước quan trọng để hỗ trợ điều tra viên pháp y trong việc tránh làm hỏng dữ liệu. Đầu tiên, khi dữ liệu được thu thập, một chuỗi hành trình bảo quản vững chắc được duy trì cho đến khi hoàn thành vụ án và các tài liệu được giải phóng hoặc tiêu hủy. Thứ hai, khi một bản sao dữ liệu pháp y đã được thu thập, một hàm băm cũng đồng thời được thu thập để cho phép xác minh tính toàn vẹn [của dữ liệu]. Mọi phân tích chỉ được thực hiện trên bản sao pháp y của bộ sưu tập dữ liệu gốc chứ không phải trên bản chính. Ngoài ra, mỗi bản sao sẽ được xác minh trước và sau khi kiểm tra bằng cách so sánh các giá trị băm với tập hợp ban đầu để chứng minh tính toàn vẹn [của dữ liệu].

Quá trình này tốn thêm rất nhiều công sức và thời gian cho một cuộc điều tra, nhưng nó mang lại một yếu tố quan trọng - bác bỏ bất kỳ khiếu nại nào cho rằng dữ liệu đã bị thay đổi, giả mạo hoặc bị hư hỏng, theo bất kỳ cách nào. Nếu giá trị băm thay đổi, hành động rất đơn giản: loại bỏ bản sao, tạo ra một bản sao mới và bắt đầu lại quá trình. Quá trình này sẽ thể hiện cho tòa án thấy hai điều quan trọng: quy trình nghiêm ngặt để bảo vệ tính toàn vẹn của dữ liệu và khả năng truy nguyên nguồn gốc thông qua các giá trị băm để chứng minh tính toàn vẹn của dữ liệu và kết quả phân tích thu được từ dữ liệu.



**MÁCH NƯỚC CHO KỲ THI** Việc hiểu được không chỉ về tầm quan trọng của bảo quản dữ liệu mà còn về quá trình đảm bảo nó [quá trình bảo quản dữ liệu] đang sử dụng các giá trị băm là một khái niệm rất có khả năng kiểm tra được.

### **Khám-phá-điện-tử (E-Discovery)**

Khám phá điện tử, hoặc *e-discovery*, là thuật ngữ được sử dụng cho các yêu cầu tạo ra tài liệu và dữ liệu như một phần của khám phá pháp lý trong các vụ kiện dân sự. Khi một vụ kiện dân sự được đệ trình, theo sự phê duyệt của tòa án, một công ty có thể bị buộc phải chuyển những dữ liệu cụ thể từ các hệ thống theo vấn đề pháp lý hiện đang có [*hàm ý chỉ vấn đề đang bị kiện tại tòa án – người dịch*]. Thông tin điện tử được coi là giống với tài liệu giấy ở một số khía cạnh và hoàn toàn khác biệt ở những khía cạnh khác. Giá trị bằng chứng có thể giống hệt nhau. Tính mong manh có thể rất đáng kể - các hồ sơ điện tử có thể bị thay đổi mà không để lại dấu vết. Tài liệu điện tử cũng có thể có siêu dữ liệu tương ứng với tài liệu, chẳng hạn như ai đã chỉnh sửa tài liệu, thông tin về phiên bản trước, v.v...

Một trong những thách thức cấp bách trong kho lưu trữ hồ sơ doanh nghiệp ngày nay là việc duy trì khối lượng thông tin điện tử. Việc theo dõi các kho thông tin dựa trên nhiều cụm từ tìm kiếm là điều thiết yếu để tuân thủ các yêu cầu khám-phá-điện-tử. Thông thường, các hệ thống sử dụng các quy trình và công cụ pháp y để thực hiện các tìm kiếm khám phá điện tử.

### **Khôi phục Dữ liệu**

*Khôi phục* theo nghĩa điều pháp y kỹ thuật số tương ứng với việc xác định thông tin có liên quan cho vấn đề đang có - được nêu một cách đơn giản,

nghĩa là khôi phục bằng chứng liên quan đến một hành động. Nhưng nếu hành động không được biết một cách chính xác thì sao? Ví dụ, giả sử một giám đốc bán hàng của một công ty nghỉ việc và làm việc với một đối thủ cạnh tranh. Vì là giám đốc bán hàng, cô ấy đã có quyền truy cập vào những thông tin nhạy cảm có lợi cho nhà tuyển dụng mới. Nhưng làm thế nào để bạn biết được liệu cô ấy có mang thông tin nhạy cảm đi cùng với mình hay không? Và ngay cả khi cô ấy đã làm vậy, làm thế nào để bạn xác định cho mục đích khôi phục thông tin nào cô ấy đã lấy đi và tìm kiếm những thông tin đó ở đâu? Bởi vì phần mềm pháp y vẫn chưa phát minh ra nút “Tìm Bằng chứng” và không có trường nào trong bất kỳ giao thức máy tính nào để cho các điều tra viên biết được đây là dữ liệu họ đang tìm kiếm, hành động khôi phục thông tin cần thiết có thể là một thách thức đáng kể. Với các ổ đĩa có dung lượng hàng terabyte ngày nay, khối lượng dữ liệu có thể gây ra khó khăn đáng kể.

Việc giao cho điều tra viên pháp y một ổ đĩa 1TB và nói: “Hãy cho tôi biết mọi thứ đã từng xảy ra trên chiếc máy này” tương đương với việc giao cho điều tra viên một nhiệm vụ không-bao-giờ-kết-thúc. Số lượng các sự kiện, tập và tiến trình xảy ra như một phần bình thường của máy tính dẫn đến hàng nghìn sự kiện cho mỗi chu kỳ đăng nhập - làm việc - đăng xuất. Đây không phải là vấn đề mò kim đáy bể, vẫn đề là mò kim đáy bể ở Kansas! Có những cách thức để cắt xén công việc, chẳng hạn như thiết lập các mốc thời gian mà hoạt động đang bị nghi ngờ đã xảy ra, xác định các từ khóa để tìm kiếm các chuỗi thông tin tạo ra một bản ghi có liên quan, và, có lẽ mạnh nhất là để xây dựng một tập dữ liệu vững chắc, xác định chính xác các hành động cụ thể có liên quan đến nhật ký về sự xuất hiện của chúng. Chiến lược thứ hai gắn liền với ý tưởng ghi nhật ký hoạt động, được thảo luận trong phần “Nhật ký sự kiện” trước đó.

## **Không khước từ**

*Không khước từ* là một đặc điểm đề cập đến việc không có khả năng từ chối một hành động đã từng xảy ra. Đây có thể là một vấn đề rất quan trọng trong các giao dịch qua máy tính liên quan đến tiền hoặc những thứ có giá trị khác. Giao dịch có xảy ra không và các bên liên quan có thực sự đã thực hiện giao dịch hay không? Đây là những câu hỏi cốt lõi về sự không khước từ. Bằng cách sử dụng các phần tử mật mã để xác lập danh tính và thông tin đăng nhập, cùng với các giá trị băm để thiết lập tính toàn vẹn, các sự kết hợp thích hợp có thể mang lại kết quả chỉ có thể xảy ra nếu các bên thực sự đã tham gia và sự kiện đã diễn ra. Việc thiết kế và tạo ra các hệ thống cho phép đặc tính này là các yếu tố thiết yếu của các hệ thống đáng tin cậy được sử dụng trong các giao dịch tài chính và các giao dịch khác. Các chi tiết tương tự có thể thu thập được thông qua việc phân tích hoạt động nhất định trên hệ thống kết hợp đăng nhập thành công và chuỗi các hoạt động tiếp theo. Câu hỏi duy nhất là liệu thông tin đăng nhập có còn an toàn hay không. Đây có thể là một câu hỏi chính đáng bởi vì những kẻ tấn công luôn đánh cắp thông tin đăng nhập và sử dụng lại chúng.



## **MÁCH NƯỚC CHO KỲ THI**

Không khước từ là một khái niệm bảo mật quan trọng. Trong thực tế, nó được liệt kê trong hai mục tiêu kỳ thi riêng biệt. Hãy nhớ rằng, nó đề cập đến việc không thể từ chối một hành động đã thực sự xảy ra. Chữ ký điện tử, việc sử dụng nhiều yếu tố xác thực và thậm chí các dấu vết kiểm toán bằng địa chỉ IP là những ví dụ về sự không khước từ và chứng minh hoặc bác bỏ rằng điều gì đó đã thực sự xảy ra.

## Tình báo Chiến lược/Phản gián

*Thu thập thông tin tình báo chiến lược* là việc sử dụng mọi nguồn lực để đưa ra các quyết định. Điều này có thể tạo ra sự khác biệt lớn trong việc liệu một công ty có được chuẩn bị cho các mối đe dọa hay không. Ý tưởng tương tự cũng phù hợp với điều tra pháp y kỹ thuật số. Tình báo chiến lược có thể cung cấp những thông tin giới hạn phạm vi điều tra đến mức có thể quản lý được. Nếu chúng ta có một ý tưởng về các hành động cụ thể mà chúng ta muốn có bằng chứng có thể chứng minh được về việc xảy ra hoặc không xảy ra, chúng ta có thể xây dựng một bộ dữ liệu tình báo chiến lược về thông tin. Nó [thông tin] ở đâu, nó là gì và những gì được phép/không được phép là tất cả những mảnh ghép của thông tin, khi được sắp xếp và phân tích, có thể dẫn đến một kế hoạch ghi-nhật-ký-dữ-liệu để giúp hỗ trợ cho việc nắm bắt sự kiện pháp y. Các sự kiện khác, chẳng hạn như thêm chương trình làm-sạch-dữ-liệu và sau đó xóa chúng, là điều quan trọng cần phải được xem xét. Danh sách các khả năng sẽ rất dài, nhưng cũng giống như thông tin tình báo về mối đe dọa chiến lược, nó vẫn có thể quản lý được, và bằng cách phối hợp làm việc với các công ty và chuyên gia khác chứ không phải riêng lẻ, một kế hoạch có ý nghĩa có thể xuất hiện.

*Thu thập thông tin phản gián* là việc thu thập thông tin nhằm mục tiêu cụ thể đến nỗ lực tình báo chiến lược của một thực thể khác. Việc biết được mọi người đang tìm kiếm gì và họ đang thu thập thông tin gì có thể cung cấp những thông tin về động cơ và các hành động tiềm năng trong tương lai của họ. Việc tạo ra và sử dụng một công cụ sao cho nó không để lại dấu vết cụ thể về vị trí, thời gian hoặc về việc nó được sử dụng cho mục đích gì là một hình thức thu thập phản gián đang thực hiện.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các nguyên tắc của điều tra pháp y kỹ thuật số. Chương mở đầu bằng một cuộc thảo luận về tài liệu và bằng chứng. Trong phần này, các chủ đề về lưu giữ pháp lý, video, khả năng chấp nhận và chuỗi bảo quản bằng chứng đã được đề cập. Thời hạn của các sự kiện, cùng với dấu thời gian và chênh lệch thời gian, đã được trình bày như một công cụ được sử dụng trong phân tích. Phần này kết thúc bằng các thẻ và báo cáo, tiếp theo là các nhật ký sự kiện và các cuộc phỏng vấn.

Phần chính tiếp theo đề cập đến việc thu thập dữ liệu. Chủ đề đầu tiên, thứ tự biến động, tiếp theo là các yếu tố bộ nhớ của đĩa, RAM và tập tin phân trang/hoán đổi. Phần này tiếp tục với thảo luận về hệ điều hành, các thiết bị và firmware. Phần này đã kết thúc bằng ảnh chụp nhanh, bộ nhớ đệm, mạng và hiện vật.

Tiếp theo là một xem xét về tại-chỗ so với đám mây, xem xét các chi tiết cụ thể của các điều khoản Quyền Kiểm toán, các vấn đề về quy định/quyền tài phán và luật thông báo về sự vi phạm dữ liệu. Tiếp theo là tính toàn vẹn, với một cuộc thảo luận về các phương pháp băm, kiểm tra tổng và vấn đề về xuất xứ.

Chương này kết thúc bằng việc đề cập đến bảo quản [bằng chứng], khám-phá-điện-tử, khôi phục dữ liệu, không khước từ và tình báo/phản gián chiến lược.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Vị trí của thông tin biến động chẵng hạn như RAM liên tục thay đổi, và việc thu thập dữ liệu nên diễn ra theo thứ tự biến động hoặc khoảng thời gian của dữ liệu. Thứ tự dưới đây liệt kê từ biến động nhất (nên được thu thập trước tiên) đến ít biến động nhất?

  - A. Các bảng định tuyến, bộ nhớ đệm ARP, các bảng tiến trình, thông kê lỗi (kernel)
  - B. Bộ nhớ (RAM)
  - C. CPU, bộ nhớ đệm, và nội dung registry
  - D. Hệ thống tập tin tạm/không gian hoán đổi.
2. Một phần tử dữ liệu phổ biến sau này sẽ cần thiết trong quá trình điều tra pháp y là thời gian hệ thống chính xác so với nguồn thời gian chính xác bên ngoài. Một bản ghi độ lệch thời gian được tính bằng cách đo thời gian hệ thống với đồng hồ bên ngoài, chẵng hạn như một máy chủ Giao thức Thời gian Mạng (NTP). Điều nào dưới đây phải được coi là có liên quan để có được một bản ghi độ lệch thời gian?

  - A. Bản ghi chênh lệch thời gian có thể bị mất nếu hệ thống bị tắt nguồn, vì vậy tốt nhất nên được thu thập trong khi hệ thống vẫn đang hoạt động.
  - B. Đồng hồ bên trong có thể không được ghi lại ở cùng một mức độ chính xác, vì vậy sự chuyển đổi có thể là cần thiết.
  - C. Thời gian đồng hồ bên ngoài có thể khác biệt trong khoảng từ 2 đến 3 giây, vì vậy tốt nhất nên lấy thời gian từ một số máy chủ NTP để có được kết quả đọc chính xác hơn.

- D.** Việc ghi lại thời gian để theo dõi giờ-công (man-hour) là một yêu cầu pháp lý.
- 3.** Thuật ngữ được sử dụng để mô tả quá trình bao gồm tất cả những người đã xử lý hoặc có quyền truy cập vào một phần bằng chứng là gì?
- A.** Khám-phá-điện-tử an toàn
- B.** Chuỗi bảo quản bằng chứng
- C.** Quy trình giải trình bằng chứng
- D.** Giám hộ bằng chứng.
- 4.** Tiêu chuẩn nào của bằng chứng cho biết bằng chứng phải thuyết phục hoặc đủ tiêu chuẩn mà không có nghi vấn?
- A.** Bằng chứng trực tiếp
- B.** Bằng chứng thích hợp
- C.** Bằng chứng có liên quan
- D.** Bằng chứng đầy đủ.
- 5.** Một thẩm phán đã ra lệnh tất cả các email phải được bảo quản và lệnh đó đang có hiệu lực. Khẳng định nào dưới đây là đúng?
- A.** Bạn có thể xóa email cũ sau khoảng thời gian lưu giữ tiêu chuẩn.
- B.** Bạn nên nhờ bộ phận pháp lý xác định hồ sơ nào phải được lưu lại.
- C.** Bạn nên tiếp tục lưu trữ tất cả email.
- D.** Bạn có thể xóa email sau khi tạo ra một bản sao để lưu lại cho quá trình khám-phá-điện-tử.
- 6.** Loại bằng chứng nào còn được gọi là bằng chứng liên kết hoặc bằng chứng vật chất và bao gồm các đối tượng hữu hình để chứng minh hoặc bác bỏ một sự kiện?
- A.** Bằng chứng trực tiếp
- B.** Bằng chứng thực tế

- C. Bằng chứng tài liệu**
- D. Bằng chứng minh họa.**
- 7.** Bạn đã được giao nhiệm vụ hỗ trợ cho quá trình điều tra pháp y về một sự cố liên quan đến hành vi sai trái của nhân viên. Người giám sát của nhân viên tin rằng bằng chứng về hành vi sai trái này có thể được tìm thấy trên máy đã trộm được giao. Lựa chọn nào sau đây mô tả *đúng nhất* những gì nên được thực hiện?
- A. Tạo ra một dòng thời gian của các sự kiện liên quan đến phạm vi.**
- B. Sao chép hồ sơ người dùng để làm giảm không gian tìm kiếm.**
- C. Đăng nhập với tư cách là người dùng và tìm kiếm thông qua những nỗ lực gần đây của họ.**
- D. Kiểm tra các mục nhập tập tin nhật ký trong hồ sơ của người dùng.**
- 8.** Điều nào dưới đây mà một thu thập video sẽ *không* được sử dụng để thu thập?
- A. Các biển ghi số sê-ri**
- B. Kết nối cáp**
- C. Hình ảnh hệ thống**
- D. Bối cảnh vật lý và sự tồn tại của hệ thống**
- 9.** Điều gì dưới đây thực hiện một chức năng tương tự như chức năng bit chẵn lẻ quen thuộc, kiểm tra tổng hoặc kiểm tra chu kỳ dự phòng?
- A. Bản ghi chênh lệch**
- B. Thuật toán mật mã**
- C. Mã xác thực**
- D. Thuật toán băm**
- 10.** Từ bước đầu tiên trong quá trình điều tra pháp y, vấn đề quan trọng nhất phải luôn luôn là điều gì dưới đây?

- A. Bảo quản dữ liệu**
- B. Chuỗi bảo quản bằng chứng**
- C. Ghi lại tất cả các hành động đã thực hiện**
- D. Chuẩn bị nhân chứng.**

## Đáp án

1. **C, A, B và D.** Các phần tử biến động nhất nên được kiểm tra và thu thập trước tiên và theo thứ tự này.
2. **A.** Bản ghi khoảng thời gian chênh lệch sẽ bị mất nếu hệ thống bị tắt nguồn, vì vậy tốt nhất nên thu thập dữ liệu trong khi hệ thống vẫn đang chạy.
3. **B.** Chuỗi bảo quản bằng chứng giải quyết cho tất cả những người đã xử lý hoặc có quyền truy cập bằng chứng.
4. **D.** *Bằng chứng đầy đủ* cho biết bằng chứng phải thuyết phục hoặc hợp lý mà không bị nghi ngờ. *Bằng chứng trực tiếp* là lời khai chứng minh một sự việc cụ thể (chẳng hạn như lời kể của nhân chứng). Kiến thức về các sự kiện thực tế có được thông qua năm giác quan của nhân chứng, không có suy luận hoặc giả định. *Bằng chứng thích hợp* cho biết bằng chứng phải đủ tiêu chuẩn và đáng tin cậy về mặt pháp lý. *Bằng chứng có liên quan* nêu rõ bằng chứng phải là hiện vật của vụ án hoặc có liên quan đến vấn đề.
5. **C.** Bạn nên tiếp tục lưu trữ tất cả email. Bạn phải tiếp tục tuân thủ lệnh tòa. Việc để cho pháp lý đưa ra quyết định khi lệnh chỉ định "tất cả e-mail" là một sai lầm. Tạo ra bản sao của email chỉ hợp pháp nếu bạn tạo các bản sao bảo mật về mặt pháp y chứ không chỉ là các bản sao lưu.
6. **B.** *Bằng chứng thực tế* còn được gọi là bằng chứng tương ứng hoặc bằng chứng vật chất và bao gồm các đối tượng hữu hình để chứng minh hoặc bác bỏ một sự việc. Bằng chứng vật chất liên kết nghi phạm với hiện trường vụ án. *Bằng chứng trực tiếp* là lời khai chứng minh một sự việc cụ thể (chẳng hạn như lời kể của nhân chứng). Kiến thức về các sự kiện thực tế có được thông qua năm giác quan của nhân chứng, không có suy luận hoặc giả định. Bằng chứng dưới dạng hồ sơ kinh doanh, các bản in, sách hướng

dẫn và các hiện vật tương tự, tạo nên phần lớn bằng chứng liên quan đến tội phạm máy tính, là *bằng chứng tài liệu*. *Bằng chứng minh* được sử dụng để hỗ trợ bồi thẩm đoàn và có thể ở dưới dạng mô hình, thí nghiệm, biểu đồ, v.v..., được cung cấp để chứng minh rằng một sự kiện đã xảy ra.

7. **A.** Phạm vi xác định ranh giới của cuộc điều tra và khung thời gian cho thấy người dùng đã làm gì trong khoảng thời gian phạm vi đó đối với các mục đang được quan tâm.
8. **C.** Một hình ảnh hệ thống là kết xuất của bộ nhớ vật lý của một hệ thống máy tính và sẽ không được ghi lại trong video. Tất cả những nguồn khác đều là nguồn thông tin tĩnh mà một video quay được là có giá trị khi ghi lại.
9. **D.** Một thuật toán băm thực hiện một chức năng tương tự như các bit chẵn lẻ quen thuộc, kiểm tra tổng hoặc kiểm tra dự phòng theo chu kỳ (CRC). Nó áp dụng các phép toán vào một luồng dữ liệu (hoặc tập tin) để tính toán một số con số là duy nhất dựa trên thông tin có trong dòng dữ liệu (hoặc tập tin).
10. A. Mặc dù tất cả những điều này đều quan trọng, nhưng từ bước đầu tiên trong quá trình điều tra pháp y, vẫn đề quan trọng nhất phải luôn là bảo quản dữ liệu.

## Phần V

### Quản trị, Rủi ro và Tuân thủ

- Chương 31 Các Biện pháp kiểm soát Bảo mật
- Chương 32 Các Quy định, Tiêu chuẩn và Khuôn khổ
- Chương 33 Các Chính sách của Tổ chức
- Chương 34 Quản lý Rủi ro
- Chương 35 Quyền Riêng tư

## Chương 31 Các Biện pháp kiểm soát Bảo mật

### Các Biện pháp kiểm soát Bảo mật

Trong chương này bạn sẽ

- Tìm hiểu về ba thể loại kiểm soát bảo mật,
- Khám phá những kiểu kiểm soát bảo mật khác nhau.

Các biện pháp kiểm soát bảo mật là những công cụ được sử dụng để giảm thiểu rủi ro trong doanh nghiệp. Có rất nhiều kiểu kiểm soát bảo mật khác nhau, và chương này xem xét những thể loại và kiểu [kiểm soát bảo mật] khác nhau để cung cấp một phương tiện tìm hiểu và phân loại các biện pháp kiểm soát.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 5.1 của kỳ thi CompTIA Security+: So sánh và đối chiếu các kiểu kiểm soát khác nhau.

## Các Biện pháp kiểm soát Bảo mật

Các *biện pháp kiểm soát bảo mật* là những cơ chế được sử dụng để tối thiểu khả năng tiếp xúc với rủi ro và giảm thiểu những tác động của tổn thất. Bằng cách sử dụng các thuộc tính bảo mật của tính bảo mật, tính toàn vẹn và tính sẵn sàng (CIA) được liên kết với dữ liệu, nhóm bảo mật có trách nhiệm xác định tập hợp các biện pháp kiểm soát thích hợp để đạt được các mục tiêu bảo mật.

Kiểm soát có thể có nhiều thể loại khác nhau, như được mô tả trong chương này. Các thể loại kiểm soát khác nhau không hoạt động như một nguyên tắc phân loại, vì sẽ có các mô tả chồng chéo và một số thể loại kiểm soát được truyền lại từ các chính sách và thủ tục của bên-thứ-ba.



**LƯU Ý** Viện Quốc gia về Tiêu chuẩn và Công nghệ (NIST) cung cấp một danh mục các biện pháp kiểm soát trong loạt NIST SP 800-53 của mình. Bản sửa đổi hiện hành, bản sửa đổi 5, liệt kê hơn 600 biện pháp kiểm soát được nhóm thành 18 thể loại theo chức năng. 18 Thể loại theo chức năng được nhóm thành 3 thể loại lớn: Quản lý, Kỹ thuật và Vận hành. Mặc dù phần lớn các biện pháp kiểm soát này gắn liền với bảo mật điện tử của thông tin, nhưng rất nhiều biện pháp kiểm soát trong số này cũng mở rộng sang thế giới thực.



**MÁCH NƯỚC CHO KỲ THI** Các kiểu biện pháp kiểm soát thường được kiểm tra trong kỳ thi – sự ghi nhớ được khuyến khích.

## Các Thể loại

Ba thể loại kiểm soát bảo mật được chỉ định trong nhiều tài liệu xác định khác nhau và các thể loại này đã trở thành tiêu chuẩn thực tế cho ngành an ninh mạng. Việc sử dụng các *thể loại* phân tách các kiểm soát thành các nhóm tách biệt dựa trên những gì kiểm soát sử dụng làm đòn bẩy của nó: kiểm soát hoạt động quản lý, hoạt động vận hành hoặc kiểm soát kỹ thuật. Từng thể loại này sẽ được mô tả trong các phần sau đây. Đối với một số biện pháp kiểm soát, có thể chúng sẽ có các khía cạnh trải dài hơn một thể loại.

## Quản lý

Các biện pháp kiểm soát *quản lý* là những kiểm soát dựa trên quản lý rủi ro tổng thể. Các biện pháp kiểm soát bảo mật này tập trung vào việc quản lý rủi ro hoặc quản lý hệ thống an ninh mạng. Việc sử dụng kiểm toán an ninh mạng là một ví dụ về kiểm soát quản lý. Bảng 31-1 liệt kê các biện pháp kiểm soát quản lý.

Họ Kiểm soát NIST	Mã định danh
Đánh giá Rủi ro	RA
Lập kế hoạch	PL
Mua lại Hệ thống và các Dịch vụ	SA
Chứng nhận, Công nhận và Đánh giá Bảo mật	CA

**Bảng 31-1** Các Biện pháp kiểm soát Quản lý



**LƯU Ý** Loạt NIST SP 800 đề cập đến các biện pháp kiểm soát thuộc cấp quản lý (managerial) là các biện pháp kiểm soát *quản lý* (management).

### Vận hành

Một biện pháp kiểm soát *vận hành* là một chính sách hoặc thủ tục được sử dụng để giới hạn rủi ro bảo mật. Những biện pháp kiểm soát bảo mật này chủ yếu được triển khai và thực thi bởi con người, trái ngược lại với các hệ thống. Các hướng dẫn cho nhân viên bảo vệ là một ví dụ về kiểm soát vận hành. Bảng 31-2 liệt kê các biện pháp kiểm soát vận hành.

Họ Kiểm soát NIST	Mã định danh
Bảo mật Nhân sự	PS
Bảo vệ Môi trường và Bảo vệ Vật lý	PE
Hoạch định Dự phòng	CP
Quản lý Cấu hình	Quản lý Cấu hình
Bảo trì	MA
Tính toàn vẹn Hệ thống và Thông tin	SI
Bảo vệ Phương tiện	MP
Ứng phó Sự cố	IR
Nâng cao nhận thức và Đào tạo	AT

**Bảng 31-2** Các Biện pháp kiểm soát Vận hành

## Kỹ thuật

Một biện pháp kiểm soát *kỹ thuật* sử dụng một số hình thức công nghệ để giải quyết một vấn đề về bảo mật vật lý. Các biện pháp kiểm soát bảo mật này chủ yếu được triển khai và thực thi bởi hệ thống thông tin thông qua các cơ chế có trong các thành phần phần cứng, phần mềm hoặc phần firmware của nó. Sinh trắc học là một ví dụ về biện pháp kiểm soát kỹ thuật. Bảng 31-3 liệt kê các biện pháp kiểm soát kỹ thuật trong họ NIST.

Họ Kiểm soát NIST	Mã định danh
Nhận diện và Xác thực	IA
Kiểm soát Truy cập	AC
Kiểm toán và Trách nhiệm giải trình	AU
Bảo vệ Hệ thống và Truyền thông	SC

**Bảng 31-3** Các Biện pháp kiểm soát Kỹ thuật



## MÁCH NƯỚC CHO KỲ THI

Sự khác biệt chính giữa các biện pháp kiểm soát vận hành và kỹ thuật là rằng các biện pháp kiểm soát vận hành là những biện pháp kiểm soát mà con người khởi xướng và tuân thủ, trong khi các biện pháp kiểm soát kỹ thuật thường được tự động hóa và liên quan đến sự thực thi của máy móc.

## Các Kiểu Kiểm soát

Các biện pháp kiểm soát cũng có thể được phân loại theo loại *kiểu kiểm soát*. Ngành an ninh mạng công nhận một số kiểu kiểm soát khác nhau và trong khi các loại này có thể mang tính mô tả, chúng không phải là một phép phân loại vì chúng không nhất thiết là độc quyền. Các biện

pháp kiểm soát có thể phù hợp với nhiều loại, tùy thuộc vào việc triển khai và sử dụng. Khóa cửa là một ví dụ về cả kiểm soát vật lý và kiểm soát ngăn chặn.

### **Ngăn chặn**

Một *biện pháp kiểm soát ngăn chặn (preventative)* là một biện pháp ngăn chặn những hành động cụ thể xảy ra, chẳng hạn như một bầy người sẽ ngăn chặn hành động theo đuôi (tailgating). Các biện pháp kiểm soát ngăn chặn hoạt động trước một sự kiện và ngăn cản nó tiến triển. Tường lửa là một ví dụ về biện pháp kiểm soát ngăn chặn, vì nó có thể chặn quyền truy cập vào một tài nguyên cụ thể.



**MÁCH NƯỚC CHO KỲ THI** Yếu tố quan trọng để vượt qua Mục tiêu Kỳ thi 5.1 là khả năng so sánh và đối chiếu các kiểu kiểm soát khác nhau. Chúng giống nhau như thế nào (so sánh) và chúng khác nhau như thế nào (đối chiếu)? Việc hiểu được sự khác biệt có thể sẽ rất tinh tế. Ví dụ, các luật với những hình phạt, nếu được thực thi, có ngăn chặn được các cuộc tấn công không? Luật pháp có thể ngăn chặn những kẻ tấn công, nhưng luật pháp không ngăn cản những kẻ tấn công sẽ tấn công nếu biện pháp ngăn chặn không ngăn cản chúng quyết định tấn công.

### **Phát hiện**

*Biện pháp kiểm soát phát hiện (detective)* là một biện pháp kiểm soát tạo điều kiện thuận lợi cho việc phát hiện một vi phạm bảo mật vật lý. Biện pháp kiểm soát phát hiện hoạt động trong một sự kiện, cảnh báo các nhân viên vận hành về các điều kiện cụ thể. Báo động là những ví dụ phổ biến về biện pháp kiểm soát phát hiện. IDS là một ví dụ về cảnh báo bảo mật CNTT phát hiện các hành vi xâm nhập.

## **Khắc phục**

Một *biện pháp kiểm soát khắc phục (corrective)* được sử dụng sau một sự kiện [*nghĩa là khi một sự kiện đã thực sự xảy ra*], với nỗ lực giảm thiểu mức độ thiệt hại. Các bộ cân bằng tải và hệ thống dự phòng hoạt động để giảm rủi ro từ việc quá tải hệ thống và do đó là các biện pháp kiểm soát khắc phục. Bản sao lưu là một ví dụ điển hình về kiểm soát khắc phục, vì chúng có thể tạo điều kiện cho việc khôi phục lại hoạt động một cách nhanh chóng.

## **Răn đe**

Một *biện pháp kiểm soát mang tính răn đe (deterrent)* có tác dụng làm nản lòng kẻ tấn công bằng cách làm giảm thiểu khả năng thành công từ quan điểm của kẻ tấn công. Bất kỳ biện pháp kiểm soát nào làm gia tăng chi phí cho kẻ tấn công đều là kiểm soát mang tính răn đe. Một ví dụ sẽ là các đạo luật và quy định làm tăng hình phạt, tăng rủi ro và chi phí cho kẻ tấn công. Một ví dụ khác là việc sử dụng việc trộn muối để băm mật khẩu để gia tăng chi phí xây dựng bảng cầu vồng.

## **Bù đắp**

Một *biện pháp kiểm soát bù đắp (compensating)* là biện pháp kiểm soát được sử dụng để đáp ứng một yêu cầu khi không có biện pháp kiểm soát nào để giải quyết mối đe dọa một cách trực tiếp. Hệ thống chữa cháy không ngăn chặn được thiệt hại do hỏa hoạn, nhưng nếu được sử dụng đúng cách, chúng có thể giảm thiểu hoặc hạn chế mức độ thiệt hại do hỏa hoạn gây ra.



## **MÁCH NƯỚC CHO KỲ THI**

Năm kiểu kiểm soát trước đây có khuynh hướng loại trừ lẫn nhau – chúng mô tả các điểm tương tác của biện pháp kiểm soát với các công cụ, kỹ thuật và quy trình của kẻ tấn công.

## Vật lý

Một *biện pháp kiểm soát vật lý (physical)* là biện pháp kiểm soát ngăn chặn các hành động vật lý cụ thể xảy ra, chẳng hạn như một bầy người ngăn cản việc theo đuôi (tailgating). Các biện pháp kiểm soát vật lý ngăn cản sự tương tác cụ thể của con người với một hệ thống và chủ yếu được thiết kế để ngăn chặn hoạt động ngẫu nhiên của một thứ gì đó. Các biện pháp kiểm soát vật lý hoạt động trước một sự kiện, ngăn chặn sự kiện đó thực sự xảy ra. Ví dụ như việc sử dụng nắp che trên các nút quan trọng, cũng như nút "DỪNG" lớn màu đỏ, được định vị để có thể dễ dàng tiếp cận. Cái trước dừng việc kích hoạt không cõi ý, trong khi cái sau tạo điều kiện kích hoạt dễ dàng trong trường hợp khẩn cấp. Để biết thêm thông tin, Chương 15, "Bảo mật Vật lý", có một phần dành cho các biện pháp kiểm soát bảo mật vật lý.



## MÁCH NƯỚC CHO KỲ THI

Các biện pháp kiểm soát vật lý tách biệt với các mô tả trước đây và có thể được sử dụng một cách độc lập với chúng. Có thể có một biện pháp kiểm soát đồng thời là biện pháp kiểm soát kỹ thuật, vật lý và ngăn chặn (ví dụ, khóa cửa).

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với các *thể loại* và *kiểu* kiểm soát bảo mật khác nhau. Các biện pháp kiểm soát bảo mật được chia thành ba thể loại: quản lý, vận hành và kỹ thuật. Kiểm soát bảo mật cũng có thể được phân loại theo kiểu kiểm soát. Các kiểu kiểm soát khác nhau được đề cập đến trong chương bao gồm ngăn chặn, phát hiện, khắc phục, răn đe, bù đắp và vật lý.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy xem xét những từ *thể loại* và *kiểu* trong câu hỏi. Các thể loại là quản lý, vận hành và kỹ thuật. Các kiểu bao gồm ngăn chặn, phát hiện, khắc phục, răn đe, bù đắp và vật lý.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Kiểu biện pháp kiểm soát bảo mật nào được sử dụng sau khi sự kiện xảy ra, trong một nỗ lực nhằm giảm thiểu mức độ thiệt hại?

  - A. Răn đe
  - B. Khắc phục
  - C. Ngăn chặn
  - D. Phát hiện.
2. Kiểu kiểm soát bảo mật nào được sử dụng để đáp ứng một yêu cầu khi yêu cầu đó không thể được đáp ứng trực tiếp?

  - A. Ngăn chặn
  - B. Vật lý
  - C. Răn đe
  - D. Bù đắp
3. Việc sử dụng một bài kiểm nghiệm xâm nhập để xác định các lỗ hổng là một ví dụ về loại kiểm soát nào?

  - A. Vận hành
  - B. Bên ngoài
  - C. Quản lý
  - D. Kỹ thuật
4. Việc sử dụng các ổ khóa kết hợp như một thủ tục kiểm soát bảo mật để hạn chế rủi ro bảo mật vật lý là một ví dụ về thể loại kiểm soát nào?

  - A. Vật lý
  - B. Kỹ thuật
  - C. Vận hành

**D. Khắc phục**

5. Một bẫy người là một ví dụ về loại kiểm soát bảo mật nào? (Chọn tất cả các đáp án đúng).
- A. Vật lý  
B. Khắc phục  
C. Hành chính  
D. Ngăn chặn
6. Điều nào dưới đây *không* phải là một thể loại kiểm soát bảo mật?
- A. Con người  
B. Quản lý  
C. Kỹ thuật  
D. Vận hành
7. Thể loại kiểm soát nào có nhiều khả năng được tự động hóa nhất?
- A. Khắc phục  
B. Kỹ thuật  
C. Vận hành  
D. Bù đắp
8. Không có cách nào để trực tiếp phát hiện và ứng phó với một mối đe dọa cụ thể. Kiểu kiểm soát tốt nhất để sử dụng cho trường hợp này là gì?
- A. Kỹ thuật  
B. Khắc phục  
C. Ngăn chặn  
D. Bù đắp
9. Một hệ thống phát hiện xâm nhập là một ví dụ về kiểu kiểm soát nào?
- A. Phát hiện  
B. Kỹ thuật  
C. Bù đắp

**D. Vận hành**

**10.** Thể loại kiểm soát nào sau đây là nhanh nhất khi ứng phó với một mối đe dọa đã biết?

- A. Vận hành**
- B. Kỹ thuật**
- C. Hành chính**
- D. Quản lý**

## Đáp án

1. **B.** Các biện pháp kiểm soát khắc phục được sử dụng sau sự kiện, với nỗ lực giảm thiểu mức độ thiệt hại. Một biện pháp kiểm soát mang tính răn đe nhằm tác động đến kẻ tấn công bằng cách làm giảm khả năng thành công [*từ quan điểm của kẻ tấn công*]. Biện pháp kiểm soát phòng ngừa là kiểm soát ngăn chặn các hành động cụ thể xảy ra. Biện pháp kiểm soát phát hiện là một kiểm soát tạo điều kiện thuận lợi cho việc phát hiện ra một vi phạm bảo mật.
2. **D.** Biện pháp kiểm soát bù đắp là biện pháp kiểm soát được sử dụng để đáp ứng một yêu cầu khi yêu cầu đó không thể được đáp ứng một cách trực tiếp. Hệ thống chữa cháy không ngăn chặn được thiệt hại do hỏa hoạn, nhưng nếu được sử dụng đúng cách, chúng có thể giảm thiểu hoặc hạn chế mức độ thiệt hại do hỏa hoạn gây ra. Một biện pháp kiểm soát ngăn chặn là biện pháp kiểm soát ngăn chặn các hành động cụ thể xảy ra. Một biện pháp kiểm soát vật lý là biện pháp kiểm soát ngăn chặn các hành động vật lý cụ thể xảy ra, chẳng hạn như một bẫy người ngăn cản việc theo đuôi (tailgating). Một biện pháp kiểm soát mang tính răn đe nhằm tác động đến kẻ tấn công bằng cách làm giảm khả năng thành công.
3. **C.** Kiểm nghiệm xâm nhập là một hình thức đánh giá rủi ro và do đó là một hành động quản lý, vì nó tư vấn cho cấp quản lý về tình hình rủi ro hiện tại có liên quan đến hệ thống.
4. **C.** Kiểm soát vận hành là một chính sách hoặc thủ tục được sử dụng để hạn chế rủi ro bảo mật. Từ khóa trong câu hỏi là *thể loại*.
5. **A** và **D.** Có khả năng là một biện pháp kiểm soát bảo mật cụ thể sẽ thuộc nhiều kiểu. Bởi vì bẫy người là một rào cản vật lý ngăn cản việc theo đuôi nên nó vừa là một biện pháp kiểm soát vật lý vừa là một biện pháp kiểm soát ngăn chặn. Các biện pháp kiểm

soát khắc phục được sử dụng sau sự kiện, với nỗ lực giảm thiểu mức độ thiệt hại. Một sự kiểm soát hành chính chỉ đơn giản là một tác nhân gây xao nhãng.

6. **A.** Con người không phải là một phạm trù được xác định của kiểm soát bảo mật. Kiểm soát bảo mật hoạt động thông qua hành động của mọi người được gọi là kiểm soát vận hành.
7. **B.** Các biện pháp kiểm soát kỹ thuật có nhiều khả năng được tự động hóa nhất vì chúng dựa trên máy móc.
8. **D.** Các biện pháp kiểm soát bù đắp được sử dụng khi không có cách trực tiếp để giải quyết rủi ro.
9. **A.** Từ khóa trong câu hỏi là *kiểu*, khiến [biện pháp kiểm soát] phát hiện là đáp án chính xác. Nếu câu hỏi đặt ra cho thể loại thì đáp án chính xác sẽ là kỹ thuật.
10. **B.** Các biện pháp kiểm soát kỹ thuật có thể được tự động hóa và do đó có thể ứng phó nhanh nhất khi có sự cố.

## Chương 32 Các Quy định, Tiêu chuẩn và Khuôn khổ

### Các Quy định, Tiêu chuẩn và Khuôn khổ

Trong chương này bạn sẽ

- Xem xét các quy định, tiêu chuẩn và luật lệ về bảo mật có thể áp dụng được,
- Khám phá những khuôn khổ chính được sử dụng trong bảo mật,
- Tìm hiểu về các điểm chuẩn đối sánh liên-quan-đến-bảo-mật quan trọng và các hướng dẫn thiết lập cấu hình an toàn.

Việc phát triển một bộ các chính sách, thủ tục và hoạt động thích hợp để đạt được mức độ bảo mật tổ chức mong muốn là một tập hợp bao gồm các nhiệm vụ phức tạp với rất nhiều sự phụ thuộc qua lại lẫn nhau. Để hỗ trợ tổ chức trong việc phát triển và triển khai những kế hoạch này là một loạt các quy định, tiêu chuẩn và khuôn khổ có thể có tác động đến toàn cảnh bảo mật của tổ chức. Chương này khám phá những nguồn thông tin này và xem xét cách thức chúng có thể được triển khai như thế nào.

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 5.2 của kỳ thi CompTIA Security+: Diễn giải về tầm quan trọng của các quy định, tiêu chuẩn hoặc khuôn khổ có tác động đến toàn cảnh bảo mật của tổ chức.

## Các Quy định, Tiêu chuẩn và Luật lệ

Hoạt động kinh doanh không bao giờ diễn ra trong môi trường chân không, ít nhất luôn có một số chính sách và thủ tục phải tuân theo. Tuy nhiên các chính sách và thủ tục này được định hướng từ các quy định, tiêu chuẩn và luật lệ. Luật lệ do các cơ quan lập pháp của chính phủ đưa ra nhằm tạo ra một loạt các điều kiện và hình phạt cụ thể. Các cơ quan chính phủ xây dựng và ban hành các quy định để triển khai các luật lệ. Các tiêu chuẩn là tập hợp các thông số kỹ thuật được-xây-dựng-trên-cơ-sở-đồng-thuận cho các sản phẩm, dịch vụ hoặc hệ thống. Một loạt các cơ quan khác nhau tạo ra các tiêu chuẩn, và dù gì đi chăng nữa thì việc ai đó muốn tuân theo chúng hay không là một quyết định kinh doanh. Luật pháp và các quy định phải được tuân thủ, nếu không, những hậu quả đã được quy định bên trong chúng có thể sẽ được viện dẫn bởi các cơ quan chính phủ.

## Đạo luật Bảo vệ Dữ liệu Chung (GDPR)

Quy định Chung về Bảo vệ Dữ liệu (General Data Protection Regulation - GDPR), vốn là tái bản được viết lại sâu và rộng hơn của các quy định về quyền riêng tư của Châu Âu, có hiệu lực vào tháng 5 năm 2018. GDPR mở ra một thế giới hoàn toàn mới liên quan đến bảo vệ dữ liệu và quyền riêng tư. Với việc thương mại toàn cầu là quan trọng đối với tất cả các quốc gia và thực tế là thương mại phụ thuộc vào việc chuyển giao thông tin, bao gồm cả dữ liệu cá nhân, khả năng truyền dữ liệu - bao gồm cả dữ liệu cá nhân - giữa các bên đã trở nên quan trọng đối với thương mại. Được quy định trong Hiến chương về các Quyền Cơ bản của Liên minh Châu Âu (EU) là quyền cơ bản để bảo vệ dữ liệu cá nhân, bao gồm cả khi các phần tử dữ liệu đó được chuyển ra ngoài Liên minh Châu Âu. Nhận thức được điều đó, bộ quy định mới có tính mở rộng và hạn chế hơn, khiến cho các điều khoản của Luật che giấu An toàn (Safe Harbor) trở nên lỗi thời. Đối với tất cả các công ty muốn giao dịch thương mại với

EU, hiện có một bộ quy định về quyền riêng tư sẽ yêu cầu các chương trình cụ thể để giải quyết các yêu cầu.

GDPR mang lại rất nhiều thay đổi - một là việc bổ nhiệm Cán bộ Bảo vệ Dữ liệu (Data Protection Officer - DPO). Vai trò này có thể được đảm nhận bởi một nhân viên hoặc nhà cung cấp dịch vụ bên-thứ-ba (ví dụ: công ty tư vấn hoặc luật) và phải là người báo cáo trực tiếp cho cấp quản lý cao nhất. DPO nên hoạt động với tính độc lập đáng kể và các điều khoản trong GDPR hạn chế quyền kiểm soát đối với DPO đối với cấp quản lý.

## GDPR

GDPR yêu cầu những cân nhắc đáng kể, bao gồm:

- Đánh giá luồng dữ liệu từ EU đến Hoa Kỳ để xác định phạm vi và quy mô của thách thức tuân-thủ-quyền-riêng-tư xuyên-biên-giới.
- Đánh giá mức độ sẵn sàng để đáp ứng các điều khoản của mô hình, khắc phục những lỗ hổng và tổ chức kiểm toán việc tuân thủ các điều khoản.
- Cập nhật các chương trình về quyền riêng tư để đảm bảo chúng có khả năng vượt qua cuộc kiểm toán của cơ quan quản lý của Liên minh Châu Âu.
- Tiến hành các bài kiểm tra cảng thẳng về thông báo vi-phạm-dữ-liệu của EU.
- Giám sát những thay đổi trong sự hỗ trợ của EU đối với các hợp đồng mẫu và các quy tắc ràng buộc của công ty.

GDPR chỉ định rõ các yêu cầu liên quan đến sự đồng thuận, và chúng mạnh mẽ hơn một cách đáng kể so với các quy định trước đây. Các yêu cầu về sự đồng thuận cũng được mô tả cho các trường hợp cụ thể như dưới đây:

- Sự đồng thuận được thông báo/xác nhận đối với việc xử lý dữ liệu. Cụ thể, “một tuyên bố hoặc một hành động khẳng định rõ ràng” từ chủ thể của dữ liệu phải được “đưa ra một cách tự do, cụ thể, sáng suốt và rõ ràng”.
- Sự đồng thuận rõ ràng để xử lý các thể loại dữ liệu đặc biệt. Sự đồng thuận rõ ràng là bắt buộc đối với “các thể loại đặc biệt” của dữ liệu, chẳng hạn như dữ liệu di truyền, dữ liệu sinh trắc học và dữ liệu liên quan đến khuynh hướng tình dục.
- Sự đồng thuận rõ ràng của cha mẹ đối với dữ liệu cá nhân của trẻ em.
- Sự đồng thuận phải cụ thể đối với từng hoạt động xử-lý-dữ-liệu và chủ thể dữ liệu có thể rút lại sự đồng thuận bất cứ lúc nào.

GDPR cung cấp các biện pháp bảo vệ các quyền mới của cá nhân và những quyền này có thể buộc các công ty phải áp dụng các chính sách mới để giải quyết các yêu cầu này. Các quyền bao gồm Quyền đối với Thông tin, Quyền Truy cập, Quyền Chính sửa, Quyền Hạn chế Xử lý, Quyền Phản đối, Quyền Xóa và Quyền Khả năng Di chuyển dữ liệu (Right to Information, Right to Access, Right to Rectification, Right to Restrict Processing, Right to Object, Right to Erasure, Right to Data Portability). Mỗi quyền này được xác định một cách rõ ràng với các chi tiết kỹ thuật cụ thể trong GDPR. GDPR cũng ghi nhận những rủi ro của việc truyền tải dữ liệu quốc tế cho các bên khác và đã bổ sung thêm các yêu cầu cụ thể rằng các vấn đề bảo vệ dữ liệu phải được giải quyết bằng những biện pháp bảo vệ thích hợp, bao gồm Quy tắc Ràng buộc của Công ty (Binding Corporate

Rules - BCR), Điều khoản Hợp đồng Mẫu (Model Contract Clauses - MCC), còn được gọi là Các điều khoản Hợp đồng Tiêu chuẩn (Standard Contractual Clauses - SCC), và các tài liệu ràng buộc về mặt pháp lý. Các công cụ này phải có hiệu lực thi hành giữa các cơ quan hoặc cơ quan công quyền, cũng như tất cả những người xử lý dữ liệu.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy nhớ rằng Đạo luật Bảo vệ Dữ liệu Chung (GDPR) chỉ định các yêu cầu đối với việc thu thập thông tin cá nhân trong Liên minh Châu Âu (EU).

### **Các Luật lệ của Quốc gia, Vùng lãnh thổ và Tiểu bang**

Luật pháp là hệ thống các quy tắc, hoặc quy chế, được đưa ra bởi chính phủ của một quốc gia, tiểu bang hoặc thành phố. Các quy chế được ban hành bởi một cơ quan lập pháp và sau đó được ký bởi quan chức cấp cao (tổng thống/thống đốc). Có rất nhiều luật lệ từ cấp quốc gia và tiểu bang có liên quan đến an ninh mạng. Với sự ra đời của các kết nối mạng toàn cầu và sự gia tăng của Internet như một phương thức kết nối máy tính giữa các gia đình, các doanh nghiệp và chính phủ trên toàn cầu, một loại tội phạm mới có thể được thực hiện. Xâm nhập máy tính là sự xâm nhập trái phép vào hệ thống máy tính thông qua bất kỳ phương tiện nào, bao gồm cả các kết nối mạng từ xa. Những tội phạm này đã đưa ra một lĩnh vực luật lệ mới có cả hậu quả thuộc quốc gia và quốc tế. Đối với các vụ phạm tội được thực hiện trong biên giới của một quốc gia, luật quốc gia sẽ được áp dụng. Đối với tội phạm xuyên-biên-giới, luật pháp quốc tế và các điều ước quốc tế là chuẩn mực. Sự xâm phạm dựa-trên-máy-tính có thể xảy ra ngay cả khi các quốc gia không có chung đường biên giới thực.

Xâm nhập máy tính bị coi là tội phạm ở nhiều quốc gia. Luật pháp quốc gia chống xâm phạm máy tính đều tồn tại ở các quốc gia như Canada,

Hoa Kỳ và các quốc gia thành viên của Liên minh Châu Âu (EU). Các luật lệ này sẽ khác nhau tùy theo quốc gia, nhưng tất cả đều có các điều khoản tương tự xác định việc xâm nhập và sử dụng trái phép tài nguyên máy tính cho các hoạt động tội phạm. Cho dù được gọi là hành vi gian lận máy tính (computer mischief) như ở Canada, hay xâm phạm máy tính (computer trespass) ở Hoa Kỳ, việc xâm nhập và sử dụng trái phép tài nguyên máy tính đều bị coi là một tội phạm với những hình phạt đáng kể. Cùng với sự toàn cầu hóa của cơ sở hạ tầng mạng máy tính, hay Internet, các vấn đề vượt qua ranh giới quốc gia đã nảy sinh và vẫn sẽ tiếp tục phát triển. Một số vấn đề này [có thể] được giải quyết thông qua việc áp dụng các luật lệ quốc gia khi có yêu cầu của chính phủ khác. Trong tương lai, một hiệp ước quốc tế có thể sẽ mở đường cho sự hợp tác chặt chẽ hơn.

Có những luật lệ kiểm soát các hoạt động như tin tặc, biến hầu hết các hành động trái phép trên mạng trở thành một hành vi phạm tội. Đạo luật Quyền riêng tư Giao tiếp Điện tử (Electronic Communications Privacy Act - ECPA) năm 1986 giải quyết vô số vấn đề về quyền riêng tư pháp lý do việc sử dụng ngày càng nhiều máy tính và các công nghệ khác dành riêng cho viễn thông. Các bộ phận của luật này đề cập đến email, liên lạc di động, quyền riêng tư tại nơi làm việc và một loạt các vấn đề khác liên quan đến giao tiếp qua điện tử. Phần I được thiết kế để sửa đổi các quy chế nghe lén của liên bang để bao gồm các liên lạc điện tử. Phần II, còn được gọi là Đạo luật Truyền thông được Lưu trữ (Stored Communications Act - SCA), được thiết lập để xác lập nền các biện pháp trường phạt hình sự đối với hành vi truy cập trái phép vào các hồ sơ điện tử và thông tin liên lạc được lưu trữ. Phần III bao gồm bộ đăng ký số đã gọi (pen register hoặc dialed number recorder) và các vấn đề về chạm và theo dõi (tap and

trace). Thông tin chạm và theo dõi liên quan đến việc ai đang giao tiếp với ai và khi nào. Dữ liệu đăng ký số đã gọi là thông tin hội thoại.

Một điều khoản chính của ECPA là nghiêm cấm người sử dụng lao động giám sát việc sử dụng máy tính của nhân viên, bao gồm cả email, trừ khi đã được sự đồng ý (ví dụ, nhấp vào "Có" trên biểu ngữ cảnh báo được coi là đồng ý). Các quy định pháp lý khác bảo vệ thông tin liên lạc điện tử khỏi khả năng bị rẽ nhánh và nghe trộm từ bên ngoài, vì người dùng được cho là có những mong muốn hợp lý về quyền riêng tư và được quyền bảo vệ được cấp theo Tu chính án thứ tư của Hiến pháp (Hoa Kỳ). Cần lưu ý rằng các biện pháp bảo vệ theo hiến pháp này chỉ áp dụng cho các cuộc khám xét và tịch thu của các cơ quan chính phủ và cơ quan thực thi pháp luật Hoa Kỳ (quyền tài phán liên bang, tiểu bang hoặc địa phương), nhưng không áp dụng cho các cá nhân hoặc người sử dụng lao động tư nhân.

Đạo luật Lạm dụng và Gian lận Máy tính (Computer Fraud and Abuse Act - CFAA) năm 1986 - được sửa đổi vào năm 1994 và 1996, vào năm 2001 bởi Đạo luật PATRIOT của Hoa Kỳ, và vào năm 2008 bởi Đạo luật Cưỡng chế Trộm cắp Danh tính và Phục hồi (Identity Theft Enforcement and Restitution Act) - đóng vai trò là nền tảng hiện tại để hình sự hóa việc truy cập trái phép vào hệ thống máy tính. CFAA quy định tội cố ý truy cập vào một máy tính đang được coi là máy tính của chính phủ hoặc được sử dụng trong giao dịch thương mại giữa các tiểu bang hoặc sử dụng máy tính cho mục đích phạm tội có tính chất liên bang, mà trong thời đại kết nối Internet ngày nay, hầu như có thể là bất kỳ máy tính nào, là hành động tội phạm. Đạo luật này cũng xem việc cố ý truyền một chương trình, mã hoặc lệnh dẫn đến thiệt hại là hành động tội phạm. Buôn bán mật khẩu hoặc thông tin truy cập tương tự cũng bị hình sự hóa.

Sau một số vụ bê bối tài chính/kế toán doanh nghiệp nổi tiếng ở Hoa Kỳ, chính phủ liên bang vào năm 2002 đã thông qua một đạo luật sâu rộng, Đạo luật Sarbanes-Oxley (SOX), đại tu các tiêu chuẩn kế toán tài chính dành cho các công ty giao dịch công khai ở Hoa Kỳ. Những thay đổi này mang tính toàn diện và chạm đến hầu hết các khía cạnh của hoạt động kinh doanh dù theo cách này hay cách khác. Đối với vấn đề bảo mật thông tin, một trong những thay đổi nổi bật nhất là điều khoản về các biện pháp kiểm soát tại Mục 404, quy định rằng tất cả các tiến trình liên quan đến báo cáo tài chính của một công ty phải được kiểm soát và kiểm toán thường xuyên. Vì phần lớn các công ty sử dụng hệ thống dựa trên máy tính nên điều này đã đặt các kiểm toán viên nội bộ vào những cửa hàng CNTT, xác minh rằng hệ thống đang có các biện pháp kiểm soát thích hợp để đảm bảo tính toàn vẹn và chính xác của báo cáo tài chính. Các biện pháp kiểm soát này đã gây ra những tranh cãi về chi phí duy trì chúng so với rủi ro của việc không sử dụng chúng.

Mục 404 yêu cầu các công ty thiết lập khuôn khổ dựa-trên-kiểm-soát được thiết kế để phát hiện hoặc ngăn chặn những gian lận dẫn đến sai sót của báo cáo tài chính. Nói một cách dễ hiểu, các biện pháp kiểm soát này sẽ phát hiện những hoạt động nội gián có thể lừa dối công ty. Điều này có những tác động đáng kể đến các kiểm soát bảo mật nội bộ, vì một quản trị viên hệ thống có quyền truy cập cấp root có thể thực hiện rất nhiều nếu không muốn nói là tất cả mọi nhiệm vụ liên quan đến gian lận và sẽ có khả năng thay đổi nhật ký và che dấu vết của họ. Tương tự như vậy, một số cấp độ người dùng có quyền lực của các chương trình kế toán tài chính cũng sẽ có khả năng đáng kể để thay đổi các hồ sơ.

Có vô số luật lệ bổ sung bao gồm những thứ như quyền riêng tư, chữ ký kỹ thuật số, hồ sơ y tế và thư rác. Các luật lệ và quy định bổ sung tồn tại ở cấp tiểu bang, và một số luật và quy định quan trọng nhất là những

luật và quy định đến từ California. California, quê hương của ngành công nghiệp công nghệ Hoa Kỳ, cũng là một tiểu bang rất tiên bộ về mặt luật pháp. California dẫn đầu về luật quyền riêng tư và bảo mật sự kiện của các thiết bị Internet vạn vật (IoT).

Dự luật Thượng viện California 1386 (California Senate Bill - SB 1386) là một đạo luật mang tính bước ngoặt liên quan đến việc tiết lộ thông tin. Nó bắt buộc rằng công dân của California phải được thông báo bất cứ khi nào PII bị mất hoặc bị tiết lộ. Kể từ khi Luật SB 1386 được thông qua, nhiều tiểu bang khác đã lấy dự luật này để làm mẫu, và mặc dù luật pháp quốc gia đã bị chặn bởi các động thái mang tính thủ tục về chính trị, nhưng cuối cùng nó cũng sẽ được thông qua. Danh sách hiện tại của các tiểu bang và vùng lãnh thổ của Hoa Kỳ yêu cầu thông báo về việc tiết lộ lên đến 49, chỉ có Alabama, New Mexico và Nam Dakota là không có đạo luật này. Mỗi đạo luật thông báo về sự tiết lộ này là khác nhau, khiến trường hợp về việc thống nhất quy chế của liên bang trở nên hấp dẫn, nhưng hiện tại nó đang nằm trong danh sách ưu tiên của hầu hết các chính trị gia.

California đã mở rộng các đạo luật về quyền riêng tư của mình bằng Đạo luật về Quyền riêng tư của Người tiêu dùng California năm 2020. Đạo luật này yêu cầu các tổ chức đạt được sự đồng thuận từ các cá nhân để thu thập và sử dụng dữ liệu của họ. Nó cũng yêu cầu họ tiết lộ cách mà dữ liệu được sử dụng như thế nào. Đạo luật cấm cho người tiêu dùng quyền yêu cầu doanh nghiệp tiết lộ các thể loại và các phần thông tin cụ thể mà doanh nghiệp thu thập, nguồn của thông tin đó, lý do tại sao doanh nghiệp thu thập và/hoặc bán thông tin đó và các thể loại của các bên-thứ-ba được cung cấp thông tin đó. Theo nhiều cách, đạo luật này chính là sự phản ánh GDPR của EU.

## Tiêu chuẩn Bảo mật Dữ liệu Ngành Thẻ Thanh toán (PCI DSS)

Ngành công nghiệp thẻ thanh toán, bao gồm cả các cường quốc MasterCard và Visa, thông qua Hội đồng Tiêu chuẩn Bảo mật PCI của mình, đã thiết kế nên một sáng kiến trong khu vực tư nhân để bảo vệ thông tin thẻ thanh toán giữa ngân hàng và người bán. *Tiêu chuẩn Bảo mật Dữ liệu Ngành Thẻ Thanh toán (PCI DSS)* là một tập hợp các quy tắc mang tính hợp đồng điều chỉnh cách thức dữ liệu thẻ tín dụng được bảo vệ (xem thanh bên “Mục tiêu và yêu cầu của PCI DSS”). Phiên bản hiện tại là 3.2, được phát hành vào tháng 4 năm 2016. Phiên bản tiếp theo, 4.0, dự kiến vào cuối năm 2020, nhưng đã bị trì hoãn lại do đại dịch COVID-19 trên toàn thế giới. PCI DSS là một sáng kiến tự nguyện của khu vực tư nhân, mang tính ưu việt trong hướng dẫn bảo mật của nó. Người bán và nhà cung cấp có thể chọn không áp dụng các biện pháp này, nhưng tiêu chuẩn có một mức giá rất cao cho việc không tuân thủ, phí giao dịch đối với các nhà cung cấp không tuân thủ có thể cao hơn đáng kể, có thể bị phạt lên đến 500.000 đô la và trong trường hợp nghiêm trọng, khả năng xử lý thẻ tín dụng có thể bị thu hồi.

### Các Mục tiêu và Yêu cầu của PCI DSS

PCI DSS v3 bao gồm 6 mục tiêu kiểm soát chứa tổng cộng 12 yêu cầu:

#### 9. Xây dựng và Duy trì một Mạng Bảo mật

**Yêu cầu 1** Cài đặt và duy trì một cấu hình tường lửa để bảo vệ dữ liệu của chủ thẻ.

**Yêu cầu 2** Không sử dụng các cấu hình mặc định được-cung-cấp-bởi-nhà-thầu đối với mật khẩu và các tham số bảo mật khác.

#### 10. Bảo vệ Dữ liệu của Chủ thẻ

**Yêu cầu 3** Bảo vệ dữ liệu của chủ thẻ đã được lưu trữ

**Yêu cầu 4** Mã hóa việc truyền tải dữ liệu của chủ thẻ qua các mạng mở và công cộng.

11. Duy trì một Chương trình Quản lý Lỗi hổng

**Yêu cầu 5** Bảo vệ tất cả các hệ thống chống lại phần mềm mã độc và thường xuyên cập nhật phần mềm hoặc chương trình chống vi-rút.

**Yêu cầu 6** Phát triển và duy trì các hệ thống và ứng dụng an toàn.

12. Triển khai các Biện pháp Kiểm soát Truy cập Mạnh mẽ

**Yêu cầu 7** Hạn chế việc truy cập vào dữ liệu của chủ thẻ chỉ cho doanh nghiệp cần-được-biết.

**Yêu cầu 8** Nhận diện và xác thực quyền truy cập vào các thành phần của hệ thống.

**Yêu cầu 9** Hạn chế quyền truy cập vật lý vào dữ liệu của chủ thẻ.

13. Giám sát và Kiểm tra Mạng Một cách thường xuyên

**Yêu cầu 10** Theo dõi và giám sát tất cả truy cập vào các nguồn tài nguyên mạng và dữ liệu của chủ thẻ.

**Yêu cầu 11** Thường xuyên kiểm tra tính bảo mật của các hệ thống và các quy trình.

14. Duy trì một Chính sách Bảo mật Thông tin

**Yêu cầu 12** Duy trì một chính sách xác định các vấn đề bảo mật thông tin cho mọi nhân viên.

PCI DSS có hai kiểu thôn tin đã được xác định: dữ liệu của chủ thẻ và dữ liệu xác thực nhạy cảm. Các yêu cầu bảo vệ đã được thiết lập đối với những phần tử này được liệt kê chi tiết trong Bảng 32-1.

	Phần tử Dữ liệu	Được phép Lưu trữ	Kết xuất Dữ liệu được Lưu trữ Không thể đọc được
Dữ liệu Tài khoản	Số Tài khoản Chính (PAN)	Được phép	Có
	Tên Chủ thẻ	Được phép	Không
	Mã Dịch vụ	Được phép	Không
	Ngày Hết hạn	Được phép	Không
Dữ liệu Xác thực Nhịp cảm	Toàn bộ Dữ liệu Theo dõi	Không	Không thể lưu trữ theo Yêu cầu 3.2
	CAV2/CVC2/CVV2/CID	Không	Không thể lưu trữ theo Yêu cầu 3.2
	PIN/PIN Block	Không	Không thể lưu trữ theo Yêu cầu 3.2



**MÁCH NƯỚC CHO KỲ THI** Tiêu chuẩn Bảo mật Dữ liệu Ngành Thanh toán (PCI DSS) bảo vệ thông tin thẻ tín dụng của khách hàng và được thiết kế để giảm thiểu sự gian lận. Tiêu chuẩn mang tính hợp đồng này có những hình phạt tài chính rất cao đối với việc không tuân thủ.

### Các Khuôn khổ Chính

Các khuôn khổ cung cấp một phương tiện để đánh giá lộ tuyến thông qua mê cung của các yêu cầu quy định và cách mà chúng có liên quan đến quản lý rủi ro như thế nào. Một trong số những khía cạnh thách thức của hoạt động an ninh mạng là xác định được nơi nào nên tập trung nỗ lực, nguồn lực nên được triển khai như thế nào và cần đặt trọng tâm cân bằng nào giữa các hạng mục ngắn-hạn và dài-hạn để tối ưu hóa các nỗ lực giảm thiểu rủi ro. Một số loại khuôn khổ chính có thể được sử dụng như một phần của phân tích này. Trong các phần tiếp theo, chúng ta sẽ cùng

xem xét các khuôn khổ từ Trung tâm An ninh Internet (Center for Internet Security), Viện Tiêu chuẩn và Công nghệ Quốc gia (National Institute of Standards and Technology) – [Hoa Kỳ], một số tiêu chuẩn ISO, tiêu chuẩn SSAE và Liên minh Bảo mật Đám mây (Cloud Security Alliance).

### **Trung tâm Bảo mật Internet (CIS)**

*Trung tâm Bảo mật Internet (CIS)* là một tổ chức phi lợi nhuận phục vụ cho cộng đồng an ninh mạng theo một số cách. Nó là người giám sát của các biện pháp kiểm soát CIS - một tập hợp bao gồm 20 biện pháp kiểm soát bảo mật hàng đầu cần được triển khai như một đường cơ sở quản lý rủi ro an ninh mạng. Bộ kiểm soát này, được phát triển theo cách thức dựa trên sự đồng thuận trong thập kỷ qua, cung cấp một lộ trình mà các biện pháp kiểm soát bảo mật nên được triển khai đầu tiên, thứ hai, v.v... Các hạng mục quy định này đại diện cho những thực tiễn tốt nhất trong nhiều tổ chức, từ chính phủ đến ngành và đều có thể được triển khai bởi hầu hết các thực thể với mọi quy mô.

CIS cũng đã xuất bản một bộ tiêu chuẩn đối sánh CIS (tham khảo trang [www.cisecurity.org/cis-benchmarks/](http://www.cisecurity.org/cis-benchmarks/)). Các điểm chuẩn đối sánh này là các hướng dẫn cấu hình an toàn, được phát-triển-đồng-thuận để củng cố một loạt các hạng mục kỹ thuật.

### **Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST) Khuôn khổ Quản lý Rủi ro (RMF)/Khuôn khổ An ninh mạng (CSF)**

*Viện Tiêu chuẩn và Công nghệ Quốc gia (NIST)* [Hoa Kỳ] cung cấp các chiến lược được khuyến nghị cho chính phủ Hoa Kỳ và những người khác về cách thức xử lý nhiều vấn đề, bao gồm rủi ro đến từ các vấn đề về an ninh mạng. Phương pháp tiếp cận được thực hiện bởi NIST là phương pháp được xây dựng xoay quanh việc quản lý rủi ro của tổ chức thông qua *khuôn khổ quản lý rủi ro* (*risk management framework* - RMF) liên

quan đến các hoạt động an ninh mạng. NIST RMF bao gồm hơn 10 ấn phẩm, bao gồm hầu hết mọi hoạt động có liên quan đến an ninh mạng.

Hoạt động thứ hai được NIST công bố là *Khuôn khổ An ninh mạng* (*Cybersecurity Framework - CSF*). CSF được thiết kế để hỗ trợ các tổ chức trong những giai đoạn ban đầu của việc lập kế hoạch bảo đảm an ninh mạng của họ. Nó chia nhỏ các kiểu hoạt động thành năm chức năng khác nhau: xác định, bảo vệ, phát hiện, ứng phó và phục hồi (identify, protect, detect, respond và recover). CSF đã được thông qua bởi một dự luật của Quốc hội vào năm 2014 định hướng NIST để xác định "một phương pháp tiếp cận được ưu tiên, linh hoạt, có thể lặp lại, dựa trên hiệu suất và hiệu-quả-về-chi-phí, bao gồm các biện pháp kiểm soát và bảo mật thông tin có thể được tự nguyện áp dụng bởi chủ sở hữu và nhà khai thác cơ sở hạ tầng tối quan trọng để giúp họ xác định, đánh giá và quản lý rủi ro về mạng". Phiên bản mới nhất của CSF được xuất bản vào tháng 3 năm 2020.

Bước thứ ba trong số những nỗ lực của NIST trong tài liệu về an ninh mạng là Khuôn khổ Lực lượng lao động An ninh mạng (*Cybersecurity Workforce Framework*) của Sáng kiến Quốc gia về Giáo dục An ninh mạng (*National Initiative for Cybersecurity Education - NICE*). Đây là một nỗ lực nhằm xác định hệ sinh thái giáo dục, đào tạo và phát triển lực lượng lao động an ninh mạng cần thiết để tạo ra lực lượng lao động cần thiết về an ninh mạng trong chính phủ và trong ngành.

### **Tổ chức Tiêu chuẩn Quốc tế (ISO) 27001/27002/27701/31000**

ISO 27001 là tiêu chuẩn quốc tế xác định hệ thống quản lý bảo mật thông tin (information security management system - ISMS). ISO 27001 là một trong nhiều tiêu chuẩn có liên quan trong họ tiêu chuẩn 27000. ISO 27002 là tài liệu xác định các kỹ thuật bảo mật và quy tắc thực hành đối với các biện pháp kiểm soát bảo mật thông tin. ISO 27701 là một phần mở rộng

về quyền riêng tư cho dòng 27000 và bổ sung thêm các yêu cầu để thiết lập và duy trì hệ thống quản lý thông tin về quyền riêng tư. Bộ tiêu chuẩn ISO 31000 là một tập hợp các hướng dẫn, nguyên tắc, khuôn khổ và quy trình để quản lý rủi ro. ISO 31000 đề cập đến tất cả các dạng rủi ro và quản lý chứ không chỉ rủi ro về an ninh mạng.

### **Ssae SOC 2 Kiểu I/II**

Tuyên bố về các Tiêu chuẩn dành cho Cam kết Chứng thực (Statement on Standards for Attestation Engagements - SSAE) là một bộ tiêu chuẩn kiểm toán được thiết lập bởi Hội đồng Chuẩn mực Kiểm toán (Auditing Standards Board) của Viện Kế toán Công chứng Hoa Kỳ (American Institute of Certified Public Accountants - AICPA) đặt ra. SOC là viết tắt của Kiểm soát Tổ chức Dịch vụ (Service Organization Controls). Báo cáo của SOC 2 tập trung vào các biện pháp kiểm soát nội bộ tại một tổ chức liên quan đến tuân thủ hoặc hoạt động, bao gồm năm nguyên tắc tin cậy (bảo mật, bí mật, xử lý toàn vẹn, tính sẵn sàng và quyền riêng tư). Tùy thuộc vào tổ chức và việc kinh doanh của bạn, một số hoặc tất cả năm nguyên tắc tin cậy sẽ được áp dụng. SOC 2 là một báo cáo riêng biệt tập trung vào các biện pháp kiểm soát tại nhà cung cấp dịch vụ có liên quan đến bảo mật, tính sẵn sàng, tính toàn vẹn của quá trình xử lý, tính bảo mật và quyền riêng tư của hệ thống. Nó đảm bảo rằng dữ liệu của bạn được lưu trữ một cách riêng tư và an toàn trong khi lưu trữ và truyền tải và bạn có thể truy cập đến chúng bất cứ lúc nào. Báo cáo SOC 1 và SOC 2 có hai dạng: Loại I và Loại II. Báo cáo loại I đánh giá liệu các biện pháp kiểm soát thích hợp có đang được thực hiện tại một thời điểm cụ thể hay không. Báo cáo loại II được thực hiện trong một khoảng thời gian để xác minh tính hiệu quả và hiệu suất vận hành của các biện pháp kiểm soát.



**MÁCH NƯỚC CHO KỲ THI** Các báo cáo SOC 2 tập trung vào các biện pháp kiểm soát nội bộ liên quan đến tuân thủ hoặc vận hành. Một báo cáo SOC kiểu I đánh giá xem liệu các biện pháp kiểm soát thích hợp có đang được thực hiện tại một thời điểm cụ thể hay không. Một báo cáo SOC kiểu II được thực hiện trong một khoảng thời gian để xác minh tính hiệu quả và hiệu suất vận hành của các biện pháp kiểm soát.

### **Liên minh Bảo mật Đám mây**

Ra đời vào năm 2008 và được hợp nhất vào năm 2009, Liên minh Bảo mật Đám mây đã phát hành tài liệu thực-tiễn-tốt-nhất toàn diện đầu tiên dành cho điện toán đám mây bảo mật, "Hướng dẫn Bảo mật cho các Khu vực Trọng tâm Tối quan trọng của Điện toán Đám mây" (Security Guidance for Critical Area of Focus for Cloud Computing) và đã trở thành cơ quan đầu ngành về các khuôn khổ, điểm chuẩn đối sánh và các tiêu chuẩn liên quan đến điện toán đám mây trên toàn thế giới. Một số tài liệu chính được phát triển bao gồm Ma trận Kiểm soát Đám mây (Cloud Controls Matrix - CCM), chứng chỉ xác thực người dùng về Chứng chỉ Kiến thức Bảo mật Đám mây (Certificate of Cloud Security Knowledge - CCSK), Chứng chỉ Chuyên gia Bảo mật Đám mây được Chứng nhận (Certified Cloud Security Professional - CCSP) (được phát triển cùng với ISC2) và một khuôn khổ bảo mật dành cho đám mây chính phủ.

### **Ma trận Kiểm soát Đám mây**

Ma trận Kiểm soát Đám mây (CCM) là một khuôn-khổ-tổng-hợp (meta-framework) của các biện pháp kiểm soát bảo mật dành-riêng-cho-đám-mây, được ánh xạ tới các tiêu chuẩn, thực tiễn tốt nhất và các quy định hàng đầu. Tài liệu này sử dụng 16 lĩnh vực để đề cập đến 133 mục tiêu kiểm soát bảo mật nhằm giải quyết tất cả các khía cạnh then chốt của

bảo mật đám mây. Các biện pháp kiểm soát được liệt kê trong tài liệu này được ánh xạ tới các tiêu chuẩn bảo mật chính của ngành, bao gồm chuỗi ISO 2700X, NIST SP 800-53, PCI DSS, ISACA COBIT và nhiều tiêu chuẩn khác.

Ví dụ về một biện pháp kiểm soát CCM được cung cấp trong Bảng 32-2.

Lĩnh vực Kiểm soát	Mã Kiểm soát CCM v3.0	Thông số kỹ thuật Kiểm soát
Quản lý Khóa và Mã hóa Bảo vệ Dữ liệu Nhạy cảm	EKM-03	Các chính sách và thủ tục sẽ được xác lập, và các quy trình hỗ trợ kinh doanh và biện pháp kỹ thuật được triển khai, đối với việc sử dụng các giao thức mã hóa để bảo vệ những dữ liệu nhạy cảm đang được lưu trữ (nghĩa là, các máy chủ lưu trữ tập tin, các cơ sở dữ liệu, và máy trạm của người-dùng-đầu-cuối, dữ liệu đang sử dụng (bộ nhớ), và dữ liệu đang được truyền tải (nghĩa là, các giao diện hệ thống, qua mạng công cộng, và các thông điệp điện tử) cũng như theo luật lệ hiện hành, luật định và các nghĩa vụ tuân thủ quy định.

**Bảng 32-2** Một Mẫu Kiểm soát từ CCM v3.0

### Kiến trúc Tham chiếu

Liên minh Bảo mật Đám mây có một Nhóm Công nghiệp (Enterprise Architecture Working Group - EAWG) đã phát triển Kiến trúc Doanh nghiệp cho việc triển khai và các dịch vụ đám mây. Khuôn khổ này vừa đóng vai trò là một phương pháp luận vừa là một bộ công cụ có thể được sử dụng bởi các kiến trúc sư bảo mật, kiến trúc sư doanh nghiệp và các chuyên gia quản lý rủi ro. Mục tiêu của khuôn khổ là phát triển và tận dụng một bộ các giải pháp chung cho phép đánh giá vị thế

hiện tại của hoạt động CNTT nội bộ và các nhà cung cấp đám mây của họ về mặt khả năng bảo mật. Khuôn khổ này cũng có thể được sử dụng để lập kế hoạch cho lộ trình để đáp ứng nhu cầu bảo mật đám mây của doanh nghiệp.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy chuẩn bị để xác định các đề mục của Liên minh Bảo mật Đám mây bằng các từ viết tắt của chúng và hiểu được sự khác biệt giữa chúng. Kiến trúc Doanh nghiệp (EA) là một khuôn khổ rộng rãi mô tả tất cả các khía cạnh, trong khi Ma trận Kiểm soát Đám mây (CCM) là danh sách các biện pháp kiểm soát bảo mật dành cho đám mây.

### **Hướng dẫn So sánh điểm chuẩn và Cấu hình Bảo mật**

*Điểm chuẩn so sánh và hướng dẫn cấu hình bảo mật* cung cấp hướng dẫn để thiết lập và vận hành hệ thống máy tính ở mức độ bảo mật đã được hiểu và được lập thành văn bản. Vì mỗi tổ chức có thể khác nhau, tiêu chuẩn cho điểm chuẩn so sánh là một tập hợp kiến thức dựa trên sự đồng thuận được thiết kế để cung cấp một tập hợp bảo mật hợp lý trên một cơ sở càng rộng càng tốt. Có rất nhiều nguồn cho các hướng dẫn này, nhưng có ba nguồn chính cho một số lượng lớn các hệ thống này. Bạn có thể nhận được hướng dẫn điểm chuẩn so sánh từ các nhà sản xuất phần mềm, từ chính phủ và từ một tổ chức độc lập như Trung tâm Bảo mật Internet (CIS) và Liên minh Bảo mật Đám mây (CSA). Không phải tất cả các hệ thống đều có điểm chuẩn so sánh, cũng như không phải tất cả các nguồn đều bao hàm tất cả các hệ thống, nhưng việc tìm kiếm và tuân theo các chỉ thị cấu hình và thiết lập chính xác có thể đi một chặng đường dài trong việc thiết lập bảo mật.

---



**MÁCH NƯỚC CHO KỲ THI** Các tổ chức thường tham chiếu tới các điểm chuẩn so sánh của Trung tâm Bảo mật Internet (CIS) để phát triển thái độ cấu hình bảo mật của mình.

Nguồn hướng dẫn của nhà cung cấp/nhà sản xuất rất dễ dàng – hãy truy cập vào trang web của nhà cung cấp sản phẩm của bạn. Các nguồn chính phủ của hơi phân tán hơn một chút, nhưng hai nguồn vững chắc là Cơ sở dữ liệu quốc gia về Lỗ hổng Bảo mật Máy tính NIST (National Vulnerability Database - NVD) và Kho lưu trữ của Chương trình Danh sách kiểm tra Quốc gia (NCP) (<https://nvd.nist.gov/ncp/repository>). Một nguồn khác là Hướng dẫn Triển khai Kỹ thuật Bảo mật (Security Technical Implementation Guides - STIG) của Cơ quan An ninh Thông tin Quốc phòng (Defense Information Security Agency - DISA) của Bộ Quốc phòng Hoa Kỳ. Đây là các hướng dẫn triển khai từng bước chi tiết, danh sách về những hướng dẫn đang sẵn có tại <https://public.cyber.mil/stigs/>.

### **Hướng dẫn Nền tảng/Nhà-thầu-Cụ-thể**

Việc thiết lập các dịch vụ bảo mật là điều rất quan trọng đối với các doanh nghiệp và một số hướng dẫn tốt nhất đến từ các nhà sản xuất dưới dạng *hướng dẫn nền tảng/nhà-thầu-cụ-thể*. Những hướng dẫn này bao gồm hướng dẫn cài đặt và thiết lập cấu hình, và trong một số trường hợp, cả hướng dẫn vận hành.

### **Máy chủ Web**

Rất nhiều máy chủ web khác nhau được sử dụng trong các doanh nghiệp, nhưng dẫn đầu thị trường là Microsoft, Apache và Nginx. Theo định nghĩa, *máy chủ web* cung cấp một kết nối giữa người dùng (máy khách) và các trang web (dữ liệu đang được cung cấp), và do đó chúng rất dễ bị tấn công. Việc thiết lập bất kỳ ứng dụng tương-tác-với-bên-ngoài nào một

cách đúng đắn là chìa khóa để ngăn ngừa rủi ro không cần thiết. May mắn thay, đối với các máy chủ web, một số nguồn thông tin có căn cứ và mang tính định hướng sẵn có để giúp cho các quản trị viên bảo mật được ứng dụng một cách thích hợp. Trong trường hợp Máy chủ IIS và Máy chủ SharePoint của Microsoft, công ty cung cấp hướng dẫn vững chắc về cấu hình máy chủ phù hợp. Apache Software Foundation cũng cung cấp một số thông tin cho các sản phẩm máy chủ web của mình.

Một nguồn thông tin tốt khác đến từ Trung tâm Bảo mật Internet, như một phần của hướng dẫn đo điểm chuẩn so sánh. Các hướng dẫn của CIS cung cấp hướng dẫn có căn cứ xác đáng và mang tính định hướng, được phát triển như một phần của nỗ lực đồng thuận giữa các nhà tư vấn, các chuyên gia và những người khác. Hướng dẫn này đã được đánh giá ngang hàng đáng kể và đã chịu đựng được sự thử thách của thời gian. Hướng dẫn CIS có sẵn cho nhiều phiên bản của Apache, Microsoft và các sản phẩm của các nhà cung cấp khác.

## **Hệ điều hành**

*Hệ điều hành (OS)* là giao diện dành cho các ứng dụng mà chúng ta sử dụng để thực hiện các tác vụ và phần cứng máy tính vật lý thực tế. Do vậy, Hệ điều hành là một thành phần then chốt đối với hoạt động bảo mật của một hệ thống. Các hướng dẫn thiết lập cấu hình toàn diện và mang tính định hướng cho tất cả các hệ điều hành chính có sẵn từ các nhà sản xuất tương ứng của chúng, từ Trung tâm Bảo mật Internet và từ chương trình DoD DISA STIGs.

## **Máy chủ Ứng dụng**

Các *máy chủ ứng dụng* là một phần của doanh nghiệp để xử lý các tác vụ cụ thể mà chúng ta liên kết với các hệ thống CNTT. Cho dù đó là máy chủ email, máy chủ cơ sở dữ liệu, nền tảng nhắn tin hay bất kỳ máy chủ nào khác, máy chủ ứng dụng là nơi công việc diễn ra. Cấu hình đúng đắn của

một máy chủ ứng dụng phụ thuộc rất nhiều vào các chi tiết cụ thể của máy chủ. Các máy chủ ứng dụng tiêu chuẩn, chẳng hạn như email và máy chủ cơ sở dữ liệu đều có các hướng dẫn từ nhà sản xuất, từ CIS và STIGs. Các máy chủ ít tiêu chuẩn hơn - những máy chủ có các tùy chỉnh đáng kể, chẳng hạn như một bộ ứng dụng tùy chỉnh được viết trong-nội-bộ cho các hoạt động kiểm soát tồn kho của bạn hoặc xử lý đơn hàng hoặc bất kỳ phần mềm trung gian tùy chỉnh nào khác - cũng đều yêu cầu cấu hình phù hợp, nhưng nhà cung cấp thực sự trong những trường hợp này là nhà xây dựng phần mềm trong-nội-bộ. Việc đảm bảo cài đặt bảo mật thích hợp và kiểm tra các máy chủ này nên là một phần của chương trình xây dựng để chúng có thể được tích hợp vào quy trình kiểm toán bảo mật thông thường nhằm đảm bảo cấu hình thích hợp được liên tục.

### Các Thiết bị Cơ sở hạ tầng Mạng

*Các thiết bị cơ sở hạ tầng mạng* là các bộ chuyển mạch, bộ định tuyến, bộ tập trung (concentrators), tường lửa và các thiết bị đặc biệt khác giúp mạng hoạt động một cách trơn tru. Việc thiết lập cấu hình các thiết bị này một cách thích hợp có thể là một thách thức nhưng là điều rất quan trọng vì các lỗi ở cấp độ này có thể ảnh hưởng xấu đến bảo mật của lưu lượng đang được chúng xử lý. Mức độ quan trọng của các thiết bị này khiến chúng trở thành mục tiêu của các cuộc tấn công bởi vì, nếu tường lửa không thành công, trong nhiều trường hợp sẽ không có dấu hiệu nào cho đến khi một cuộc điều tra phát hiện ra rằng nó không thực hiện được công việc của mình. Việc đảm bảo các thiết bị này được thiết lập cấu hình và bảo trì một cách đúng đắn không phải là công việc có vẻ ngoài bóng bẩy, mà là công việc đòi hỏi sự quan tâm chuyên nghiệp của nhân viên đã được đào tạo một cách thích hợp và được hỗ trợ bởi các cuộc kiểm tra cấu hình định kỳ để đảm bảo chúng luôn được thiết lập cấu hình đúng cách. Đối với hầu hết các thiết bị này, rủi ro lớn nhất nằm ở cấu hình

người dùng của thiết bị thông qua các bộ quy tắc và các bộ quy tắc này dành riêng cho từng người dùng và không thể bắt buộc theo hướng dẫn cài đặt của nhà sản xuất. Cấu hình và xác minh phù hợp là dành riêng cho từng địa điểm và nhiều khi là dành riêng cho từng thiết bị. Nếu không có một bộ chính sách và thủ tục vững chắc để đảm bảo rằng công việc này đang được thực hiện một cách đúng đắn thì các thiết bị này - trong khi chúng có thể đang hoạt động - sẽ không hoạt động theo một cách an toàn.

## Tóm tắt Chương

Trong chương này, đầu tiên bạn làm quen với các quy định, tiêu chuẩn và khuôn khổ hiện hành có thể tác động đến tình hình bảo mật của tổ chức. Chương mở đầu bằng việc xem xét các quy định, tiêu chuẩn và luật lệ. Trong danh mục này, Quy định Chung về Bảo vệ Dữ liệu (GDPR) của Liên minh Châu Âu cũng như một số luật lệ của quốc gia, tiểu bang và vùng lãnh thổ đã được đề cập. Phần đầu tiên kết thúc với Tiêu chuẩn Bảo mật Dữ liệu Ngành Thẻ Thanh toán (PCI DSS).

Phần chính tiếp theo bao gồm các khuôn khổ chủ yếu được sử dụng trong doanh nghiệp. Các khuôn khổ được thảo luận đến từ Trung tâm Bảo mật Internet (CIS), Khuôn khổ Quản lý Rủi ro Công nghệ (RMF)/Khuôn khổ An ninh Mạng (CSF) của Viện Tiêu chuẩn và Công nghệ Quốc gia (Hoa Kỳ), Tổ chức Tiêu chuẩn Quốc tế (ISO 27001/27002/27701/31000), SSAE SOC Loại I/II và Liên minh Bảo mật Đám mây (ma trận kiểm soát đám mây và kiến trúc tham chiếu).

Chương này kết thúc bằng việc xem xét các loại điểm chuẩn khác nhau và hướng dẫn cấu hình an toàn. Trong phần này, các hướng dẫn dành riêng cho nền tảng và nhà cung cấp đã được trình bày, bao gồm các hướng dẫn dành cho máy chủ web, hệ điều hành, máy chủ ứng dụng và các thiết bị hạ tầng mạng.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

- 1.** Các khuôn khổ tiêu-chuẩn-ngành chủ yếu rất hữu ích cho những mục đích nào dưới đây?
  - A.** Liên kết với một tiêu chuẩn dựa-trên-kiểm-toán.
  - B.** Liên kết CNTT và bảo mật với chiến lược kinh doanh của doanh nghiệp.
  - C.** Cung cấp tổ chức cấp-cao trên các quy trình.
  - D.** Tạo ra các sơ đồ để lập thành tài liệu các kiến trúc hệ thống.
- 2.** Thuật ngữ nào dưới đây là một quy định về quyền riêng tư?
  - A.** CFAA
  - B.** SOX
  - C.** GDPR
  - D.** PCI DSS.
- 3.** Những gì dưới đây là các danh sách kiểm soát bảo mật có thể được sử dụng trong một doanh nghiệp? (Chọn tất cả đáp án đúng)
  - A.** ISO 27001
  - B.** CSA CCM
  - C.** Danh sách hàng đầu 20 của CIS
  - D.** NIST RMF.
- 4.** Báo cáo nào được thực hiện trong một khoảng thời gian để xác minh tính hiệu quả và hiệu suất hoạt động của các biện pháp kiểm soát?
  - A.** SOC Loại I
  - B.** Báo cáo kiểm toán PCI DSS
  - C.** CSA CCM

#### D. SOC Loại II.

5. Những gì dưới đây không phải là một mục tiêu kiểm soát của PCI DSS?
  - A. Xây dựng và duy trì một mạng bảo mật
  - B. Duy trì một chương trình quản lý lỗ hổng
  - C. Thiết lập một vị trí CSO
  - D. Triển khai các biện pháp kiểm soát truy cập mạnh mẽ.
6. Tiêu chuẩn ISO nào đề cập đến các hoạt động quản lý rủi ro?
  - A. ISO 27001
  - B. ISO 27701
  - C. ISO 27002
  - D. ISO 31000.
7. Hướng dẫn dành cho việc thiết lập và vận hành hệ thống máy tính ở mức độ bảo mật được hiểu và lập thành văn bản từ điều nào sau đây? (Chọn tất cả các đáp án đúng).
  - A. ISO
  - B. CIS
  - C. Các nguồn của chính phủ
  - D. Nhà cung cấp/nhà sản xuất.
8. Những gì dưới đây không phải là các luật lệ của Hoa Kỳ liên quan đến an ninh mạng (Chọn tất cả các đáp án đúng).
  - A. CFAA
  - B. PCI DSS
  - C. GDPR
  - D. Sarbanes Oxley (SOX).
9. Người ta sẽ tìm kiếm các hướng dẫn cấu hình an toàn, được phát triển-đồng-thuận ở đâu để củng cố một loạt các hạng mục kỹ thuật?
  - A. CIS

**B. ISO**

**C. Nhà cung cấp/nhà sản xuất**

**D. Các đồng nghiệp.**

**10.** Hướng dẫn cấu hình toàn diện và mang tính mô tả dành cho tất cả các hệ điều hành chính có sẵn từ hướng dẫn nào sau đây? (Chọn tất cả các đáp án đúng).

**A. Nhà cung cấp/nhà sản xuất**

**B. NIST**

**C. CIS**

**D. ISO.**

## Đáp án

1. **B.** Các khuôn khổ tiêu-chuẩn-ngành cung cấp một phương pháp để liên kết CNTT và bảo mật với chiến lược kinh doanh của doanh nghiệp.
2. **C.** GDPR là chỉ thị về quyền riêng tư của Liên minh Châu Âu với những hậu quả sâu rộng trên các ngành công nghiệp và thậm chí cả ranh giới quốc gia.
3. **B** và **C.** Ma trận Kiểm soát Đám mây của Liên minh Bảo mật Đám mây là danh sách các biện pháp kiểm soát bảo mật liên quan đến việc triển khai đám mây. Danh sách 20 hàng đầu của CIS là một tập hợp các biện pháp kiểm soát bảo mật theo thứ tự cho doanh nghiệp. Cả ISO 27001 và NIST RMF đều là các tài liệu thủ tục, không phải danh sách các biện pháp kiểm soát.
4. **D.** Báo cáo loại II của SOC được thực hiện trong một khoảng thời gian để xác minh hiệu quả và hiệu suất hoạt động của các biện pháp kiểm soát. Mặt khác, báo cáo SOC Loại I đánh giá liệu các biện pháp kiểm soát thích hợp có đang được áp dụng tại một thời điểm cụ thể hay không.
5. **C.** Các mục tiêu kiểm soát PCI DSS bao gồm:
  1. Xây dựng và duy trì một mạng bảo mật,
  2. Bảo vệ dữ liệu của chủ thẻ,
  3. Duy trì một chương trình quản lý lỗ hổng bảo mật,
  4. Thực hiện các biện pháp kiểm soát truy cập mạnh mẽ,
  5. Thường xuyên giám sát và kiểm tra mạng,
  6. Duy trì một chính sách bảo mật thông tin.Không nơi nào bắt buộc các vị trí công ty cụ thể.
6. **D.** ISO 31000 bao gồm các quy trình và thủ tục quản lý rủi ro.

7. **B, C và D.** Điểm chuẩn so sánh và hướng dẫn cấu hình bảo mật cung cấp hướng dẫn để thiết lập và vận hành hệ thống máy tính ở một mức độ bảo mật được hiểu và được lập thành văn bản. Có rất nhiều nguồn cho các hướng dẫn này, nhưng có ba nguồn chính cho một số lượng lớn các hệ thống này. Bạn có thể nhận hướng dẫn điểm chuẩn so sánh từ các nhà sản xuất phần mềm, từ chính phủ và từ một tổ chức độc lập như Trung tâm Bảo mật Internet (CIS) hoặc Liên minh Bảo mật Đám mây (CSA). ISO là một tổ chức tiêu chuẩn và không giải quyết các chi tiết triển khai cụ thể.
8. **B và C.** PCI DSS là tiêu chuẩn tự nguyện, dựa-trên-hợp-đồng và GDPR là chỉ thị của EU, không phải luật lệ của Hoa Kỳ.
9. **A.** Từ khóa là *sự đồng thuận*. CIS đã phát triển một bộ hướng dẫn cấu hình bảo mật dựa-trên-sự-đồng-thuận để cung cấp bảo mật một loạt các hạng mục kỹ thuật.
10. **A và C.** Các nhà cung cấp/nhà sản xuất và Trung tâm Bảo mật Internet đều cung cấp hướng dẫn cấu hình toàn diện cho các hệ điều hành. Một nguồn khác là chương trình STIG của Bộ Quốc phòng. NIST và ISO phát triển hướng dẫn cho các chính sách và quy trình, nhưng không xây dựng các cấu hình cụ thể cho các hệ điều hành.

## Chương 33 Các Chính sách Tổ chức

### Các Chính sách Tổ chức

Trong chương này bạn sẽ

- Khám phá các chính sách được sử dụng để quản lý bảo mật của tổ chức,
- Xem xét các quy trình được sử dụng trong quản lý rủi ro của các bên-thứ-ba.

Các chính sách và thủ tục chi phối hoạt động của tổ chức và đại diện cho một tập hợp các yêu cầu được phát triển từ cả các nguồn bên trong lẫn bên ngoài. Các yêu cầu bên ngoài có thể đến từ luật pháp và quy định, điều khoản hợp đồng hoặc đặc tả thông số kỹ thuật của khách hàng. Có những tình huống pháp lý trong đó các hành động kinh doanh cụ thể được yêu cầu bởi luật pháp hoặc quy định. Trong nhiều trường hợp, các luật lệ hoặc quy định chỉ rõ rằng các chính sách cụ thể được áp dụng để ảnh hưởng đến việc tuân thủ. Việc hiểu rõ các yêu cầu cụ thể của môi trường kinh doanh có thể đòi hỏi phải có sự hỗ trợ từ các chức năng hỗ trợ kinh doanh, hướng dẫn từ các nhóm ngành hoặc trợ giúp từ các nguồn khác. Việc xác định các chính sách và thủ tục bảo mật có liên quan áp dụng cho các mối quan hệ với bên-thứ-ba là một nỗ lực quan trọng để đảm bảo rằng tất cả các yếu tố của chúng được đáp ứng trong quá trình hoạt động kinh doanh. Điểm mấu chốt rất đơn giản: trong một số tình huống kinh doanh, các chính sách và thủ tục có thể bị bắt buộc bởi các quy định bên ngoài và có thể sự hỗ trợ là cần thiết để đảm bảo sự tuân thủ.



ADMINISTRATION & SECURITY  
VIETNAM

**Mục tiêu Chứng nhận** Chương này đề cập đến mục tiêu 5.3 của kỳ thi CompTIA Security+: Giải thích tầm quan trọng của các chính sách đối với bảo mật của tổ chức.

## Nhân sự

Một phần đáng kể của các vấn đề về bảo mật do-con-người-gây-ra là kết quả của những thực tiễn bảo mật kém cỏi. Những thực tiễn kém cỏi này có thể là của một người dùng cá nhân không tuân theo các chính sách hoặc quy trình bảo mật đã được thiết lập hoặc có thể do thiếu các chính sách, quy trình bảo mật hoặc đào tạo [về bảo mật] trong tổ chức của người dùng đó. Thông qua việc thiết lập, thực thi và giám sát các chính sách liên quan đến nhân sự - *quản lý nhân sự* - một tổ chức có thể tạo ra một khuôn khổ trao quyền cho nhân viên của mình để đạt được các mục đích kinh doanh nhưng vẫn giữ cho họ bị hạn chế trong các thực tiễn bảo mật đã được khuyến nghị. Phần này bao gồm nhiều chủ đề về bảo mật có liên quan đến quản lý nhân sự.

## Chính sách Sử dụng Có thể được chấp thuận

Một *chính sách sử dụng có thể được chấp thuận (acceptable use policy - AUP)* nêu ra những gì tổ chức được coi là sử dụng thích hợp các tài nguyên của mình, chẳng hạn như hệ thống máy tính, email, Internet và mạng. Các tổ chức nên lo lắng về bất kỳ việc sử dụng cho mục đích cá nhân nào đối với các tài sản của tổ chức nhưng không mang lại lợi ích cho công ty.

Mục tiêu của chính sách là đảm bảo năng suất của nhân viên trong khi hạn chế được trách nhiệm tiềm ẩn của tổ chức do việc sử dụng không phù hợp những tài sản của tổ chức gây ra. Chính sách nên phân định một cách rõ ràng về những hoạt động nào không được chấp thuận. AUP cần giải quyết các vấn đề như việc sử dụng các nguồn lực để tiến hành công việc kinh doanh cá nhân, cài đặt phần cứng hoặc phần mềm, truy cập từ xa vào hệ thống và mạng, sao chép phần-mềm-thuộc-sở-hữu của công ty và trách nhiệm của người dùng trong việc bảo vệ tài sản của công ty, bao gồm cả dữ liệu, phần mềm và phần cứng. Các tuyên bố về các hình phạt

khả dĩ nếu bỏ qua bất kỳ chính sách nào (chẳng hạn như chấm dứt hợp đồng) cũng nên được đưa vào.

Liên quan đến việc sử dụng thích hợp các hệ thống và mạng máy tính của tổ chức bởi các nhân viên là việc sử dụng một cách thích hợp bởi tổ chức. Điều quan trọng nhất của những vấn đề này là liệu tổ chức có xem xét việc giám sát việc sử dụng hệ thống và mạng của nhân viên là có phù hợp hay không. Nếu việc giám sát được coi là phù hợp, tổ chức nên bao gồm tuyên bố về tác động này trong một biểu ngữ xuất hiện khi nhân viên đăng nhập vào hệ thống. Điều này liên tục cảnh báo nhân viên và những kẻ xâm nhập tiềm ẩn, rằng hành động của họ phải chịu sự giám sát và mọi hành vi lạm dụng hệ thống sẽ không được dung thứ. Nếu tổ chức cần sử dụng bất kỳ thông tin nào thu thập được trong quá trình giám sát trong một vụ án dân sự hoặc hình sự, vấn đề liệu nhân viên có kỳ vọng về quyền riêng tư hay không, hoặc liệu việc tổ chức đang giám sát có hợp pháp hay không, sẽ được đơn giản hóa nếu tổ chức có thể chỉ ra tuyên bố được hiển thị nhiều lần của mình rằng việc sử dụng hệ thống cấu thành sự đồng ý đối với việc giám sát. Trước khi tiến hành bất kỳ hoạt động giám sát nào hoặc trước khi những từ ngữ thực tế trên thông báo cảnh báo được tạo ra, cỗ vấn pháp lý của tổ chức cần được tham vấn để xác định cách thức thích hợp để giải quyết vấn đề này.

AUP đủ quan trọng để chúng thường được trình bày cho nhân viên trong quá trình chào đón-nhân-viên (on-boarding), với các đợt bồi dưỡng trên cơ sở hàng năm. AUP là cơ sở cho hành vi của nhân viên với hệ thống và các chi tiết cần được làm mới để mọi người có khả năng tuân thủ chúng.



## MÁCH NƯỚC CHO KỲ THI

Hãy đảm bảo rằng bạn hiểu được rằng một chính sách sử dụng có thể được chấp thuận phác thảo nên những gì

CompTIA Security+ - All in One - Exam Guide

1115 | Page

Chuyển ngữ: Nhóm dịch Quản trị và Bảo mật Hệ thống

được coi là hành vi có thể được chấp thuận cho người dùng của một hệ thống máy tính. Chính sách này thường đi cùng với chính sách sử dụng Internet của tổ chức.

### **Luân chuyển Công việc**

Một chính sách khác mang lại rất nhiều lợi ích là *luân chuyển công việc*. Việc luân chuyển qua các công việc khác nhau đem lại cho các cá nhân cái nhìn tốt hơn về cách thức các bộ phận khác nhau của tổ chức có thể tăng cường (hoặc cản trở) công việc kinh doanh như thế nào. Vì vấn đề bảo mật thường là mối quan tâm thứ yếu đối với mọi người trong công việc của họ nên việc luân chuyển các cá nhân qua các vị trí bảo mật có thể giúp tìm hiểu rộng hơn nhiều về các vấn đề bảo mật của tổ chức. Một lợi ích phụ nữa là sự luân chuyển cũng loại bỏ sự cần thiết phải dựa vào một cá nhân để có được chuyên môn bảo mật. Nếu mọi nhiệm vụ bảo mật chỉ thuộc phạm vi công việc của một nhân viên, bảo mật [của tổ chức] sẽ bị ảnh hưởng nếu cá nhân đó rời khỏi tổ chức. Ngoài ra, nếu chỉ một cá nhân hiểu lĩnh vực bảo mật, nếu cá nhân đó trở nên bất bình và quyết định gây hại cho tổ chức thì việc khôi phục sau cuộc tấn công của họ có thể sẽ rất khó khăn.



### **MÁCH NƯỚC CHO KỲ THI**

Việc luân chuyển người dùng giữa các vai trò giúp đảm bảo rằng các hoạt động gian lận không thể được duy trì và cải thiện được nhận thức về bảo mật trong các vai trò khác nhau trong một tổ chức.

### **Kỳ nghỉ Bắt buộc**

Các tổ chức đã cung cấp thời gian nghỉ phép cho nhân viên của họ trong rất nhiều năm. Tuy nhiên, cho đến thời gian gần đây, một số tổ chức đã buộc nhân viên phải dành thời gian này nếu họ không muốn. Một số nhân

viên được lựa chọn “sử dụng hoặc mất đi” thời gian nghỉ phép của họ và nếu họ không sử dụng toàn bộ thời gian [nghỉ phép] của mình, họ sẽ mất ít nhất một phần thời gian đó. Nhiều lập luận có thể được đưa ra về lợi ích của việc nghỉ phép, nhưng quan trọng hơn, xét từ quan điểm bảo mật, một nhân viên không bao giờ nghỉ việc là một dấu hiệu tiềm ẩn của một hoạt động bất chính. Những nhân viên không bao giờ nghỉ phép có thể tham gia vào các hoạt động như gian lận hoặc tham ô và có thể sợ rằng nếu họ đi nghỉ vào kỳ nghỉ, tổ chức sẽ phát hiện ra các hoạt động bất hợp pháp của họ. Do đó, việc yêu cầu nhân viên sử dụng thời gian nghỉ phép của họ thông qua chính sách *kỳ nghỉ bắt buộc* cũng có thể là một cơ chế bảo vệ an ninh. Việc sử dụng kỳ nghỉ bắt buộc như một công cụ để phát hiện gian lận sẽ đòi hỏi nhân viên khác cũng phải được đào tạo về các chức năng của nhân viên đang đi nghỉ. Có được một người thứ hai làm quen với các thủ tục bảo mật cũng là một chính sách tốt trong trường hợp có điều gì đó xảy ra với người chính.

### **Phân tách Nhiệm vụ**

*Phân tách nhiệm vụ* là một nguyên tắc được áp dụng trong rất nhiều tổ chức để đảm bảo rằng không có một cá nhân đơn lẻ nào có khả năng tiến hành các giao dịch một mình. Điều này có nghĩa là mức độ tin tưởng vào bất kỳ một cá nhân nào bị giảm đi, và khả năng bất kỳ cá nhân nào gây ra thiệt hại nghiêm trọng cho tổ chức cũng sẽ giảm đi. Một ví dụ có thể là một tổ chức trong đó một người có khả năng đặt hàng các thiết bị, nhưng một cá nhân khác thực hiện thanh toán. Một cá nhân muốn thực hiện một giao dịch mua trái phép vì lợi ích cá nhân của riêng họ sẽ phải thuyết phục một người khác cùng thực hiện giao dịch.

Việc phân tách các nhiệm vụ như một công cụ bảo mật là một thực tiễn tốt, nhưng có thể bị quá đà và chia nhỏ các giao dịch thành quá nhiều phần hoặc đòi hỏi sự giám sát quá nhiều. Điều này dẫn đến sự không

hiệu quả và thực sự có thể sẽ kém an toàn hơn, vì các cá nhân có thể không xem xét kỹ lưỡng các giao dịch do họ biết những người khác cũng sẽ xem xét chúng. Sự cám dỗ là hoàn thành nhanh một thứ gì đó và giả định rằng ai đó sẽ kiểm tra nó hoặc đã kiểm tra nó.

---



**MÁCH NƯỚC CHO KỲ THI** Một khía cạnh khác của nguyên tắc phân tách nhiệm vụ là nó phân chia trách nhiệm trong một tổ chức để từ đó không một cá nhân riêng lẻ nào trở thành một nhân vật không thể thiếu với tất cả “chìa khóa dẫn đến vương quốc” hoặc kiến thức duy nhất về cách khiến cho mọi thứ hoạt động. Nếu đủ nhiệm vụ đã được phân phối thì việc chỉ định một người chính và một người dự phòng cho mỗi nhiệm vụ sẽ đảm bảo rằng sự tổn thất của bất kỳ cá nhân nào sẽ không có tác động tai hại đến tổ chức.

### **Đặc quyền Ít nhất**

Một trong những nguyên tắc cơ bản nhất trong bảo mật là *đặc quyền ít nhất*, có nghĩa là một đối tượng (có thể là người dùng, ứng dụng hoặc tiến trình) chỉ nên có các quyền và đặc quyền cần thiết để thực hiện nhiệm vụ của nó, và không có thêm các quyền bổ sung. Việc giới hạn các đặc quyền sẽ hạn chế tổng mức độ thiệt hại mà đối tượng có thể gây ra, do đó hạn chế mức độ tiếp xúc với thiệt hại của tổ chức. Người dùng chỉ nên có quyền truy cập vào thông tin và hệ thống cần thiết để thực hiện nhiệm vụ công việc của họ. Việc thực thi nguyên tắc đặc quyền ít nhất giúp tổ chức bảo vệ các tài nguyên nhạy cảm nhất của mình và giúp đảm bảo rằng bất kỳ ai đang tương tác với những tài nguyên này đều có lý do hợp lệ để làm như vậy.

---



**MÁCH NƯỚC CHO KỲ THI** Nguyên tắc đặc quyền ít nhất tuy nhiên bối rắng người dùng chỉ nên có mức độ quyền truy cập cần thiết để thực hiện công việc của mình.

### **Không gian Bàn làm việc Gọn gàng**

Việc ngăn chặn sự tiếp cận với thông tin cũng rất quan trọng trong khu vực làm việc. Các công ty có những thông tin nhạy cảm nên có chính sách *bàn làm việc gọn gàng* quy định rằng không được để thông tin nhạy cảm mà không được bảo vệ trong khu vực làm việc khi người lao động không có mặt để làm nhiệm vụ giám sát. Ngay cả khi rời khỏi khu vực bàn làm việc và đi vào phòng tắm cũng có thể khiến cho thông tin bị lộ ra ngoài và có thể bị xâm phạm. Chính sách bàn làm việc gọn gàng phải xác định và cấm những thứ thoát nhìn không rõ ràng, chẳng hạn như mật khẩu trên giấy dán LƯU Ý dưới bàn phím và tấm lót chuột hoặc trong ngăn kéo bàn không an toàn.

### **Kiểm tra Lý lịch**

Nhân sự là chìa khóa của vấn đề bảo mật trong doanh nghiệp. Việc thuê nhân sự giỏi luôn là một thách thức trong lĩnh vực kỹ thuật, nhưng việc thuê những người đáng tin cậy cũng không kém phần quan trọng, đặc biệt là những người có vai trò chủ chốt có khả năng tiếp cận hệ thống nhiều hơn. Việc thực hiện *kiểm tra lý lịch* định kỳ cung cấp cho nhóm Nhân sự những thông tin cần thiết được yêu cầu để đưa ra các quyết định chính xác. Kiểm tra lý lịch có thể xác nhận công việc trước đây, lý lịch tội phạm, nền tảng tài chính và thậm chí cả hành vi trên mạng xã hội. Tùy thuộc vào ngành, công ty và vị trí, các yếu tố khác nhau từ những lĩnh vực này có thể được bao gồm [*trong quá trình kiểm tra lý lịch - người dịch*].



**LƯU Ý** Người ta thường nghe nói rằng việc thuê một tin tặc bảo mật tài năng đòi hỏi việc phải chấp nhận một ai đó có quá khứ mờ ám. Bỏ qua tính xác thực của nhận xét đó, câu hỏi thực sự cần đặt ra không phải là “Tôi có thuê người này không?” mà đúng hơn là “Tôi có sợ sa thải họ không?”

### **Thỏa thuận Không tiết lộ**

*Thỏa thuận không tiết lộ (NDA)* là những tài liệu tiêu chuẩn của công ty được sử dụng để giải thích ranh giới của tài liệu bí mật của công ty, những thông tin cần được thực thi các biện pháp kiểm soát để ngăn chặn việc tiết lộ chúng cho các bên trái phép. NDA thường được sử dụng để phân định mức độ và loại thông tin cũng như những người mà nó có thể được chia sẻ. NDA có thể được thực hiện giữa bất kỳ hai bên nào, trong đó một bên muốn rằng tài liệu đang được chia sẻ sẽ không được chia sẻ thêm, thực thi tính bảo mật thông qua hợp đồng.



**MÁCH NƯỚC CHO KỲ THI** Các thỏa thuận không tiết lộ là những tài liệu ràng buộc về mặt pháp lý. Các NDA đã được ký kết thường được yêu cầu bởi người sử dụng lao động trong quá trình giới thiệu để đảm bảo nhân viên nhận thức được về quyền riêng tư và tính bảo mật liên quan đến dữ liệu của công ty.

### **Phân tích Phương tiện Xã hội**

Sự gia tăng của các *ứng dụng và mạng truyền thông xã hội* đã làm thay đổi nhiều khía cạnh của hoạt động kinh doanh. Cho dù được sử dụng cho mục đích tiếp thị, truyền thông, quan hệ khách hàng hay một số mục đích khác, mạng truyền thông xã hội có thể được coi là một hình thức bê-

thứ-ba. Một trong những thách thức khi làm việc với các mạng và/hoặc ứng dụng xã hội là các điều khoản sử dụng của chúng. Trong khi mối quan hệ với bên-thứ-ba điển hình bao gồm một tập hợp các thỏa thuận được thương lượng liên quan đến các yêu cầu thì không có bất kỳ cuộc thương lượng nào với các mạng truyền thông xã hội. Lựa chọn duy nhất là chấp nhận các điều khoản dịch vụ của họ, vì vậy điều quan trọng là phải hiểu ý nghĩa của các điều khoản này đối với việc sử dụng mạng xã hội của doanh nghiệp.

Việc sử dụng các trang mạng xã hội của nhân viên tại nơi làm việc mang lại nhiều rủi ro hơn, dưới dạng các vi-rút, sâu và thu thập dữ liệu lừa đảo trực tuyến. Trong những năm trước, các nhà tuyển dụng lo lắng về việc nhân viên sử dụng máy tại nơi làm việc để mua sắm trên eBay hoặc lướt Web hơn là làm việc. Ngày nay, các rủi ro ngày càng tăng lên ngoài thời gian đã mất để giờ đây bao gồm cả việc đưa phần mềm độc hại vào máy làm việc. Thông thường các công ty sử dụng AUP để hạn chế nhân viên sử dụng cá nhân vào những thứ như mạng xã hội, mạng-ngang-hàng (P2P), BitTorrent và các ứng dụng không-liên-quan-đến-công-việc khác.

### **Giới thiệu (Onboarding)**

Yếu tố quan trọng khi *giới thiệu* nhân sự là đảm bảo rằng nhân sự đó nhận thức và hiểu được trách nhiệm của họ đối với việc bảo mật thông tin và tài sản của công ty. Các thỏa thuận với các đối tác kinh doanh có xu hướng khá cụ thể đối với các điều khoản gắn với kỳ vọng chung gắn liền với quá trình hoạt động của doanh nghiệp. Đảm bảo các yếu tố bảo mật chính xác được bao hàm trong quá trình giới thiệu là điều cần thiết để thiết lập các kỳ vọng phù hợp của nhân viên. Những cân nhắc này cần được thực hiện trước khi thiết lập mối quan hệ, không phải được bổ sung thêm vào khi mối quan hệ sắp kết thúc.



## MÁCH NƯỚC CHO KỲ THI

Chính sách giới thiệu nên bao gồm các điều khoản về việc xử lý dữ liệu, loại bỏ dữ liệu, sử dụng có thể được chấp thuận, và bất kỳ biện pháp trừng phạt nào có thể được đưa ra do việc sử dụng sai mục đích.

## Kết thúc (Offboarding)

*Kết thúc* đề cập đến các quy trình và thủ tục được sử dụng khi một nhân viên rời khỏi một tổ chức. Xét từ góc độ bảo mật, quá trình kết thúc đối với nhân sự là rất quan trọng. Việc chấm dứt hợp đồng với nhân viên cần được điều chỉnh để bao gồm việc chấm dứt hoặc vô hiệu hóa mọi tài khoản, bao gồm cả những tài khoản đã được kích hoạt trên thiết bị di động. Không có gì lạ khi tìm thấy những nhân viên bị chấm dứt hợp đồng với tài khoản hoặc thậm chí thiết bị của công ty vẫn kết nối được với mạng công ty nhiều tháng sau khi bị chấm dứt hợp đồng. Tài khoản email nên được xóa ngay lập tức như một phần của chính sách và quy trình chấm dứt hợp đồng của nhân viên. Các thiết bị di động do công ty cung cấp phải được thu hồi sau khi chấm dứt. Các thiết bị mang-theo-thiết-bị-của-riêng-bạn (BYOD) phải được chấm dứt quyền truy cập vào các tài nguyên của công ty như một phần của quá trình kết thúc. Kiểm tra thường xuyên đối với các tài khoản cũ hoặc chưa bị chấm dứt nên được thực hiện để đảm bảo đã xóa hoặc vô hiệu hóa tài khoản của nhân viên đã bị chấm dứt hợp đồng. Phỏng vấn nghỉ việc có thể là những công cụ mạnh mẽ để thu thập thông tin khi mọi người rời khỏi tổ chức.



**MÁCH NƯỚC CHO KỲ THI** Các thủ tục giới thiệu và kết thúc của doanh nghiệp nên được ghi nhận lại thành tài liệu rõ ràng để đảm bảo tính tuân thủ với các yêu cầu pháp lý.

### **Đào tạo Người dùng**

*Đào tạo người dùng* là việc rất quan trọng để đảm bảo rằng người dùng nhận thức được và đang tuân thủ các chính sách và thủ tục thích hợp như một phần của các hoạt động tại nơi làm việc của họ. Như trong tất cả các khóa đào tạo liên-quan-đến-nhân-sự, cần chú ý đến hai yếu tố. Đầu tiên, việc tái đào tạo theo thời gian là điều cần thiết để đảm bảo rằng nhân sự giữ được trình độ kiến thức phù hợp. Thứ hai, khi mọi người thay đổi công việc, một quá trình đánh giá lại cơ sở đào tạo là cần thiết và có thể cần phải đào tạo bổ sung. Việc duy trì hồ sơ đào tạo chính xác của nhân sự là cách duy nhất có thể quản lý việc này trong bất kỳ doanh nghiệp quan trọng nào.

### **Gamification**

*Gamification* là việc sử dụng các trò chơi để tạo điều kiện cho việc đào tạo người dùng. Phương pháp luận này có một số ưu điểm khá thú vị. Đầu tiên, nó làm cho việc học vẹt tài liệu đào tạo trở nên bớt nhàn chán hơn. Thứ hai, nó cho phép một cách tiếp cận dựa-trên-tình-huống toàn diện hơn để đào tạo, với những hậu quả của những quyết định tồi sẽ được chia sẻ với những người tham gia khóa đào tạo. Thứ ba, nó cho phép đào tạo nhóm bằng cách sử dụng các chức năng công việc của mọi người theo cách tạo điều kiện thuận lợi cho cả việc học và kiểm tra các chính sách và thủ tục trong một môi trường không-bị-đe-dọa.

## Bắt cờ (Capture the Flag)

*Sự kiện bắt cờ* là việc đào tạo kỹ năng máy tính thực-hành trong đó người dùng được kiểm tra để xem liệu họ có thể thực hiện các hành động cụ thể hay không. Nếu họ thực hiện các hành động một cách chính xác, họ sẽ phát hiện ra một lá cờ cho thấy rằng họ đã hoàn thành bài kiểm tra một cách thành công. Nhiều cuộc thi tin tặc là các biến thể của các sự kiện bắt-cờ.

## Các chiến dịch Phishing(Phishing Campaigns)

Các *chiến dịch phishing* là một loạt các cuộc tấn công lừa đảo được kết nối nhắm vào một tổ chức. Vì lừa đảo phishing là một phương thức hoạt động của kỹ thuật xã hội, nên mức độ hiểu biết của học viện, tổ chức và cá nhân về đích nhắm mục tiêu của họ càng lớn thì cơ hội thành công càng lớn. Các chiến dịch lừa đảo phishing sử dụng kiến thức phổ biến này để làm tăng tỷ lệ cược của họ, thay vì chỉ tấn công mục tiêu một cách ngẫu nhiên. Đây là lý do tại sao thông tin liên lạc nội bộ liên quan đến các nỗ lực lừa đảo phishing là cực kỳ quan trọng, để cảnh báo người dùng khác rằng hệ thống có thể đang bị tấn công và ý thức cảnh giác cao hơn đối với hình thức tấn công này luôn được đảm bảo.

## Mô phỏng Phishing

Để giúp người dùng tìm hiểu và xác định các cuộc tấn công lừa đảo, có một số phương pháp *mô phỏng lừa đảo phishing* chống lại người dùng. Một nỗ lực lừa đảo phishing được gửi đến người dùng và nếu họ trở thành con mồi của nó, hệ thống sẽ thông báo cho người dùng rằng đây chỉ là một cuộc diễn tập và họ nên thận trọng hơn. Điều này cũng tạo ra một khoảnh khắc có thể đào tạo được, trong đó người dùng có thể được đào tạo chi tiết một cách chính xác về lý do tại sao họ nên phát hiện ra nỗ lực lừa đảo phishing.

## **Đào tạo Dựa-trên-máy-tính (Computer-based Training)**

*Đào tạo dựa-trên-máy-tính (CBT)* là việc sử dụng một chương trình máy tính để quản lý quá trình đào tạo của người sử dụng. Các mô-đun tự theo nhịp độ có thể tạo điều kiện phát triển kỹ năng trên nhiều loại kỹ năng khác nhau và tính linh hoạt của CBT rất hấp dẫn. Không phải tất cả người học đều học tốt trong những trường hợp này, nhưng đối với những người đó, CBT cung cấp một phương pháp đào tạo có khả năng mở rộng và rất hợp lý.

## **Đào tạo Dựa-trên-vai-trò (Role-based Training)**

Để việc đào tạo có hiệu quả, nó cần được nhắm mục tiêu đến người dùng để có liên quan đến vai trò của họ trong chủ đề đào tạo. Mặc dù mọi nhân viên có thể cần được đào tạo nhận thức chung về bảo mật, nhưng họ cũng cần được *đào tạo nhận thức dựa-trên-vai-trò* cụ thể trong các lĩnh vực mà họ có trách nhiệm cá nhân. Đào tạo dựa-trên-vai-trò liên quan đến trách nhiệm bảo mật thông tin là một phần quan trọng của đào tạo về bảo mật thông tin.

Nếu một người có trách nhiệm công việc có thể ảnh hưởng đến bảo mật thông tin thì cần đào tạo theo vai-trò-cụ-thể để đảm bảo rằng cá nhân đó hiểu được những trách nhiệm liên quan đến bảo mật thông tin. Một số vai trò, chẳng hạn như quản trị viên hệ thống hoặc nhà phát triển, có những trách nhiệm bảo mật thông tin đã được xác định một cách rõ ràng. Những vai trò của những người khác, chẳng hạn như quản lý dự án hoặc quản lý mua hàng, có những tác động bảo mật thông tin ít rõ ràng hơn, nhưng những vai trò này cũng cần phải được đào tạo. Trên thực tế, các vai trò ít-ảnh-hưởng hơn nhưng có tác-động-lớn-hơn của quản lý cấp trung có thể có ảnh hưởng lớn đến văn hóa bảo mật thông tin, và do đó, nếu muốn đạt được một kết quả cụ thể thì cần phải đào tạo.



**MÁCH NƯỚC CHO KỲ THI** Hãy chắc chắn rằng bạn đã quen thuộc với các phương pháp đào tạo người dùng khác nhau và chúng đóng vai trò như thế nào trong bảo mật của tổ chức.

### Sự đa dạng của các Kỹ thuật Đào tạo

Không phải tất cả người học đều học theo cùng một kiểu, một số người học bằng cách nhìn, một số người lại học tốt hơn bằng cách nghe. Hầu hết mọi người đều học tốt hơn bằng cách thực hành, nhưng trong một số lĩnh vực, việc thực thi một nhiệm vụ là không thực tế hoặc không khả thi. Điểm mấu chốt là có rất nhiều phương pháp đào tạo, và để có kết quả tốt nhất, điều quan trọng là phải khéo léo kết hợp được các phương pháp đào tạo với tài liệu để có được kết quả tốt nhất. Trong phần trước, một số phương pháp đào tạo khác nhau đã được đề cập đến, bao gồm trò chơi hóa, các bài tập bắt cờ và mô phỏng. Thậm chí, còn có nhiều phương pháp hơn nữa để hoàn thiện nhiều giải pháp đào tạo đa dạng, bao gồm các bài giảng trực-tiếp, nội dung trực tuyến và phát triển kỹ năng dựa-trên-thực-tiễn. Điều quan trọng là phải khéo léo kết hợp được tài liệu với phương pháp và người học, sau đó kiểm tra kết quả để đảm bảo đạt được sự thành công trong đào tạo.

### Quản lý Rủi ro Bên-Thứ-ba

Mỗi doanh nghiệp sẽ có các bên-thứ-ba tương ứng với hoạt động kinh doanh của họ. Cho dù các bên-thứ-ba này là nhà thầu, nhà cung cấp hoặc đối tác kinh doanh, họ đều mang lại cơ hội cho cả rủi ro và phần thưởng.

*Quản lý rủi ro của bên-thứ-ba* là một quá trình tương đối đơn giản. Bước đầu tiên là nhận ra rằng rủi ro đang hiện hữu. Bạn cần phải kiểm kê và đánh giá những rủi ro này và sau đó phát triển các biện pháp giảm thiểu cần thiết để giữ chúng trong phạm vi có thể chấp nhận được. Khái niệm quan trọng là rủi ro không biến mất một cách kỳ diệu vì có một bên-thứ-

ba tham gia, nó vẫn cần được quản lý như tất cả các rủi ro kinh doanh khác.

### **Các Nhà cung cấp**

*Nhà cung cấp* là các công ty hoặc các cá nhân cung cấp nguyên vật liệu hoặc dịch vụ cho một doanh nghiệp. Những mặt hàng này được mua sắm như một phần của quy trình nghiệp vụ và đại diện cho một số hình thức để xuất giá trị đối với công ty đang mua chúng. Nhưng cùng với giá trị cũng có thể đi kèm với rủi ro. Ví dụ, nếu một đề mục có mã nhúng để khiến cho nó hoạt động, điều gì sẽ xảy ra nếu mã nhúng có lỗ hổng? Điều gì sẽ xảy ra nếu một mặt hàng được mua cho một mục đích cụ thể không đáp ứng được các thông số kỹ thuật của nó? Một loạt các rủi ro có thể được đưa ra bởi các nhà cung cấp và những rủi ro này cần phải được kiểm tra và xử lý theo các quy trình quản lý rủi ro tiêu chuẩn.

### **Chuỗi cung ứng**

Một *chuỗi cung ứng* là một tập hợp các công ty hoạt động cùng nhau để quản lý sự dịch chuyển của hàng hóa và dịch vụ giữa các công ty. Nếu bạn đặt hàng một bộ phận từ một nhà cung cấp nước ngoài mà sẽ trở thành một bộ phận của sản phẩm của bạn đang được sản xuất ở một nước khác, làm thế nào để tất cả các bộ phận đến đúng nơi vào đúng thời điểm để lắp ráp? Chuỗi cung ứng xử lý các chi tiết khiến cho tất cả những điều này xảy ra. Từ vận chuyển, đến hải quan và các quy định khác, đến quản lý lịch trình, đây là tất cả các chi tiết cần thiết để các mặt hàng đi từ nơi này đến nơi khác. Nếu một công ty chỉ có một nhà cung cấp duy nhất thì quá trình này tương đối đơn giản. Tuy nhiên, việc có nhiều nhà cung cấp cho nhiều bộ phận ở các giai đoạn khác nhau của chuỗi giá trị của bạn phải làm việc cùng nhau là điều quan trọng của chuỗi cung ứng. Đại dịch năm 2020 đã minh họa điều này một cách rõ ràng, khi các quốc gia đóng cửa biên giới, các công ty gặp khó khăn trong hoạt động, các nhà

máy đóng cửa do công nhân bị ốm và các đơn đặt hàng tại-nhà - và không có điều nào đồng nhất hoặc xảy ra trong cùng một khoảng thời gian. Sự gián đoạn của chuỗi cung ứng toàn cầu gây ra những ảnh hưởng tiếp theo, trong đó các bộ phận dự kiến bị trì hoãn vì các bộ phận không liên quan ở nơi khác bị trì hoãn, do đó làm gián đoạn các chuỗi cung ứng khác nhau. Nhu cầu hiểu và quản lý rủi ro của các chức năng chuỗi cung ứng và chi phí thực của chúng trở nên rất rõ ràng. Rõ ràng là với việc quản lý chuỗi cung ứng bao quát, chi phí thấp hơn có thể đạt được, nhưng có nguy cơ sẽ gặp phải thất bại khi chuỗi cung ứng có vấn đề.

### **Đối tác Kinh doanh**

Các *đối tác kinh doanh* là các thực thể cùng chia sẻ một mối quan hệ với một công ty trong các hoạt động kinh doanh của họ. Các đối tác kinh doanh có thể được kết nạp vào nỗ lực kinh doanh vì nhiều lý do: chia sẻ rủi ro, chia sẻ trách nhiệm pháp lý, chia sẻ chi phí, tận dụng kiến thức chuyên môn và hơn thế nữa. Chìa khóa để tìm hiểu và điều hướng các đối tác kinh doanh liên quan đến an ninh mạng và rủi ro là đảm bảo rằng các rủi ro và trách nhiệm của cả hai phía đối tác đều đã được hiểu và thống nhất trước khi sự kiện rủi ro xảy ra. Mọi mối quan hệ hợp tác đều có rủi ro và phần thưởng, điều quan trọng là hiểu được cấp độ của từng loại và đưa ra các quyết định kinh doanh với một sự hiểu biết rõ ràng về các yếu tố này.

### **Thỏa thuận Mức Dịch vụ (SLA)**

Một *thỏa thuận mức dịch vụ (SLA)* là thỏa thuận được thương lượng giữa các bên nêu ra chi tiết những mong đợi giữa khách hàng và nhà cung cấp dịch vụ. SLA về cơ bản thiết lập mức hiệu suất cần thiết của một dịch vụ theo hợp đồng nhất định. Các SLA thường được bao gồm như một phần của hợp đồng dịch vụ và đặt ra mức độ kỳ vọng về mặt kỹ thuật. Một SLA có thể xác định các dịch vụ cụ thể, mức hiệu suất liên quan đến dịch vụ,

cách thức quản lý và giải quyết vấn đề, v.v... SLA được thương lượng giữa khách hàng và nhà cung cấp và đại diện cho các điều khoản đã-được-thống-nhất. Các yêu cầu bảo mật cụ thể có thể được chỉ định trong SLA và được thực thi sau khi cả hai bên đồng ý. Khi đã được ký kết, SLA sẽ trở thành một tài liệu ràng buộc về mặt pháp lý.

### **Biên bản Ghi nhớ (MOU)**

Một *biên bản ghi nhớ (MOU)* và *biên bản thỏa thuận (MOA)* là các văn bản pháp lý được sử dụng để mô tả một thỏa thuận song phương giữa các bên. Chúng là các thỏa thuận bằng văn bản thể hiện một tập hợp các hành động dự kiến giữa các bên liên quan đến một số mục đích hoặc mục tiêu chung. Thông thường, MOU có các mô tả cấp-cao-hơn, trong khi MOA cụ thể hơn, tuy nhiên, ranh giới giữa hai thuật ngữ pháp lý này rất mờ nhạt và chúng thường được sử dụng thay thế cho nhau. Cả hai đều chính thức và chi tiết hơn một cái bắt tay đơn giản, nhưng nhìn chung chúng thiếu các quyền ràng buộc của một hợp đồng. MOU/MOA cũng thường được sử dụng giữa các đơn vị khác nhau trong phạm vi một tổ chức để trình bày chi tiết các kỳ vọng liên quan đến lợi ích kinh doanh chung, bao gồm cả các yêu cầu về bảo mật.

### **Phân tích Hệ thống Đo lường (MSA)**

Rất nhiều quy trình quản lý rủi ro bảo mật dựa vào việc đo lường các sự vật hoặc sự kiện. Các phép đo và hệ thống đo lường phải được hiệu chuẩn để đảm bảo chúng đang đánh giá đối tượng quan tâm thực tế. *Phân tích hệ thống đo lường (MSA)* là một lĩnh vực nghiên cứu để kiểm tra các hệ thống đo lường về độ chính xác và độ chuẩn xác. Trước khi một doanh nghiệp dựa vào các hệ thống đo lường, điều quan trọng là phải tìm hiểu xem liệu hệ thống đo lường đã được chọn có được chấp nhận cho mục đích sử dụng hay không, để tìm hiểu các nguồn khác nhau của sự biến đổi có trong nó và để xác định và tìm hiểu các nguồn gốc của sai lệch,

lỗi và các yếu tố có liên quan đến độ lặp lại và độ tái lập. Việc thực hiện phân tích hệ thống đo lường trên các hệ thống đo lường được sử dụng trong hệ thống bảo mật là quá trình có cấu trúc để có được thông tin đó và có được sự tự tin vào các biện pháp đã được phát triển và sử dụng từ hệ thống.

### **Thỏa thuận Đối tác Kinh doanh (BPA)**

*Thỏa thuận Đối tác kinh doanh (BPA)* là một thỏa thuận pháp lý giữa các đối tác thiết lập nên các điều khoản, điều kiện và kỳ vọng của mỗi quan hệ giữa các đối tác. Những chi tiết này có thể bao hàm nhiều vấn đề, bao gồm các vấn đề điển hình như phân chia lãi và lỗ, trách nhiệm của từng đối tác, việc thêm hoặc loại bỏ đối tác và bất kỳ vấn đề nào khác. Đạo luật Đối tác thống nhất (Uniform Partnership Act - UPA), được thiết lập bởi luật lệ và công ước của tiểu bang, đưa ra một bộ quy tắc thống nhất liên quan đến các quan hệ đối tác để giải quyết bất kỳ điều khoản đối tác nào. Các điều khoản trong UPA được thiết kế là "một kích thước phù hợp với tất cả" và thường không vì lợi ích tốt nhất của bất kỳ quan hệ đối tác cụ thể nào. Để tránh những kết quả không mong muốn có thể xảy ra từ các điều khoản UPA, tốt nhất là các quan hệ đối tác nên trình bày các chi tiết cụ thể trong một BPA.



**MÁCH NƯỚC CHO KỲ THI** Hãy chắc chắn rằng bạn hiểu được sự khác biệt giữa các thỏa thuận về khả năng tương tác lẫn nhau như SLA, BPA, và MOU/MOA của kỳ thi CompTIA Security+. Tất cả những thỏa thuận này đều có thể được sử dụng để truyền đạt các yêu cầu bảo mật giữa các bên, nhưng từng thỏa thuận sẽ cụ thể về thời điểm nó nên được sử dụng. Hãy xem xét cách sử dụng để biết được những gợi ý sẽ được áp dụng.

## Kết thúc Vòng đời (EOL)

*Kết thúc Vòng đời (EOL)* hoặc *kết thúc hỗ trợ* là khi nhà sản xuất ngừng bán một mặt hàng nào đó. Trong hầu hết các trường hợp, nhà sản xuất không còn cung cấp các dịch vụ bảo trì hoặc cập nhật nữa. Trong một số trường hợp, ngày này được thông báo là một ngày trong tương lai, sau khi kết thúc sự hỗ trợ. Khi một thứ gì đó bước vào giai đoạn EOL, nó đã đi đến cuối vòng đời của nó và việc nâng cấp/thay thế cần phải được lên kế hoạch và thực thi. Khi một sản phẩm [phần mềm hoặc ứng dụng] bước vào giai đoạn EOL, các bản vá bảo mật có thể vẫn được sản xuất và phân phối.

## Kết thúc Vòng đời Dịch vụ - Kết thúc Thời gian sử dụng (EOSL)

*Kết thúc Thời gian sử dụng (EOSL)* là thuật ngữ được sử dụng để biểu thị rằng một thứ gì đó đã hết "thời hạn sử dụng". Khi EOSL xảy ra, nhà cung cấp mặt hàng hoặc dịch vụ đó thường sẽ không bán hoặc cập nhật nó nữa. Đôi khi kết thúc việc cập nhật sẽ là một ngày cụ thể trong tương lai. EOSL thường xảy ra do các mô hình mới hơn đã được phát hành, thay thế cho mô hình cũ hơn. Trong giai đoạn EOSL, một số nhà sản xuất vẫn có thể cung cấp các tùy chọn bảo trì, nhưng thường ở mức giá khá cao. Các phiên bản phần mềm cũ đã gặp phải vấn đề này, trong đó các hệ thống quan trọng không thể dễ dàng được nâng cấp và thay vào đó phải có hợp đồng với nhà cung cấp ban đầu để duy trì hệ thống trước thời điểm EOSL bình thường.



## MÁCH NƯỚC CHO KỲ THI

Đừng bị nhầm lẫn! *Kết thúc Vòng đời (EOL)* là thuật ngữ được sử dụng để biểu thị rằng một thứ gì đó đã kết thúc "vòng đời hữu ích" của nó. *Kết thúc Vòng đời Dịch vụ (EOSL)* hoặc *kết thúc sự hỗ trợ* là khi nhà sản xuất ngừng bán một mặt hàng. Trong

hầu hết các trường hợp, nhà sản xuất không còn cung cấp các dịch vụ bảo trì hoặc các gói cập nhật nữa.

### **NDA**

Các thỏa thuận không tiết lộ đã được đề cập trước đây cũng trong chương này, và chúng hoạt động theo cùng một cách thức liên quan đến các bên-thứ-ba. Bất kể khi nào thông tin được chia sẻ với một bên-thứ-ba, bất kể trong hay ngoài công ty, nếu thực thể đang chia sẻ mong muốn có những điều khoản mang tính hợp đồng để giới hạn việc chia sẻ hoặc tiết lộ, một DNA sẽ được sử dụng.

### **Dữ liệu**

Việc tích hợp hệ thống với nội bộ hoặc các bên-thứ-ba thường có liên quan đến chia sẻ dữ liệu. Dữ liệu có thể được chia sẻ vì mục đích xử lý hoặc lưu trữ. Biện pháp kiểm soát trên dữ liệu là một vấn đề cực kỳ quan trọng trong các mối quan hệ với bên-thứ-ba. Một loạt các câu hỏi cần phải được giải quyết. Ví dụ, câu hỏi về “ai sở hữu dữ liệu” – cả dữ liệu đã được chia sẻ với các bên-thứ-ba lần những dữ liệu sau đó được phát triển như một phần của mối quan hệ - là một vấn đề cần phải được xác lập.

### **Phân loại**

Một thành phần quan trọng của bảo mật CNTT là việc bảo vệ thông tin được xử lý và lưu trữ trên hệ thống máy tính và mạng. Các tổ chức xử lý rất nhiều loại thông tin khác nhau và họ cần nhận thức được rằng không phải thông tin nào cũng có tầm quan trọng hoặc độ nhạy cảm như nhau. Điều này đòi hỏi phải phân loại thông tin thành nhiều thể loại khác nhau, mỗi thể loại sẽ có những yêu cầu riêng để xử lý thông tin. Các yếu tố ảnh hưởng đến việc phân loại thông tin cụ thể bao gồm giá trị của nó đối với tổ chức (tác động của nó đối với tổ chức sẽ là gì nếu thông tin này bị mất đi?), tuổi của nó và các luật lệ hoặc quy định chi phối việc bảo vệ

thông tin đó. Phân loại dữ liệu được đề cập chi tiết trong Chương 35, "Quyền riêng tư".

### **Quản trị**

*Quản trị* dữ liệu là quá trình quản lý tính sẵn sàng, hữu ích, toàn vẹn và bảo mật của dữ liệu trong các hệ thống của doanh nghiệp. Việc này phải được thực hiện theo chính sách, vì nó liên quan đến một số lượng lớn chủ sở hữu và người dùng dữ liệu. Quản trị dữ liệu nên có các tiêu chuẩn và chính sách dữ liệu được thiết lập để kiểm soát việc sử dụng, bảo mật và lưu giữ dữ liệu. Quản trị hiệu quả đảm bảo rằng việc sử dụng dữ liệu nhất quán với các chính sách, các phần tử dữ liệu là đáng tin cậy và dữ liệu không bị sử dụng sai mục đích. Vai trò và trách nhiệm của những người liên quan đến quản trị dữ liệu được đề cập đến trong Chương 35, "Quyền riêng tư".

### **Lưu giữ**

*Lưu giữ* dữ liệu là quá trình quản lý vòng đời của dữ liệu với trọng tâm là thời điểm dữ liệu kết thúc vòng đời hữu ích của nó đối với một tổ chức. Việc duy trì những dữ liệu cũ, dư thừa không còn phục vụ cho mục đích kinh doanh chỉ thể hiện những rủi ro hệ thống, do đó cần phải được xóa khỏi hệ thống và được tiêu hủy một cách thích hợp. Việc có được một chính sách lưu giữ dữ liệu được phối hợp không chỉ đơn thuần là gán nhãn thời gian lưu trữ các loại dữ liệu khác nhau. Một số loại dữ liệu, hồ sơ tài chính, hồ sơ thuế, v.v... có các yêu cầu quy định cụ thể về thời gian chúng phải được duy trì. Chính sách lưu giữ cũng phải tính đến những vấn đề như lệnh tạm giữ kiện tụng về các phần tử dữ liệu cụ thể, tạm dừng việc tiêu hủy các phần tử đó và các mối quan tâm về quy định. Việc phát triển một chính sách lưu giữ dữ liệu tương đối dễ dàng, nhưng việc triển khai chính sách này một cách hiệu quả và có hiệu lực có thể sẽ khó khăn hơn đáng kể do tính chất đa dạng của dữ liệu trong toàn doanh

nghiệp và thách thức gây ra bởi các quy trình tổ tụng theo từng hạng-mục-cụ-thể.



**MÁCH NƯỚC CHO KỲ THI** Lệnh tạm giữ kiện tụng là chỉ thị của tòa án nhằm lưu giữ tất cả các hồ sơ liên quan đến đối tượng của một vụ kiện và lệnh này được ưu tiên hơn các chính sách lưu giữ dữ liệu thông thường.

### Các Chính sách Thông tin đăng nhập

*Chính sách thông tin đăng nhập* đề cập đến các quy trình, dịch vụ và phần mềm được sử dụng để lưu trữ, quản lý và ghi nhật ký việc sử dụng thông tin đăng nhập của người dùng. Các giải pháp quản lý thông tin đăng nhập dựa-trên-người-dùng thường nhằm mục đích hỗ trợ người dùng cuối quản lý bộ mật khẩu ngày càng nhiều của họ. Có các sản phẩm quản lý thông tin đăng nhập cung cấp một phương tiện an toàn để lưu trữ thông tin đăng nhập của người dùng và cung cấp chúng trên nhiều nền tảng, từ các kho lưu trữ cục bộ đến các vị trí lưu trữ đám mây. Các giải pháp quản lý thông tin đăng nhập hệ thống mang lại những lợi thế tương tự cho chủ sở hữu hệ thống, cung cấp một phương tiện để quản lý những người được cấp quyền truy cập vào các tài nguyên khác nhau trong toàn doanh nghiệp.

Phương pháp quan trọng được sử dụng để kiểm soát quyền truy cập vào hầu hết các hệ thống vẫn là phương pháp dựa trên mật khẩu. Cùng với chính sách tài khoản được thực thi một cách mạnh mẽ để cấm chia sẻ mật khẩu và thông tin đăng nhập, việc sử dụng mật khẩu tạo ra nền tảng để hỗ trợ cho khái niệm rằng mỗi ID người dùng phải có thể truy nguyên được hoạt động của một người. Mật khẩu cần phải được quản lý để cung cấp mức độ bảo vệ thích hợp. Chúng cần phải đủ mạnh để chống lại các

cuộc tấn công và không quá khó để người dùng ghi nhớ. Một chính sách tài khoản có thể hoạt động để đảm bảo rằng các bước cần thiết đã được thực hiện để ban hành một giải pháp mật khẩu an toàn, cho cả người dùng và hệ thống cơ sở hạ tầng mật khẩu.

### **Nhân viên**

Người dùng, hoặc *nhân viên*, yêu cầu thông tin đăng nhập để truy cập các tài nguyên hệ thống cụ thể như một phần nhiệm vụ công việc của họ. Việc quản lý ai nhận được thông tin đăng nhập nào là một phần của hệ thống quản lý quyền truy cập và cấp phép và phải được quản lý thông qua chính sách thông tin đăng nhập. Chi tiết về thông tin đăng nhập và chính sách kiểm soát truy cập được đề cập trong Chương 24, "Triển khai Xác thực và Cấp phép".

### **Bên-thứ-ba**

Cũng giống như người dùng bên trong một công ty yêu cầu thông tin đăng nhập để truy cập hệ thống, có những trường hợp bên-thứ-ba cũng yêu cầu những thông tin đăng nhập. Cho dù thông tin đăng nhập cho một hệ thống hay quyền truy cập vật lý, thông tin đăng nhập của *bên-thứ-ba* nên được quản lý bằng các chính sách để đảm bảo chúng được cấp khi cần thiết cho các bên phù hợp, và khi không còn cần quyền truy cập, chúng sẽ được thu hồi một cách thích hợp.

### **Các Thiết bị**

Thiết bị là các phần tử vật lý yêu cầu quyền truy cập vào mạng hoặc hệ thống của doanh nghiệp. Để có được quyền truy cập này, chúng cũng yêu cầu thông tin đăng nhập giống như người dùng là con người. Không giống như người dùng con người, các thiết bị không có khả năng thay đổi mật khẩu của chúng, vì vậy chúng thường được kích hoạt với mật khẩu rất dài để ngăn chặn việc bị bẻ khóa và có thời gian hết hạn mật khẩu lâu-hơn-bình-thường. Điều này khiến cho các tài khoản thiết bị trở thành mục tiêu

tự nhiên cho những kẻ tấn công, trong khi mật khẩu rất dài của chúng có thể không bẻ khóa được, nhưng chúng có thể bị đánh cắp. Tài khoản thiết bị phải được kiểm soát bởi chính sách và được giám sát theo phạm vi sử dụng.

### Các Tài khoản Dịch vụ

Các *tài khoản dịch vụ* là những tài khoản đặc biệt được sử dụng để cấp quyền cho dịch vụ hoặc hoạt động hệ thống không-do-con-người-khởi-xướng (non-human-initiated). Rất nhiều hệ thống máy tính có các dịch vụ tự động hoạt động như một phần của hệ điều hành để kích hoạt một số chức năng nhất định. Các chương trình đặc biệt này yêu cầu quyền giống như tất cả các chương trình hoạt động và tài khoản dịch vụ là cơ chế được sử dụng để cho phép các mục này hoạt động. Tài khoản cũng đòi hỏi việc kiểm tra và giám sát vì chúng chạy dưới chế độ nền (background) và thường có những năng lực đáng kể. Doanh nghiệp cần có một chính sách để xác định ai có thể kích hoạt và vận hành các tài khoản này cũng như các chức năng kiểm toán của chúng.



### MÁCH NƯỚC CHO KỲ THI

Vì các tài khoản thiết bị và tài khoản dịch vụ không có người vận hành nên mật khẩu của chúng có các thuộc tính đặc biệt, bao gồm cả thời gian hết hạn rất dài. Điều này khiến cho chúng dễ bị lạm dụng hơn, vì vậy phạm vi và việc sử dụng chúng cần phải được giám sát.

### Các Tài khoản Quản trị viên/Tài khoản Root

Các tài khoản *quản trị viên* (*administrator*) và *tài khoản gốc* (*root*) có các đặc quyền cao hơn và đòi hỏi sự giám sát chặt chẽ hơn về việc ai được cung cấp những thông tin đăng nhập này cũng như cách chúng được sử dụng và giám sát như thế nào. Thông tin chi tiết liên quan đến các biện

pháp bảo vệ bổ sung cần thiết cho các tài khoản này được nêu chi tiết trong Chương 24, "Triển khai Xác thực và Cấp phép".

### Các Chính sách Tổ chức

Các bộ phận quan trọng trong bất kỳ phương pháp tiếp cận triển khai bảo mật của tổ chức nào cũng đều bao gồm các chính sách, thủ tục, tiêu chuẩn và hướng dẫn được thiết lập để nêu chi tiết những gì người dùng và quản trị viên nên thực hiện để duy trì tính bảo mật của hệ thống và mạng. Nói chung, những tài liệu này cung cấp hướng dẫn cần thiết để xác định cách thức bảo mật sẽ được triển khai trong tổ chức như thế nào. Với hướng dẫn này, công nghệ và cơ chế bảo mật cụ thể cần thiết có thể được lên kế hoạch.

Các *chính sách* là những tuyên bố rộng rãi, cấp-cao về những gì tổ chức muốn hoàn thành. Chúng được đưa ra bởi cấp quản lý khi đặt ra quan điểm của tổ chức về một số vấn đề. Thủ tục là các hướng dẫn theo-từng-bước về cách triển khai các chính sách trong tổ chức. Chúng mô tả một cách chính xác cách thức mà nhân viên được kỳ vọng sẽ hành động trong một tình huống nhất định hoặc để hoàn thành một nhiệm vụ cụ thể. Tiêu chuẩn là các yếu tố bắt buộc liên quan đến việc thực hiện một chính sách. Chúng là các thông số kỹ thuật đã được chấp nhận, cung cấp các chi tiết cụ thể về cách một chính sách sẽ được thực thi như thế nào. Một số tiêu chuẩn được định hướng bởi bên ngoài. Ví dụ, các quy định đối với các tổ chức tài chính và ngân hàng đòi hỏi các biện pháp bảo mật nhất định phải được thực hiện theo quy định của pháp luật. Các tiêu chuẩn khác có thể được tổ chức đặt ra để đáp ứng các mục tiêu bảo mật của chính mình. Các hướng dẫn là các khuyến nghị liên quan đến một chính sách. Thuật ngữ quan trọng trong trường hợp này là các *khuyến nghị* - hướng dẫn không phải là các bước bắt buộc.

## Quản lý Thay đổi

Mục đích của *quản lý thay đổi* là đảm bảo sự tuân thủ các quy trình thích hợp khi những sửa đổi đối với cơ sở hạ tầng CNTT được thực hiện. Những sửa đổi này có thể được thúc đẩy bởi một số sự kiện khác nhau, bao gồm luật lệ mới, các phiên bản cập nhật của phần mềm hoặc phần cứng, triển khai phần mềm hoặc phần cứng mới và các cải tiến đối với cơ sở hạ tầng. Thuật ngữ *quản lý* ngụ ý rằng quá trình này cần phải được kiểm soát theo một cách thức có hệ thống nào đó và đó thực sự là mục đích. Những thay đổi đối với cơ sở hạ tầng có thể có tác động bất lợi đến hoạt động. Các phiên bản mới của hệ điều hành hoặc phần mềm ứng dụng có thể không tương thích với phần mềm hoặc phần cứng khác mà tổ chức đang sử dụng. Nếu không có quy trình để quản lý sự thay đổi, một tổ chức có thể đột nhiên thấy bản thân mình không thể tiến hành hoạt động kinh doanh. Một quy trình quản lý thay đổi nên bao gồm các giai đoạn khác nhau, bao gồm phương pháp để yêu cầu thay đổi cơ sở hạ tầng, quy trình xem xét và phê duyệt yêu cầu, kiểm tra hậu quả của thay đổi, giải quyết (hoặc giảm thiểu) bất kỳ tác động bất lợi nào mà thay đổi có thể gánh chịu, thực hiện thay đổi và lập tài liệu về quá trình liên quan đến thay đổi.

## Kiểm soát Thay đổi

*Kiểm soát thay đổi* là quá trình về việc những thay đổi được tìm nguồn gốc, phân tích và quản lý như thế nào. Kiểm soát thay đổi là một tập hợp con của quản lý thay đổi tập trung vào các chi tiết của một thay đổi và cách thức mà nó được lập thành văn bản.



## MÁCH NƯỚC CHO KỲ THI

Quản lý thay đổi là về quá trình áp dụng sự thay đổi. Kiểm soát thay đổi là về các chi tiết của bản thân sự thay đổi.

## Quản lý Tài sản

*Quản lý tài sản* là các chính sách và quy trình được sử dụng để quản lý các thành phần của hệ thống, bao gồm phần cứng, phần mềm và dữ liệu được chứa bên trong chúng. Để bảo vệ hệ thống, người ta phải có một số hình thức kiểm soát đối với những tài sản này và việc quản lý tài sản bao gồm các quy trình được sử dụng để giữ cho doanh nghiệp có quyền kiểm soát chủ động những thành phần có giá trị này. Việc không kiểm soát được phần cứng có thể dẫn đến việc các thiết bị mạng hoặc máy tính giả mạo truy cập vào hệ thống. Việc không kiểm soát phần mềm có thể dẫn đến các lỗ hổng ở cấp-hệ-thống cho phép những kẻ tấn công chiếm quyền kiểm soát trên hệ thống và dữ liệu của nó. Không kiểm soát được nội dung dữ liệu có thể dẫn đến nhiều hình thức lỗi. Điều này khiến cho việc quản lý tài sản trở thành một trong những khía cạnh quan trọng nhất của bảo mật và nó được xếp hạng ở phần đầu của hầu như mọi danh sách tiêu chuẩn về các biện pháp kiểm soát.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với tầm quan trọng của các chính sách đối với sự bảo mật của tổ chức. Chương mở đầu bằng một phần thảo luận về các chính sách nhân sự. Các chính sách này bao gồm chính sách sử dụng có thể được chấp thuận, luân chuyển công việc và nghỉ phép bắt buộc. Tiếp theo là một cuộc thảo luận về sự tách biệt nhiệm vụ và ít đặc quyền nhất. Các chính sách khác cũng được thảo luận trong phần này bao gồm chính sách bàn làm việc gọn gàng, sử dụng kiểm tra lý lịch, thỏa thuận không tiết lộ và phân tích phương tiện truyền thông xã hội. Các chính sách giới thiệu và kết thúc cũng đã được trình bày. Phần nói về đào tạo người dùng bao gồm các chủ đề về trò chơi hóa, sự kiện bắt-cờ, các chiến dịch và mô phỏng lừa đảo, đào tạo dựa-trên-máy-tính và đào tạo dựa-trên-vai-trò. Tiếp theo là xem xét tính đa dạng của các kỹ thuật đào tạo.

Sau đó, chương này đã xem xét các chính sách quản lý rủi ro của bên-thứ-ba, bao gồm các chính sách dành cho nhà cung cấp, chuỗi cung ứng và các đối tác kinh doanh. Các văn bản pháp lý về thỏa thuận mức dịch vụ, biên bản ghi nhớ, phân tích hệ thống đo lường và thỏa thuận đối tác kinh doanh đã được trình bày. Một cuộc thảo luận về những cân nhắc kết thúc-vòng-đời và kết-thúc-vòng-đời-dịch-vụ đã được trình bày. Phần này đã kết thúc bằng việc xem xét các chính sách NDA liên quan đến các bên-thứ-ba.

Các chính sách dữ liệu bao gồm phân loại, quản trị và lưu giữ dữ liệu đã được trình bày. Tiếp theo, việc xem xét các chính sách thông tin đăng nhập bao gồm nhân sự, bên-thứ-ba, thiết bị và tài khoản dịch vụ đã được nêu ra.

Chương này kết thúc bằng việc xem xét các chính sách tổ chức bao gồm quản lý thay đổi, kiểm soát thay đổi và quản lý tài sản.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Điều nào dưới đây là một mô tả về một thỏa thuận đối tác kinh doanh (BPA)?

  - A. Một thỏa thuận được thương lượng giữa các bên nêu chi tiết về những kỳ vọng giữa khách hàng và nhà cung cấp dịch vụ
  - B. Một thỏa thuận pháp lý giữa các chủ thể thiết lập các điều khoản, điều kiện và kỳ vọng của mối quan hệ giữa các thực thể.
  - C. Một thỏa thuận đặc biệt giữa các tổ chức có hệ thống CNTT được kết nối với nhau, mục đích của nó là ghi nhận lại các yêu cầu bảo mật liên quan đến kết nối với nhau.
  - D. Một thỏa thuận bằng văn bản thể hiện một tập hợp các hành động dự kiến giữa các bên liên quan đến một số mục đích hoặc mục tiêu chung.
2. Điều nào dưới đây được sử dụng để vẽ cơ bản, thiết lập mức độ hiệu suất cần thiết của một dịch vụ theo hợp đồng nhất định?

  - A. Biên bản ghi nhớ (MOU)
  - B. Thỏa thuận không tiết lộ (NDA)
  - C. Biên bản thỏa thuận (MOA)
  - D. Thỏa thuận mức dịch vụ (SLA)
3. Điều nào sau đây là một vấn đề cần phải được giải quyết nếu một tổ chức thực thi chính sách nghỉ phép bắt buộc?

  - A. Việc thực thi chính sách nghỉ phép bắt buộc trong hầu hết các trường hợp là một chính sách tốn kém.

- B.** Việc sử dụng kỳ nghỉ bắt buộc như một công cụ để phát hiện gian lận sẽ đòi hỏi những người khác cũng phải được đào tạo về các chức năng của nhân viên đang đi nghỉ.
- C.** Các kỳ nghỉ thường xảy ra vào thời điểm không thích hợp nhất đối với tổ chức và có thể ảnh hưởng đến khả năng hoàn thành các dự án hoặc cung cấp dịch vụ của tổ chức.
- D.** Việc bắt buộc nhân viên đi nghỉ trong khi họ không muốn thường xuyên sẽ khiến cho nhân viên bất mãn và có thể gây ra một mối đe dọa bảo mật khác.
- 4.** Lý do nào sau đây là tốt nhất để tổ chức có chính sách luân chuyển công việc? (Chọn tất cả các đáp án đúng).
- A.** Vì bảo mật thường là mối quan tâm thứ yếu đối với mọi người trong công việc của họ nên việc luân chuyển các cá nhân qua các vị trí bảo mật có thể dẫn đến hiểu biết rộng hơn nhiều về các vấn đề bảo mật của tổ chức.
- B.** Nó giúp duy trì tinh thần của nhân viên ở mức cao.
- C.** Nó đảm bảo tất cả các hoạt động quan trọng vẫn có thể được hoàn thành nếu việc cắt giảm ngân sách dẫn đến việc một số nhân viên phải thôi việc.
- D.** Nó loại bỏ sự cần thiết phải dựa vào một cá nhân để có kiến thức chuyên môn về bảo mật.
- 5.** Phát biểu nào sau đây là đúng khi bàn về phân tách nhiệm vụ? (Chọn tất cả các đáp án đúng).
- A.** Phân tách nhiệm vụ là một nguyên tắc được áp dụng trong nhiều tổ chức để đảm bảo rằng không một cá nhân nào có khả năng thực hiện các giao dịch một mình.
- B.** Thực hiện phân tách nhiệm vụ có nghĩa là mức độ tin cậy đối với bất kỳ cá nhân nào bị giảm đi và khả năng của bất kỳ cá

nhân nào gây ra thiệt hại nghiêm trọng cho tổ chức cũng giảm đi.

- C.** Phân tách các nhiệm vụ như một công cụ bảo mật là một thực tiễn tốt, nhưng có thể làm quá đà và chia nhỏ các giao dịch thành quá nhiều phần hoặc yêu cầu giám sát quá nhiều.
- D.** Phân tách nhiệm vụ dàn trải trách nhiệm trong một tổ chức để không một cá nhân nào trở thành cá nhân không thể thiếu với tất cả "chìa khóa dẫn đến vương quốc" hoặc kiến thức duy nhất về cách thức khiến cho mọi thứ hoạt động.
- 6.** Phát biểu nào sau đây là đúng đối với chính sách bàn làm việc gọn gàng đối với bảo mật? (Chọn tất cả các đáp án đúng).
- A.** Mặc dù chính sách bàn làm việc gọn gàng tạo ra một môi trường làm việc dễ chịu, nhưng nó thực sự có rất ít tác động đến bảo mật.
- B.** Không được để thông tin nhạy cảm mà không được bảo mật trong khu vực làm việc khi người lao động không có mặt để làm nhiệm vụ bảo vệ nó.
- C.** Ngay cả khi rời khỏi khu vực bàn làm việc và đi vào phòng tắm cũng có thể khiến thông tin bị lộ và có thể bị xâm phạm.
- D.** Chính sách bàn làm việc gọn gàng phải xác định và cấm những thứ thoát nhìn không rõ ràng, chẳng hạn như mật khẩu trên giấy dán LƯU Ý đặt bên dưới bàn phím và tấm lót chuột.
- 7.** Điều nào sau đây là thuật ngữ chỉ tài liệu được sử dụng để giải thích về những ranh giới của tài liệu bí mật của công ty, thông tin cần được kiểm soát để ngăn chặn việc tiết lộ cho các bên trái phép và để đạt được thỏa thuận tuân theo các giới hạn này?
- A.** Thỏa thuận không tiết lộ (NDA)
- B.** Thỏa thuận truy cập dữ liệu (Data access agreement - DAA)
- C.** Thỏa thuận tiết lộ dữ liệu (Data disclosure agreement - DDA)

- D. Thỏa thuận phát hành dữ liệu (Data release agreement - DRA)**
- 8.** Tên gọi được đặt cho một chính sách nêu rõ những gì một tổ chức coi là sử dụng hợp lý các nguồn lực của mình - chẳng hạn như hệ thống máy tính, email, Internet và mạng - là gì?
- A. Chính sách sử dụng tài nguyên (Resource usage policy - RUP)**
  - B. Chính sách sử dụng tài nguyên được chấp nhận (Acceptable use of resource policy - AURP)**
  - C. Chính sách sử dụng của tổ chức (Organizational use policy - OUP)**
  - D. Chính sách sử dụng được chấp thuận (Acceptable use policy - AUP)**
- 9.** Thuật ngữ chính xác để theo dõi các vấn đề liên quan đến việc nâng cấp một thành phần trong cụm lắp ráp con - cụ thể là tên gọi của phiên bản phần mềm mới hơn - là gì?
- A. Rủi ro của nhà cung cấp**
  - B. Kiểm soát thay đổi**
  - C. Rủi ro chuỗi cung ứng**
  - D. Quản lý thay đổi.**
- 10.** Tài khoản nào trong số những tài khoản này có rủi ro lớn hơn do sự xâm nhập của tin tặc từ bên ngoài?
- A. Tài khoản người dùng**
  - B. Tài khoản tạm thời**
  - C. Tài khoản dịch vụ**
  - D. Tài khoản của bên-thứ-ba.**

## Đáp án

1. **B.** Một thỏa thuận đối tác kinh doanh là một thỏa thuận mang tính pháp lý giữa các chủ thể thiết lập các điều khoản, điều kiện và kỳ vọng về mối quan hệ giữa các chủ thể.
2. **D.** Một thỏa thuận mức dịch vụ (SLA) về cơ bản đặt ra mức hiệu suất cần thiết cho một dịch vụ theo hợp đồng nhất định.
3. **B.** Việc sử dụng kỳ nghỉ bắt buộc như một công cụ để phát hiện gian lận sẽ đòi hỏi người khác cũng phải được đào tạo về các chức năng của nhân viên đang đi nghỉ. Do đó, tổ chức phải đảm bảo rằng họ có một người thứ hai quen thuộc với nhiệm vụ của nhân viên đang đi nghỉ.
4. **A** và **D.** Vì bảo mật thường được mọi người, trong công việc của họ, coi là mối quan tâm thứ yếu, nên việc luân chuyển các cá nhân thông qua các vị trí bảo mật có thể mang lại hiểu biết rộng hơn nhiều về các vấn đề bảo mật của tổ chức. Một lợi ích phụ nữa là nó cũng loại bỏ sự cần thiết phải dựa vào một cá nhân để có chuyên môn bảo mật. Nếu tất cả các nhiệm vụ bảo mật là lĩnh vực chỉ của một nhân viên, bảo mật sẽ bị ảnh hưởng nếu cá nhân đó rời khỏi tổ chức.
5. **A, B, C** và **D.** Tất cả các đáp án đều đúng khi thảo luận về việc phân tách nhiệm vụ.
6. **B, C** và **D.** Chính sách bàn làm việc gọn gàng thực sự có thể có tác động tích cực đến bảo mật vì những lý do đã được liệt kê.
7. **A.** Thỏa thuận không tiết lộ (NDA) là tài liệu tiêu chuẩn của công ty được sử dụng để giải thích ranh giới của tài liệu bí mật của công ty, thông tin cần phải được kiểm soát để ngăn chặn việc tiết lộ cho các bên trái phép.

- 8. D.** Chính sách sử dụng được chấp thuận (AUP) nêu rõ những gì tổ chức coi là sử dụng thích hợp các tài nguyên của mình, chẳng hạn như hệ thống máy tính, email, Internet và mạng.
- 9. B.** Theo dõi và quản lý các chi tiết của một thay đổi là kiểm soát thay đổi. Quá trình này là quản lý thay đổi.
- 10. C.** Các tài khoản không có người dùng như các tài khoản thiết bị và tài khoản dịch vụ có nguy cơ bị tin tặc lạm dụng cao hơn vì không có khả năng thay đổi mật khẩu.

## Chương 34    Quản lý Rủi ro

### Quản lý Rủi ro

Trong chương này, bạn sẽ:

- Khám phá những khái niệm về quản lý rủi ro,
- Kiểm tra những quy trình được sử dụng trong quản lý rủi ro.

Quản lý rủi ro là một chức năng nghiệp vụ cốt lõi của một doanh nghiệp bởi vì thông qua quy trình quản lý rủi ro, một doanh nghiệp có thể tối đa những khoản lợi nhuận trên khoản đầu tư của mình. Việc hiểu được tác động kinh doanh của những hoạt động tương ứng với doanh nghiệp là chìa khóa cho sự thành công trong kinh doanh. Điều này có thể được thực hiện bằng cách sử dụng một phân tích tác động kinh doanh. Sử dụng dữ liệu từ phân tích, kết hợp với một phân tích về các mối đe dọa và một quy trình đánh giá rủi ro, doanh nghiệp có thể hiểu được về nguồn gốc của các yếu tố rủi ro mà họ đang phải đối mặt và mức độ cường độ của chúng.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu chứng nhận 5.4 của kỳ thi CompTIA Security+: Tổng hợp những quy trình và khái niệm quản lý rủi ro.

## Các Kiểu Rủi ro

Rủi ro đến từ nhiều nguồn khác nhau. Một cách để tổ chức những rủi ro khác nhau là phân loại chúng thành một chuỗi các thể loại. CompTIA Security+ công nhận 6 *kiểu rủi ro* sau đây: bên ngoài, trong nội bộ, các hệ thống kế thừa, nhiều bên, trộm cắp tài sản sở hữu trí tuệ và tuân thủ/cấp phép phần mềm. Những kiểu rủi ro khác nhau này không phải là độc nhất và sẽ được thảo luận trong những phần tiếp theo.

### Bên ngoài

Những mối đe dọa *từ bên ngoài* đến từ bên ngoài tổ chức và, theo định nghĩa, bắt đầu mà không cần truy cập vào hệ thống. Quyền truy cập vào hệ thống được dành cho người dùng, người có nhu cầu nghiệp vụ để biết và có những tài khoản được cấp phép trên hệ thống. Những người bên ngoài trước tiên phải chiếm đoạt được một trong số những tài khoản này. Bước bổ sung này và sự phụ thuộc vào những kết nối bên ngoài thường khiến cho những kẻ tấn công dễ bị phát hiện hơn.

### Trong nội bộ

Những mối đe dọa *từ bên trong* bao gồm những nhân viên bất mãn và những nhân viên có thiện chí mắc lỗi hoặc gắp sự cố. Các mối đe dọa nội bộ có xu hướng gây ra thiệt hại nhiều hơn, vì thủ phạm đã thực sự được cấp một số hình thức truy cập. Rủi ro liên quan đến mức độ truy cập và giá trị của tài sản đang được tiếp cận. Ví dụ: nếu quản trị viên hệ thống làm việc trên domain controller vô tình xóa một giá trị quan trọng và làm hỏng hệ thống, thì việc này có thể tổn kém tương đương với việc một người bên ngoài trái phép thực hiện một cuộc tấn công DoS chống lại doanh nghiệp.

### Các Hệ thống Kế thừa

*Các hệ thống kế thừa* là những hệ thống cũ hơn đang tồn tại trước. Nhưng tuổi tác thực sự không phải là vấn đề - vấn đề thực sự đằng sau những

gì làm cho một hệ thống trở thành một hệ thống kế thừa là khái niệm nợ kỹ thuật. Nợ kỹ thuật là chi phí xảy ra qua thời gian do không bảo trì hệ thống một cách hoàn toàn. Việc cắt giảm chi phí có thể được hợp pháp hóa trong thời điểm hiện tại, nhưng theo thời gian, những khoản cắt giảm đó trở thành vấn đề. Hãy lấy việc sửa đổi hệ thống làm ví dụ. Nếu một hệ thống đã có những sửa đổi tùy chỉnh theo thời gian để thích ứng với quy trình nghiệp vụ của công ty thì những sửa đổi đó hoạt động như thế nào khi một phiên bản mới hơn ra mắt? Một nguyên nhân phổ biến cho việc không cập nhật hoặc nâng cấp hệ thống là nó sẽ làm hỏng thứ gì đó hoặc làm mất hiệu lực bảo hành hiện có. Theo thời gian, sự thiếu duy trì [trạng thái] hiện tại hoặc trôi khỏi trạng thái mong muốn này sẽ làm gia tăng thêm chi phí. Giống như tất cả các khoản nợ đều có lãi suất, khoản nợ kỹ thuật phát triển theo thời gian đến mức nó có thể trở thành vấn đề chính trong các dự án CNTT liên quan đến việc cập nhật các hệ thống cũ hơn. Trong một thế giới với các mối đe dọa và véc-tơ rủi ro không ngừng phát triển, bản thân việc không có khả năng ứng phó cũng chính là một rủi ro.

## Nhiều bên

Trong quản lý rủi ro truyền thống, yếu tố thúc đẩy đang được xem xét là rủi ro đối với doanh nghiệp của một ai đó. Trong một hệ thống hai-bên truyền thống (một kẻ tấn công chống lại một công ty), các phương trình rủi ro là tương đối dễ xác định và tối ưu. Tuy nhiên, khi một hệ thống có nhiều bên, mỗi bên đều có những cách xác định rủi ro của riêng mình, việc quản lý phương trình rủi ro tổng thể sẽ trở nên phức tạp. Nếu như một công ty đang đàm phán để thực hiện một thay đổi lớn trong hệ thống, và tất cả các bên liên quan đều trong phạm vi công ty thì đây vẫn được xem là một bên duy nhất, nhưng nếu nguồn tài chính cho dự án đến từ công ty khác, và các nhà thầu phụ có tham gia, những xác định mức rủi

ro có thể chấp nhận được của các bên khác sẽ nhanh chóng trở thành một vấn đề.

### **Đánh cắp IP (Tài sản Sở hữu Trí tuệ)**

Nếu bạn đặt ra câu hỏi cho một kỹ thuật viên CNTT về rủi ro an ninh mạng, bạn có thể nhận được một câu trả lời liên quan đến mất mát dữ liệu, ransomware, vi-rút, malware, hoặc lừa đảo. Đây hầu hết là những vấn đề về kỹ thuật, vì đây là thế giới mà hầu hết các chuyên gia an ninh mạng đang sống trong đó. Nhưng đặt ra câu hỏi tương tự cho CEO, và các đế mục kinh doanh chẳng hạn như hành vi trộm cắp tài sản trí tuệ sẽ xuất hiện ngay lập tức. Trộm cắp tài sản trí tuệ có thể gây tổn hại một cách nghiêm trọng đến sức khỏe tương lai của một công ty. Nếu một công ty tiêu tốn rất nhiều nguồn lực vào việc phát triển một sản phẩm hay một thị trường và sau đó bị cắt xén bởi các bên khác đã không phải tiêu tốn những nguồn lực đó, doanh số có thể biến mất và dòng doanh thu trong tương lai có thể bị cạn kiệt. Không giống như những tài sản vật chất, những tài sản kỹ thuật số có thể bị đánh cắp chỉ thông qua việc sao chép, và đây là con đường mà những kẻ tấn công sử dụng để tấn công dữ liệu tài sản trí tuệ. Kẻ tấn công sẽ cố gắng chiếm được quyền truy cập và sao chép dữ liệu, đồng thời cố gắng không để lại dấu vết, khiến cho hành vi trộm cắp không hoàn toàn rõ ràng cho đến khi một đối thủ cạnh tranh sử dụng thông tin và đưa ra một sản phẩm "bị đánh cắp" dưới dạng một bản sao.

Hành vi trộm cắp tài sản trí tuệ rất khó để xác định, và khi bản sao đã có mặt trên thị trường thì biện pháp duy nhất là các tòa án thông qua các hành động bảo vệ bí mật thương mại và bản quyền. Đây là một vấn đề cực kỳ quan trọng đối với các cuộc tấn công quốc tế được-nhà-nước-bảo-trợ vì những nguồn tài nguyên hợp pháp đang gặp phải thách thức trong việc sử dụng một cách có hiệu quả. Những cuộc điều tra và truy tố

hành vi trộm cắp tài sản trí tuệ là các đề mục chính được FPI theo đuổi như một phần của chiến lược an ninh mạng của mình.

### **Tuân thủ/Cấp phép Phần mềm**

Phần mềm có mặt ở khắp mọi nơi, nó hình thành nên trực xương sống chức năng của các hệ thống của chúng ta. Nguồn cung của phần mềm này là thông qua việc cấp phép và trong nhiều rất nhiều trường hợp là sự tin tưởng. Các bản sao của rất nhiều sản phẩm phần mềm có thể được tạo ra và được sử dụng mà không có giấy phép, và điều này gây ra những rủi ro trong *tuân thủ/cấp phép phần mềm*. Hình thức rủi ro này được đối phó tốt nhất bằng cách sử dụng các chính sách và thủ tục để ngăn chặn hành động này, tiếp theo đó là kiểm toán nội bộ để xác thực tính tuân thủ với các chính sách.



**MÁCH NƯỚC CHO KỲ THI** Hãy có khả năng xác định các loại rủi ro khác nhau — bên ngoài, bên trong, các hệ thống kế thừa, nhiều bên, trộm cắp IP và tuân thủ/cấp phép phần mềm. Hãy tìm hiểu những chiến lược và quy trình quản lý rủi ro nào trong các phần tiếp theo nên được áp dụng cho từng loại rủi ro nhất định đã được thảo luận.

### **Các Chiến lược Quản lý Rủi ro**

Quản lý rủi ro có thể được mô tả tốt nhất như là một quy trình đưa-ra-quyết-định. *Các chiến lược quản lý rủi ro* bao gồm các yếu tố về đánh giá mối đe dọa, đánh giá rủi ro, và các khái niệm triển khai bảo mật, tất cả đều được định vị trong nhận thức về quản lý doanh nghiệp. Theo những thuật ngữ đơn giản nhất, khi bạn quản lý rủi ro, bạn xác định những gì có thể xảy ra đối với doanh nghiệp của bạn, bạn đánh giá tác động nếu như điều đó xảy ra, và bạn quyết định những gì bạn có thể thực hiện để kiểm soát tác động đó nhiều nhất có thể nếu bạn hoặc nhóm quản lý của

bạn cho rằng đó là điều cần thiết. Sau đó, bạn quyết định hành động hoặc không, và, cuối cùng, bạn đánh giá kết quả của quyết định của bạn. Quy trình có thể lặp lại, vì thực tiễn tốt nhất trong ngành chỉ ra một cách rõ ràng rằng một khía cạnh quan trọng của việc quản lý rủi ro một cách hiệu quả là coi nó như một quy trình liên tục tiếp diễn.

Những rủi ro là điều tuyệt đối – chúng không thể được loại bỏ hoặc loại trừ. Bạn có thể thực hiện những hành động để thay đổi những ảnh hưởng mà một rủi ro gây ra cho một hệ thống, nhưng bản thân rủi ro vẫn không thực sự thay đổi, bất kể hành động mà bạn thực hiện để giảm nhẹ rủi ro. Một rủi ro lớn sẽ luôn là một rủi ro lớn. Tuy nhiên, bạn có thể thực hiện những hành động để giảm thiểu tác động của những rủi ro đó nếu như nó xảy ra. Một số ít các chiến lược có thể được sử dụng để quản lý rủi ro. Rủi ro có thể được tránh, chuyển, giảm nhẹ hoặc chấp thuận.

Hãy hiểu rằng rủi ro không thể được loại bỏ một cách hoàn toàn. Một rủi ro có thể vẫn còn tồn tại sau khi triển khai các biện pháp kiểm soát được gọi là một *rủi ro tồn dư*. Bạn phải đánh giá thêm những rủi ro tồn dư để xác định nơi các biện pháp kiểm soát bổ sung là cần thiết để giảm thiểu rủi ro thêm nữa. Điều này cũng cống cỗ thêm tuyên bố trước đó trong chương này rằng quy trình quản lý rủi ro là quy trình lặp lại.



**MÁCH NƯỚC CHO KỲ THI** Bạn có thể thực hiện 4 điều để ứng phó với rủi ro: chấp thuận nó, chuyển nó đi, tránh nó, và giảm nhẹ nó. Hãy tìm hiểu về những khác biệt, vì tất cả những khác biệt này sẽ được trình bày dưới dạng các lựa chọn đáp án khả dĩ cho một câu hỏi, và kịch bản chi tiết sẽ áp dụng cho một đáp án tốt hơn những đáp án khác.

## **Chấp thuận**

Khi bạn đang phân tích một rủi ro cụ thể, sau khi xem xét cẩn thận về chi phí để tránh, chuyển giao hoặc giảm thiểu rủi ro so với xác suất xảy ra và tác động tiềm ẩn của nó, phản ứng tốt nhất là *chấp thuận rủi ro* [*điều này chưa chắc đã là hợp lý – người dịch*. *Chấp thuận rủi ro chỉ hợp lý khi không thể thay đổi xác suất xảy ra, hoặc chi phí giảm nhẹ tác động là không thể chấp nhận được đối với doanh nghiệp*]. Ví dụ, một nhà quản lý có thể chọn để cho phép một lập trình viên đưa ra những thay đổi “khẩn cấp” đối với hệ thống sản xuất (vi phạm phân tách nhiệm vụ rõ ràng) do hệ thống không thể ngừng hoạt động trong một khoảng thời gian nhất định. Nhà quản lý chấp nhận rằng rủi ro mà lập trình viên có thể thực hiện những thay đổi trái phép là lớn hơn so với yêu cầu về tính-sẵn-sàng-cao của hệ thống đó. Tuy nhiên, luôn phải có một số các biện pháp kiểm soát bổ sung, chẳng hạn như đánh giá của cấp quản lý hoặc quy trình phê duyệt đã được tiêu chuẩn hóa, để đảm bảo rủi ro giả định đã được quản lý một cách thích hợp.

## **Tránh**

*Tránh* rủi ro có thể được thực hiện theo rất nhiều cách. Mặc dù bạn không thể loại bỏ những mối đe dọa khỏi môi trường nhưng bạn có thể điều chỉnh mức độ tiếp xúc của hệ thống với những mối đe dọa. Việc không triển khai một mô-đun làm gia tăng rủi ro là một cách tránh rủi ro.

## **Chuyển**

*Chuyển* rủi ro là khi rủi ro trong một tình huống được kiểm soát bởi một thực thể khác. Như đã được đề cập trước đây trong ấn phẩm này xoay quanh những vấn đề chẳng hạn như điện toán đám mây, các hợp đồng và thỏa thuận pháp lý sẽ chỉ rõ những bên nào đang gánh chịu những rủi ro nào. Việc này sẽ xác định ai chịu những trách nhiệm và ai nắm giữ những rủi ro – xác định trước việc chuyển [rủi ro] cụ thể. Những sai lầm mà nhiều người mắc phải là giả định về chuyển giao rủi ro. Việc chuyển rủi

ro chỉ xảy ra theo các thỏa thuận pháp lý này được xác định trong hợp đồng.

Một ví dụ phổ biến khác về chuyển giao rủi ro là sự bảo vệ chống lại hành vi gian lận mà người tiêu dùng gặp phải với thẻ tín dụng của họ. Rủi ro được chuyển cho một bên khác, từ đó, mọi người có thể sử dụng thẻ tín dụng của mình một cách tự tin. Như đã được thảo luận trước đây, việc chuyển giao này nằm trong bản in ấn chi tiết của thỏa thuận hợp đồng thẻ tín dụng.

### **Bảo hiểm An ninh mạng**

Một phương pháp phổ biến về việc chuyển giao rủi ro là mua *bảo hiểm an ninh mạng*. Bảo hiểm cho phép rủi ro được chuyển cho một bên-thứ-ba để quản lý những loại rủi ro cụ thể đối với rất nhiều bên, từ đó, giảm thiểu được chi phí riêng lẻ.

### **Giảm nhẹ**

Rủi ro cũng có thể được *giảm nhẹ* thông qua việc áp dụng các biện pháp kiểm soát để giảm thiểu tác động của một cuộc tấn công. Các biện pháp kiểm soát có thể cảnh báo những nhân viên vận hành để từ đó mức độ tiếp xúc [với rủi ro] được giảm thiểu thông qua sự can thiệp vào quy trình. Khi một hành động xảy ra nằm ngoài phạm vi hồ sơ rủi ro đã được chấp thuận, một bộ các quy tắc thứ hai có thể được áp dụng, chẳng hạn như gọi điện cho khách hàng để xác minh trước khi hoàn tất một giao dịch. Các biện pháp kiểm soát như vậy có thể hoạt động để giảm thiểu rủi ro tương ứng với những hoạt động tiềm ẩn những rủi-ro-cao.

### **Phân tích Rủi ro**

Để quản lý một cách hiệu quả bất kỳ điều gì, điều cần thiết là phải có những thước đo thích hợp để định hướng cho chuỗi hành động. Trong trường hợp với rủi ro, điều này cũng luôn đúng. Để quản lý rủi ro, cần phải đo lường được tổn thất và tổn thất tiềm năng, và phần lớn những

thông tin này đến từ cách thức *phân tích rủi ro*. Phân tích rủi ro được thực hiện thông qua một loạt những bài tập cụ thể để khám phá ra sự tồn tại và mức độ của rủi ro trong toàn bộ doanh nghiệp. Sau đó, thông qua những phân tích sâu thêm, thông tin có thể được tinh chỉnh thành một kế hoạch khả thi để quản lý rủi ro đến một mức độ có thể chấp nhận được.

### [Sổ] Đăng ký Rủi ro

Một *đăng ký rủi ro* là một danh sách các rủi ro tương ứng với một hệ thống. Nó cũng có thể chứa những thông tin bổ sung tương ứng với các thành phần của rủi ro, chẳng hạn như các thể loại để nhóm các rủi ro tương tự nhau, xác suất xảy ra, tác động đến tổ chức, các yếu tố giảm nhẹ, và những dữ liệu khác. Không có bất kỳ một hình thức được tiêu chuẩn hóa nào [*hàm ý rằng đăng ký rủi ro sẽ tùy thuộc vào bối cảnh và tình huống của tổ chức*]. Học viện Quản lý Dự án (PMI) có một định dạng và những nguồn khác sẽ có các định dạng khác. Tài liệu tham chiếu *ISO Guide 73:2009 Quản lý Rủi ro – Từ vựng định nghĩa một đăng ký rủi ro* là một “bản ghi chứa thông tin về những rủi ro đã được xác định”.

### Ma trận Rủi ro / Bản đồ Nhiệt

Một *ma trận rủi ro* hoặc *bản đồ nhiệt* được sử dụng để hiển thị một cách trực quan về những kết quả của một phân tích rủi ro định tính. Phương pháp này cho phép kinh nghiệm và phán đoán của chuyên gia để đảm nhiệm một vai trò nổi bật trong quá trình đánh giá rủi ro và dễ dàng hơn so với việc cố gắng xác định một cách chính xác một con số cho từng thành phần của rủi ro. Để đánh giá rủi ro một cách định tính, trước tiên bạn cần xác định khả năng xảy ra của một mối đe dọa và những hậu quả nếu nó [mối đe dọa] xảy ra. Sau đó, bạn định giá trị của từng mối đe dọa và nhân chúng lại với nhau để có được giá trị của rủi ro. Với một ma trận rủi ro/bản đồ nhiệt 5 x 5, như được minh họa trong Hình 34-1, chỉ đơn

giản là bạn sử dụng giá trị 1 đến 5 cho từng trục, và việc này tạo ra kết quả là rủi ro có giá trị từ 1 đến 25. Những giá trị này sau đó có thể được phân loại là không đáng kể, trung bình, lớn, hoặc nghiêm trọng.

Likelihood	Almost Certain (5)	Moderate 5	Major 10	Major 15	Critical 20	Critical 25
	Likely (4)	Minor 4	Moderate 8	Major 12	Major 16	Critical 20
	Possible (3)	Minor 3	Moderate 6	Moderate 9	Major 12	Major 15
	Unlikely (2)	Minor 2	Minor 4	Moderate 6	Moderate 8	Major 10
	Rare (1)	Minor 1	Minor 2	Minor 3	Minor 4	Moderate 5
Consequence						

**Hình 34-1** Ma trận rủi ro/bản đồ nhiệt

### **Đánh giá Biện pháp kiểm soát Rủi ro**

Một *đánh giá biện pháp kiểm soát rủi ro* là một công vụ được sử dụng bởi Cơ quan Quản lý Ngành Tài chính (Finalcial Industry Regulatory Authority – FINRA) để đánh giá một loạt các rủi ro tương ứng với các tổ chức thành viên của họ. Những câu hỏi được đặt ra về một loạt các chủ đề, bao gồm cả an ninh mạng. Những đáp án cho các câu hỏi này vẽ ra một bức tranh tương đối chi tiết về những rủi ro tiềm ẩn mà một công ty đã tiếp xúc, dựa trên các chính sách và thực tiễn của họ.

### **Tự-Đánh-giá Biện pháp kiểm soát Rủi ro**

*Tự-đánh-giá biện pháp kiểm soát rủi ro* là một kỹ thuật sử dụng đội ngũ quản lý và nhân viên ở mọi cấp độ để xác định và đánh giá rủi ro và các biện pháp kiểm soát tương ứng. Những thông tin này được thu thập và phân tích để tạo ra một bản đồ rủi ro toàn diện hơn và các biện pháp kiểm soát đang sử dụng để giải quyết rủi ro. Việc thu hút nhiều quan

điểm trong quá trình thu thập thông tin, xác định những mức độ tiếp xúc với rủi ro và xác định những hành động khắc phục cung cấp những quan điểm khác nhau và khám phá ra những lỗ hổng đã bị bỏ qua.

### **Nâng cao nhận thức Rủi ro**

*Nhận thức về rủi ro* là những kiến thức về rủi ro và những hậu quả. Nhận thức về rủi ro là điều thiết yếu đối với một loạt nhân sự, với những nội dung được điều chỉnh theo sự đóng góp của họ cho doanh nghiệp. Đối với một số nhân viên, việc hiểu được rủi ro và biện pháp bảo vệ chống lại những kỹ thuật xã hội là điều quan trọng. Với những người khác, chẳng hạn như những người thiết kế hệ thống, hiểu biết chi tiết hơn về rủi ro và những lỗ hổng gây nên rủi ro là điều cần thiết. Đối với cấp quản lý và điều hành, một hiểu biết về toàn thể hệ sinh thái rủi ro là cần thiết bởi vì họ phải cân bằng được những rủi ro và phần thưởng thông qua các sáng kiến hệ thống chính. Cũng giống như phần mở đầu của chương trình 12-bước nổi tiếng là việc công nhận vấn đề và nhận thức được rủi ro là điều quan trọng nếu muốn quản lý nó.

### **Rủi ro Cố hữu**

*Rủi ro cố hữu* được xác định bằng tổng lượng rủi ro tồn tại trong trường hợp thiếu đi những biện pháp kiểm soát. Điều này có thể gây ra nhầm lẫn, như định nghĩa về "không có biện pháp kiểm soát" có thể bao gồm không có biện pháp kiểm soát truy cập, không khóa cửa, không kiểm tra lý lịch nhân sự - về bản chất, là một môi trường tương đương với việc mọi thứ đều gặp phải những rủi ro cao. Một diễn giải tốt hơn sẽ là rằng rủi ro cố hữu là mức rủi ro hiện tại với tập hợp các biện pháp kiểm soát hiện tại thay vì khái niệm giả định về việc thiếu bất kỳ biện pháp kiểm soát nào. Một ví dụ có lẽ sẽ giúp hiểu rõ hơn điều này. Chiếc xe ô-tô của bạn có rất nhiều nút điều khiển để hỗ trợ cho việc tự-lái, nhưng nó vẫn có những rủi ro liên quan. Đây chính là rủi ro cố hữu, nó tương ứng với

sự vận hành của hệ thống trong phạm vi một môi trường. Và khi môi trường thay đổi, rủi ro cỗ hũu cũng có thay đổi – những gì đã từng được coi là an toàn về tốc độ và môi trường sẽ khác nhau giữa một ngày nắng không có xe cộ qua lại, buổi tối đông xe cộ và trời mưa to, và ban đêm với lưu lượng phương tiện giao thông ở mức trung bình. Mỗi tình huống này đều có những rủi ro cỗ hũu khác nhau và có thể cần các biện pháp kiểm soát cụ thể để giảm rủi ro xuống mức có thể chấp nhận được.

### Rủi ro Tồn dư

Sự hiện diện của những rủi ro trong một hệ thống là điều tuyệt đối – chúng không thể được loại bỏ hoặc loại trừ hoàn toàn. Như đã được đề cập trước đây trong chương này, 4 hành động có thể được thực hiện để ứng phó với rủi ro: chấp nhận, chuyển, tránh và giảm nhẹ. Bất kể rủi ro nào đã không được chuyển, giảm nhẹ, hoặc tránh đều được gọi là *rủi ro tồn dư*, và, theo định nghĩa, sẽ được chấp thuận. Bạn không thể loại bỏ rủi ro tồn dư, nhưng bạn có thể quản lý rủi ro để định hướng rủi ro tồn dư đến mức có thể chấp nhận được.

### Rủi ro Kiểm soát

*Rủi ro kiểm soát* là một thuật ngữ được sử dụng để chỉ định rõ rủi ro tương ứng với khả năng xảy ra những sai sót nghiêm trọng trong các báo cáo tài chính của một công ty. Rủi ro này có thể được biểu thị bằng một số cách: hoặc không có một bộ các biện pháp kiểm soát nội bộ thích hợp để giảm thiểu một rủi ro cụ thể hoặc bộ các biện pháp kiểm soát nội bộ hiện đang sử dụng bị lỗi. Các hệ thống nghiệp vụ dựa trên các hệ thống CNTT có một rủi ro cỗ hũu tương ứng với những rủi ro an ninh mạng. Điều khiển cho các rủi ro này trở thành những rủi ro kiểm soát chính là khi chúng tác động đến chức năng nghiệp vụ theo một cách dẫn đến các sai sót hoặc lỗi về mặt tài chính. Trong trường hợp tổ chức không có đủ các biện pháp kiểm soát nội bộ đang được sử dụng để ngăn chặn và phát

hiện các lỗi hoặc hành vi gian lận thì tổ chức đã gấp một văn đề về rủi ro kiểm soát, trái ngược với rủi ro cỗ hũu.



**MÁCH NƯỚC CHO KỲ THI** Rủi ro cỗ hũu là tổng rủi ro đang hiện diện khi thiếu đi các biện pháp kiểm soát. Rủi ro tồn dư là tổng rủi ro còn lại sau khi các biện pháp kiểm soát đã được tính đến. Rủi ro kiểm soát là rủi ro có ảnh hưởng cụ thể đến báo cáo tài chính.

### **Khẩu vị Rủi ro**

Những công ty khác nhau trong những lĩnh vực và môi trường kinh doanh khác nhau có những mức độ tiếp xúc rủi ro khác nhau, do đó chúng cũng có những khả năng chịu đựng (dung sai) rủi ro khác nhau. *Khẩu vị rủi ro* là thuật ngữ được sử dụng để mô tả khả năng chịu đựng rủi ro của một công ty. Thậm chí, ngay cả trong phạm vi một lĩnh vực, với những công ty có cùng quy mô, đang hoạt động trong những khu vực gần như tương tự nhau, cũng vẫn sẽ có thể có những khác biệt trong mức độ rủi ro mà mỗi công ty cảm thấy thoải mái để chấp nhận. Khẩu vị rủi ro này liên quan đến các yếu tố kinh doanh khác chăng hạn như phần thưởng và tổn thất. Cấu trúc điều hành của mỗi công ty cần phải xác định được khẩu vị rủi ro thích hợp cho công ty đó, và điều đó trở thành giới hạn trên của mức rủi ro có thể chấp nhận được trong hoạt động của công ty.

### **Các Quy định Ánh hưởng đến Hoàn cảnh Rủi ro**

Các quy định có thể có một tác động đáng kể đến mức độ tiếp xúc với rủi ro. Đôi khi, tác động này là một hành động trực tiếp của một quy định, chăng hạn như các công ty tài chính bị các cơ quan quản lý bắt buộc phải có các mức độ mã hóa nhất định để bảo vệ những loại quy trình nhất định. Các trường hợp khác thì ít trực tiếp hơn, vì việc giám sát cụ thể là cần thiết để báo cáo, và các công ty thay đổi những hoạt động để tránh

việc phải báo cáo. Phạm vi của các quy định rất rộng, nhưng một số quy định phổ biến liên quan đến an ninh mạng bao gồm Sarbanes-Oxley, các quy định tài chính khác nhau về bảo vệ dữ liệu và Tiêu chuẩn Bảo mật Dữ liệu Ngành Thẻ Thanh toán (Payment Card Industry Data Security Standard – PCI-DSS) đối với dữ liệu thẻ tín dụng.

Các quy định định hướng cho những phản ứng của công ty bởi vì việc không tuân theo các quy định có thể dẫn đến các khoản phạt, vốn thể hiện sự tổn thất. Do đó, các quy định có thể được coi là rủi ro với khả năng hầu như chắc chắn sẽ phải gánh chịu tổn thất.



## MÁCH NƯỚC CHO KỲ THI

Điều quan trọng là hãy nhớ rằng các quy định được áp dụng cho rất nhiều lĩnh vực an ninh mạng. Hãy biết rằng Đạo luật Sarbanes-Oxley 2002 bảo vệ các nhà đầu tư khỏi các hành vi gian lận của các tập đoàn và các báo cáo tài chính xấu, và Tiêu chuẩn Bảo mật Dữ liệu Ngành Thẻ Thanh toán (PCI-DSS) là một tập hợp các tiêu chuẩn và chính sách bảo mật để các công ty tuân theo nhằm tối ưu hóa sự bảo mật cho thẻ thanh toán của người tiêu dùng và tương

## Các Kiểu Đánh giá Rủi ro

*Đánh giá rủi ro* là một phương pháp để phân tích những rủi ro tiềm ẩn dựa trên các mô hình thống kê và toán học. Bạn có thể sử dụng bất kỳ một mô hình nào trong số rất nhiều mô hình khác nhau để tính toán những giá trị đánh giá rủi ro tiềm ẩn. Một phương pháp phổ biến là việc tính toán giá trị tổn thất hàng năm dự kiến (annual loss expectancy – ALE). Việc tính toán ALE tạo ra một giá trị bằng tiền của sự tác động. Phép tính này bắt đầu bằng việc tính toán một giá-trị-tổn-thất-đơn-lẻ dự kiến (single-loss expectancy – SLE), sẽ được trình bày chi tiết ở phần sau của chương này.

## Định tính

Đánh giá rủi ro *định tính* là quá trình xác định một cách chủ quan về tác động của một sự kiện có ảnh hưởng đến một dự án, chương trình hoặc lĩnh vực kinh doanh. Đánh giá rủi ro định tính thường liên quan đến việc sử dụng những ý kiến đánh giá của chuyên gia và các mô hình để hoàn thành việc đánh giá. Kiểu đánh giá rủi ro này phụ thuộc rất nhiều vào những ý kiến đánh giá và kinh nghiệm của các chuyên gia và cũng có thể mắc phải những định kiến. Ma trận rủi ro/bản đồ nhiệt đã được trình bày trước đó là một ví dụ về mô hình rủi ro định tính.

## Định lượng

Đánh giá rủi ro *định lượng* là quá trình xác định một cách khách quan về những tác động của một sự kiện có ảnh hưởng đến một dự án, chương trình hoặc lĩnh vực kinh doanh. Đánh giá rủi ro định lượng thường liên quan đến việc sử dụng các tham số và các mô hình để hoàn thành việc đánh giá. Đánh giá rủi ro định lượng áp dụng những thông tin lịch sử và những xu hướng để cỗ gắng dự đoán hiệu suất trong tương lai. Kiểu đánh giá rủi ro này phụ thuộc rất nhiều vào dữ liệu lịch sử và việc thu thập những dữ liệu này thường khá khó khăn. Đánh giá rủi ro định lượng cũng có thể phụ thuộc nhiều vào các mô hình để cung cấp những thông tin ra-quyết-định dưới hình thức các tham số định lượng, vốn cỗ gắng đo lường các mức độ rủi ro trên một thang đo phổ biến. Những mô hình về giá-trị-tổn-thất-đơn-lẻ dự kiến, giá trị tổn thất hàng năm dự kiến, và tỷ lệ xảy ra hàng năm (annualized rate of occurrence) – sẽ được thảo luận sau trong chương này – là những ví dụ về phân tích rủi ro định lượng.



## MÁCH NƯỚC CHO KỲ THI

Hãy tìm hiểu về sự khác biệt giữa đánh giá rủi ro định tính và định lượng. Định lượng có nghĩa là bạn có thể tính

toán thực tế một điều gì đó, trong khi định tính có tính chủ quan hơn, với những giá trị như cao, trung bình và thấp.

### **Khả năng Xảy ra**

*Khả năng xảy ra* là cơ hội mà một rủi ro cụ thể sẽ xảy ra. Thước đo này có thể là định tính hoặc định lượng, như vừa được thảo luận. Đối với các thước đo định tính, khả năng xảy ra thường được xác định trên cơ sở hàng năm để từ đó nó có thể được so sánh với các thước đo hàng năm khác. Nếu được xác định một cách định lượng, nó được sử dụng để tạo ra một kết quả tác động theo thứ-tự-xếp-hạng.

### **Tác động**

*Tác động* của một sự kiện là một thước đo tổn thất thực tế khi một mối đe dọa khai thác được một lỗ hổng. Tiêu chuẩn Xử lý Thông tin Liên bang (Federal Information Processing Standard – FIPS) 199 định nghĩa 3 cấp độ tác động bằng cách sử dụng những thuật ngữ cao, trung bình và thấp. Tác động cần phải được xác định theo bối cảnh của từng tổ chức, khi những gì là cao đối với một số công ty có thể là thấp đối với những công ty lớn hơn nhiều. Phương pháp phổ biến là xác định các mức tác động theo tầm quan trọng của việc kinh doanh. Tác động có thể là về chi phí (đô-la), hiệu suất (thỏa thuận mức dịch vụ [SLA] hoặc các yêu cầu khác), lịch trình (các sản phẩm có thể chuyển giao) hoặc bất kỳ hạng mục quan trọng nào khác. Tác động cũng có thể được phân loại theo thuộc tính bảo mật thông tin liên quan đến vấn đề: tính bảo mật, tính toàn vẹn và tính sẵn sàng.

Rủi ro là khả năng xảy ra việc một điều gì đó không hoạt động như đã được lập kế hoạch và gây ra tác động bất lợi. Tác động là chi phí liên quan đến rủi ro đã hiện thực hóa. Tác động có thể có nhiều hình thức — từ tính mạng con người, như thương tật hoặc tử vong, đến mất mát tài sản, mất an toàn, tổn thất tài chính, hoặc mất danh tiếng. Tổn thất hiếm

khi là tuyệt đối và có thể xảy ra ở mọi quy mô và sự kết hợp khác nhau. Các mức độ rủi ro khác nhau có thể dẫn đến những mức độ tác động khác nhau. Đôi khi các sự kiện bên ngoài có thể gây ảnh hưởng đến tác động. Nếu những người khác trong cùng ngành đã từng trải qua một loại tổn thất cụ thể, và công ty của bạn có được thời gian và cảnh báo để giảm thiểu nó, nhưng không phải thế, môi trường được xác định bởi các yếu tố bên ngoài này thực sự có thể làm gia tăng tác động đối với công ty của bạn từ loại sự kiện này. Ví dụ, việc thất bại trong việc vá lỗ hệ thống có thể gây ra những tác động nghiêm trọng đến một tổ chức, như các vụ vi phạm dữ liệu gần đây đã cho thấy. Tuy nhiên việc không vá lỗ một hệ thống khi bạn đã biết nó sẽ được sử dụng để chống lại bạn, thậm chí còn tồi tệ hơn, vì nó gần như sẽ dẫn đến các cuộc tấn công tiếp theo.

## Sinh mạng

Rất nhiều hệ thống CNTT liên quan đến sức khỏe, và sự thất bại của một vài trong số những hệ thống này có thể dẫn đến thương tật và tử vong cho các bệnh nhân. Những hệ thống CNTT cũng thường là thành phần không thể thiếu trong việc vận hành máy móc trong các cơ sở công nghiệp, và những lỗ của chúng có thể có những tác động tương tự. Thương tật và tổn thất về *sinh mạng* là những kết quả tác động mà các bản sao lưu không thể giải quyết và có thể dẫn đến những hậu quả vượt trên những điều khác. Là một phần của phân tích tác động kinh doanh (BIA), bạn sẽ cần phải xác định những hệ thống này và đảm bảo rằng chúng được dự phòng đầy đủ, để tránh những tác động đến sinh mạng con người.

## Tài sản

Thiệt hại về *tài sản* có thể dẫn đến những rủi ro không thể giảm nhẹ được. Thiệt hại về tài sản đối với những tài sản thuộc-sở-hữu-công-ty, thiệt hại đối với tài sản của những người khác, và thậm chí những tổn

hại đối với môi trường do rò rỉ chất độc trong các ngành công nghiệp là những ví dụ về thiệt hại có thể bị gây ra bởi lỗi bảo mật CNTT. Điều này có thể đặc biệt đúng trong những công ty có các nhà máy sản xuất và các quy trình vật lý hệ thống thông tin và máy tính khác. Nếu bạn cho rằng thiệt hại về tài sản không thể xảy ra đối với tổ chức của bạn chỉ vì nó chỉ có những máy tính văn phòng, hãy xem xét cách mà phần mềm độc hại Shamoon đã phá hủy tài nguyên máy tính của Saudi Aramco đến mức công ty phải mua thiết bị thay thế, vì việc đưa các máy tính trở lại trạng thái sạch sẽ, không phải là một giải pháp được đảm bảo hoặc kịp thời.

## An toàn

*An toàn* là điều kiện được bảo vệ khỏi, hoặc không có khả năng gây ra, nguy hiểm, rủi ro hoặc thương tích. An toàn có ý nghĩa từ cả quan điểm rủi ro kinh doanh và khi bạn xem xét mức độ quan tâm của một ai đó đối với hạnh phúc của con người. Trong môi trường sản xuất, với các thiết bị và máy móc di chuyển có thể gây ra nguy hiểm cho người lao động, các quy định của chính phủ đặt ra những hành động cụ thể để giảm thiểu rủi ro và khiến cho nơi làm việc trở nên an toàn nhất có thể. Ngày nay, máy tính càng tham gia nhiều hơn vào tất cả những khía cạnh của doanh nghiệp, và chúng có thể gây tác động đến sự an toàn. Những thất bại dẫn đến các vấn đề an toàn sẽ gây ra sự đình trệ công việc và làm gia tăng thất mà lẽ ra đã có thể tránh được. Các điều kiện không an toàn là kết quả của các vấn đề về máy tính sẽ phải đổi mới với sự phản nổ về quy định giống như các nhà máy không an toàn đã gây ra trong quá trình sản xuất — tiền phạt và các khiếu nại hình sự.

## Tài chính

Theo nhiều cách thức, *tài chính* là trọng tài cuối cùng của mọi hoạt động bởi vì nó là cách chúng ta giữ được thành quả. Chúng ta có thể đo lường lợi nhuận thông qua doanh số bán hàng và lợi nhuận, và chúng ta có thể

đo lường tổn thất thông qua các rủi ro không thể được giảm nhẹ. Chúng ta có thể nắm bắt hầu hết các sự kiện, đặt ra giá trị đô-la (giá trị bằng tiền) cho chúng, và kết toán sổ sách. Điều này trở thành một vấn đề là khi các tác động vượt quá chi phí dự kiến liên quan đến rủi ro tồn dư đã được lập kế hoạch vì khi đó chi phí sẽ có tác động trực tiếp đến lợi nhuận. Những tác động đến việc kinh doanh cuối cùng trở thành tác động tài chính. Bắt đầu có thể là một bản vá lỗi bị bỏ sót cho phép ransomware xâm nhập vào hệ thống. Điều này dẫn đến tác động kinh doanh cuối cùng làm gia tăng thêm chi phí, vốn là điều đáng lẽ nên tránh.

## Danh tiếng

*Danh tiếng* của công ty là điều rất quan trọng trong thị trường. Bạn sẽ giao dịch với một ngân hàng có hồ sơ kế toán kém chất lượng hoặc làm mất thông tin cá nhân [của khách hàng]? Bán lẻ trực tuyến thì thế nào? Liệu cơ sở khách hàng có suy nghĩ kỹ càng trước khi nhập thông tin thẻ tín dụng của họ sau khi bị vi phạm dữ liệu không? Đây không phải là những câu hỏi hoàn toàn mang tính giả thuyết, những sự kiện này thực sự đã xảy ra và kết quả là danh tiếng của công ty đã bị tổn hại, do đó, gây ra thiệt hại cho các công ty trong cơ sở khách hàng và doanh thu.



## MÁCH NƯỚC CHO KỲ THI

Rủi ro được thuyết minh bằng tác động. Các tác động có thể có những ảnh hưởng đến sinh mạng, tài sản, an toàn, danh tiếng, và tài chính. Thông thường, rất nhiều tác động diễn ra từ một sự cố, và tài chính luôn luôn phải chi trả cho tất cả. Hãy chuẩn bị để phân tích cú pháp của câu hỏi để xác định xem liệu trọng tâm của nó là rủi ro, tác động hay một hậu quả cụ thể.

## Giá trị Tài sản

*Giá trị tài sản (AV)* là tổng số tiền cần phải có để thay thế một tài sản. Thuật ngữ này được sử dụng cùng với hệ số tiếp xúc rủi ro (EF), một thước đo về mức độ rủi ro của một tài sản, để xác định giá-trị-tổn-thất-đơn-lẻ dự kiến (SLE).



**MÁCH NƯỚC CHO KỲ THI** Hãy tìm hiểu những thuật ngữ SLE, ALE, và ARO và cách thức mà chúng được sử dụng để tính toán tổn thất tiềm năng. Bạn có thể được cung cấp một kịch bản, được yêu cầu tính toán SLE, ALE và ARO, và được trình bày các lựa chọn trả lời bao gồm những giá trị có thể là kết quả của các phép tính sai.

### Giá-trị-tổn-thất-đơn-lẻ dự kiến (Single-Loss Expectancy - SLE)

*Giá-trị-tổn-thất-đơn-lẻ dự kiến (SLE)* là giá trị của một tổn thất đã được dự kiến từ một sự kiện đơn lẻ. Nó được tính bằng cách sử dụng công thức dưới đây:

$$\text{SLE} = \text{giá trị tài sản (AV)} \times \text{hệ số tiếp xúc rủi ro (EF)}$$

Hệ số tiếp xúc rủi ro (EF) là một thước đo cường độ tổn thất của một tài sản.

Ví dụ, để tính toán hệ số tiếp xúc rủi ro, hãy giả định giá trị tài sản của một tòa nhà văn phòng nhỏ và những gì bên trong của nó là 2 triệu đô-la Mỹ. Đồng thời, giả định rằng tòa nhà này đang chứa trung tâm cuộc gọi của một doanh nghiệp, và tổn hại hoàn toàn của trung tâm sẽ làm mất đi một nửa năng lực của công ty.

Do đó, hệ số tiếp xúc rủi ro là 50%, và SLE được tính như sau:

$$(\text{SLE}) 2 \text{ triệu đô-la Mỹ} \times 0.5 = 1 \text{ triệu đô-la Mỹ}$$

## Tổn thất Hàng năm Dự kiến (Annualized Loss Expectancy - ALE)

Sau khi SLE đã được tính toán, sau đó *tổn thất hàng năm dự kiến (ALE)* được tính toán chỉ đơn giản bằng cách nhân SLE với khả năng xảy ra hoặc tổng số lần mà sự kiện được dự kiến xảy ra trong 1 năm, vốn còn được gọi là *tỷ lệ xảy ra hàng năm (annualized rate of occurrence – ARO)*:

$$\text{ALE} = \text{SLE} \times \text{ARO}$$

Điều này thể hiện những tổn thất được dự kiến trong suốt 1 năm căn cứ vào ALE. Nếu nhiều sự kiện được xem xét, tổng số học của tất cả các SLE và ARO có thể được tính toán để cung cấp một con số tổng thể.

## Tỷ lệ Xảy ra Hàng năm (Annualized Rate of Occurrence - ARO)

*Tỷ lệ xảy ra hàng năm (ARO)* là đại diện cho tần suất của sự kiện, được đo trong một năm tiêu chuẩn. Nếu như sự kiện được dự kiến là sẽ xảy ra 1 lần trong 20 năm thì ARO là 1/20. Thông thường, ARO được xác định bằng dữ liệu lịch sử, kể cả từ những trải nghiệm của chính công ty hoặc từ những khảo sát trong ngành. Tiếp tục với ví dụ của chúng ta, giả định là một sự kiện hỏa hoạn tại địa điểm của doanh nghiệp này được dự kiến xảy ra khoảng 1 lần trong 20 năm. Với thông tin này, ALE là:

$$1 \text{ triệu đô-la Mỹ} \times 1/20 = 50,000 \text{ đô-la Mỹ}$$

ALE xác định một ngưỡng để đánh giá tỷ lệ chi phí/lợi ích của một biện pháp ứng phó nhất định. Do đó, một biện pháp ứng phó để bảo vệ doanh nghiệp này một cách thỏa đáng nên tiêu tốn không nhiều hơn ALE đã được tính toàn là 50,000 đô-la Mỹ mỗi năm.



### LƯU Ý

Có rất nhiều tài nguyên sẵn có để giúp tính toán ALE. Có những cơ sở dữ liệu chứa những thông tin để giúp các doanh nghiệp (các

tổ chức thành viên) quản lý hệ số tổn thất từ những thảm họa thiên nhiên như các cơn bão, động đất, v.v... Những cơ sở dữ liệu này bao gồm những thông tin về các nguy cơ đối với tài sản như hỏa hoạn, sét, hành động phá hoại, gió bão, mưa đá, v.v..., và thậm chí bao gồm những thông tin chi tiết để giúp đánh giá, ví dụ, tính hiệu quả của hệ thống vòi phun chữa cháy trong tòa nhà của bạn.

## **Thảm họa**

Các *thảm họa* là những sự kiện nghiêm trọng gây ra sự gián đoạn. Khung thời gian của sự gián đoạn có thể khác nhau, và mức độ của sự gián đoạn cũng vậy, nhưng điểm chung là sự kiện bên ngoài gây ra sự gián đoạn là sự kiện không thể ngăn chặn được. Chúng ta có thể biết trước [*sự kiện gây gián đoạn*], nhưng không nhất thiết ngăn chặn được. Các thảm họa thông thường bao gồm các sự kiện liên quan đến thời tiết và các sự kiện mà mọi người đều biết rằng cuối cùng sẽ xảy ra, không chỉ là ở đâu hoặc khi nào. Thảm họa do-con-người-gây-ra có thể đơn giản như việc một cấu hình sai dẫn đến mất một lượng dữ liệu đáng kể. Theo định nghĩa, "do-con-người-gây-ra" cho thấy thảm họa là kết quả của hành động của một số người nào đó. Chúng ta có thể thấy trước, có thể phòng ngừa được ở một mức độ nào đó, nhưng thậm chí những tai nạn vẫn có thể xảy ra. Việc có được chiến lược quản lý và giảm thiểu rủi ro đối với thảm họa là điều cực kỳ quan trọng.

Vào thời điểm cuốn sách này được viết, cả thế giới đang bị bao trùm bởi đại dịch COVID-19. Trên toàn thế giới, các văn phòng, các doanh nghiệp, trường học, nhà thờ và nhiều địa điểm tập trung khác đã bị phong tỏa trong nhiều tháng. Nhân viên làm việc tại nhà, nếu như họ có thể làm thế, thông qua Internet. Kết quả tác động vẫn đang tiếp diễn tính đến mùa hè năm 2020, nhưng hệ quả là rất rõ ràng - một đại dịch toàn cầu

sẽ là một trong những thảm họa lớn nhất mà thế hệ hiện tại đã từng trải qua, và đang thay đổi nhiều doanh nghiệp và nhiều quy trình nghiệp vụ.



**LƯU Ý** Theo FEMA, xấp xỉ 40 – 60% các doanh nghiệp nhỏ không bao giờ còn có thể tiếp tục mở cửa kinh doanh trở lại sau một thảm họa. Sau một thảm họa, 90% các công ty nhỏ hơn sẽ thất bại (đóng cửa) trong vòng 1 năm nếu như họ không thể khôi phục hoạt động trong vòng 5 ngày.

### **Môi trường**

Một trong những nguồn lớn nhất của các mối đe dọa đến từ môi trường. Những thay đổi *mang tính môi trường* có thể đến từ một loạt các nguồn khác nhau – thời tiết, sấm sét, các cơn bão, và thậm chí, các cơn bão mặt trời – và chúng đều có thể gây ra những thay đổi đối với các hệ thống theo cách gây ra sự gián đoạn những hoạt động bình thường. Những thay đổi này có thể làm gia tăng rủi ro. Mặc dù các biện pháp bảo mật CNTT không thể làm thay đổi các yếu tố môi trường có thể tác động đến các hoạt động nhưng chúng có thể có ảnh hưởng đến những rủi ro tương ứng với các vấn đề về môi trường. Việc khiến cho các hệ thống có khả năng phục hồi có thể làm giảm thiểu những tác động và giảm nhẹ những nguồn rủi ro này đối với doanh nghiệp. Và đôi khi, những tác động này có thể được cảm nhận từ khoảng cách rất xa, ví dụ, bạn có thể sao lưu đến một địa điểm ở xa như thế nào nếu như địa điểm ở xa này bị ngừng hoạt động do mất điện là kết quả của việc một nhánh cây bị gãy đổ do một cơn bão?

### **Do Con-người-gây-ra**

Những mối đe dọa *do-con-người-gây-ra* là những mối đe dọa có thể được cho là do hành động của một người gây ra. Tuy nhiên, những mối đe dọa

này không chỉ giới hạn ở các hành động thù địch của kẻ tấn công, chúng còn bao gồm những tai nạn của người dùng và quản trị viên hệ thống. Người dùng có thể đại diện cho một trong những rủi ro lớn nhất trong hệ thống CNTT. Nhiều tập tin bị mất do người dùng vô tình xóa nhầm hơn là bởi tin tặc, và đối với nhóm đang cố gắng khôi phục những tập tin đã bị mất, thẩm quyền không ảnh hưởng đến nỗ lực khôi phục. Các hành động của người dùng, chẳng hạn như vệ sinh mạng kém và sử dụng lại mật khẩu, đã được chứng minh là điểm khởi đầu cho nhiều sự kiện an ninh mạng lớn trong vài năm qua. Một quản trị viên hệ thống thiết lập cấu hình cho bản sao lưu không đúng cách, lỗi được phát hiện khi cần sao lưu và không có dữ liệu nào trên bản sao lưu để khôi phục có thể dễ dàng trở thành một thảm họa. Đây không phải là kết quả của một hoạt động thù địch, nhưng dù sao thì nó cũng có tính chất phá hoại. Các biện pháp kiểm soát thích hợp để quản lý rủi ro đối với hệ thống phải bao gồm các biện pháp kiểm soát chống lại cả các hành vi vô tình và các hành vi có mục đích.

### **Nội bộ so với Bên ngoài**

Như đã được đề cập trước đây cũng trong chương này, các mối đe dọa có thể đến từ các nguồn bên trong lẫn bên ngoài. Các mối đe dọa bên trong có nguồn gốc của chúng nằm trong phạm vi của một tổ chức, trong khi các rủi ro từ bên ngoài đến từ bên ngoài [tổ chức]. Khi các thảm họa được xem xét, chúng có thể được coi là có nguồn gốc từ bên trong hoặc bên ngoài công ty. Mặc dù luôn có thể dễ dàng đổ lỗi cho thế lực bên ngoài, nhưng trong rất nhiều trường hợp, các chính sách và thủ tục nội bộ làm gia tăng hồ sơ rủi ro của doanh nghiệp đối với các rủi ro bên ngoài đã được hiểu một cách dễ dàng. Nếu các quyết định của chuỗi cung ứng được đưa ra với một nhà cung cấp duy nhất ở nước ngoài chỉ vì một lợi thế nhỏ về giá, không có biện pháp dự phòng và sau đó một thảm họa ập đến quốc gia của nhà cung cấp, thì đây là rủi ro bên trong hay bên

ngoài? Nó có thể được xem như cả hai, nhưng một quyết định chính sách nội bộ dẫn đến rủi ro khi tiếp tục với một nhà cung cấp duy nhất.



**MÁCH NƯỚC CHO KỲ THI** Khi thực hiện đánh giá một mối đe dọa, hãy đảm bảo chắc chắn rằng bạn đã xem xét các mối đe dọa từ môi trường, do-con-người-gây-ra, và trong nội bộ. Trong kỳ thi, hãy đọc tình huống trước câu hỏi một cách cẩn thận để phân biệt nguồn nào trong số những nguồn đe dọa này là đáp án tốt nhất, khi nhiều nguồn là khá phổ biến nhưng chỉ một nguồn thường có rủi ro cao hơn.

### **Phân tích Tác động Kinh doanh (BIA)**

*Phân tích tác động kinh doanh (BIA)* là một quá trình được sử dụng để xác định những nguồn và giá trị tác động tương đối của các yếu tố rủi ro trong một quy trình. Đây cũng là tên gọi thường được sử dụng để mô tả một tài liệu được tạo ra bằng cách giải quyết những câu hỏi tương ứng với các nguồn rủi ro và các bước được thực hiện để giảm nhẹ chúng trong doanh nghiệp. BIA cũng phác thảo nên việc tổn thất của bất kỳ chức năng tối quan trọng nào của bạn sẽ có tác động đến tổ chức như thế nào. Phần này sẽ khám phá một loạt các thuật ngữ và khái niệm liên quan đến việc tiến hành một BIA.

### **Mục tiêu về Thời gian Khôi phục (RTO)**

Thuật ngữ *mục tiêu về thời gian khôi phục (RTO)* được sử dụng để mô tả đích nhắm mục tiêu về thời gian được thiết lập để khôi phục lại hoạt động sau một sự cố. Đây là một khoảng thời gian được xác định bởi doanh nghiệp, căn cứ vào nhu cầu của doanh nghiệp. Một RTO ngắn hơn dẫn đến việc tiêu tốn nhiều chi phí hơn bởi vì nó đòi hỏi sự phối hợp và nguồn lực nhiều hơn. Thuật ngữ này được sử dụng một cách phổ biến trong các hoạt động liên tục kinh doanh và khôi phục sau thảm họa.

## Mục tiêu Thời điểm Khôi phục (RPO)

*Mục tiêu về thời điểm khôi phục (RPO), một khái niệm hoàn toàn khác với RTO, là khoảng thời gian đại diện cho khoảng thời gian tối đa mà việc mất dữ liệu là có thể chấp nhận được. RPO xác định tần suất của hoạt động sao lưu cần thiết để ngăn chặn mức tổn thất dữ liệu không thể chấp nhận được. Một ví dụ đơn giản về việc xác lập RPO là trả lời cho câu hỏi sau: Bạn có thể chấp nhận mất bao nhiêu dữ liệu? Việc thực hiện lại công việc có thể chấp nhận được là bao nhiêu?*



### LƯU Ý

RTO và RPO dường như là có liên quan nhưng trong thực tế, chúng đo lường những điều hoàn toàn khác nhau. RTO phục vụ cho mục đích xác định các yêu cầu đối với liên tục kinh doanh, trong khi RPO giải quyết vấn đề về tần suất sao lưu dự phòng. Một điều khả dĩ là có một RTO 1 ngày và RPO 1 giờ, hoặc một RTO 1 giờ và 1 RPO 1 ngày. Yếu tố quyết định là nhu cầu của doanh nghiệp.



### MÁCH NƯỚC CHO KỲ THI

Hãy hiểu được sự khác biệt giữa RTO và RPO. RTO phục vụ cho mục đích xác định các yêu cầu đối với liên tục kinh doanh trong khi RPO giải quyết vấn đề tần suất sao lưu dự phòng.

## Thời gian Sửa chữa Trung bình (MTTR)

*Thời gian sửa chữa trung bình (MTTR) là một thước đo phổ biến về việc cần bao lâu để khắc phục một lỗi nhất định. Đây là thời gian trung bình và nó có thể hoặc không bao gồm thời gian cần thiết để có được các bộ phận thay thế. Danh sách Các từ viết tắt của CompTIA Security+ xác định *thời gian trung bình để khôi phục* (mean time to recover) như một ý nghĩa*

thay thế của MTTR. Trong cả hai trường hợp, MTTR được tính toán như sau:

$$\text{MTTR} = (\text{tổng thời gian ngừng hoạt động}) / (\text{số lần ngừng hoạt động})$$

Độ sẵn sàng là một thước đo tổng thời gian mà một hệ thống thực hiện chức năng đã định của nó. Độ tin cậy là một thước đo tần suất lỗi của hệ thống. Độ sẵn sàng có liên quan đến, nhưng khác với, độ tin cậy và thường được thể hiện bằng một tỷ lệ phần trăm của thời gian mà hệ thống đang trong trạng thái hoạt động của nó. Để tính toán độ sẵn sàng, cả MTBF và MTTR đều được cần đến:

$$\text{Độ sẵn sàng} = \text{MTBF} / (\text{MTBF} + \text{MTTR})$$

Giả sử một hệ thống có MTBF là 6 tháng và việc sửa chữa mất 30 phút, độ sẵn sàng sẽ được tính như sau:

$$\text{Độ sẵn sàng} = 6 \text{ tháng} / (6 \text{ tháng} + 30 \text{ phút}) = 99.9884\%$$

### **Thời gian Trung bình Giữa các lần Lỗi (MTBF)**

*Thời gian trung bình giữa các lần lỗi (MTBF)* là một thước đo phổ biến về độ tin cậy của một hệ thống và là sự thể hiện thời gian trung bình giữa các lần hệ thống bị lỗi. Thời gian giữa các lần bị lỗi được đo từ thời gian một hệ thống quay trở lại hoạt động cho đến lần bị lỗi tiếp theo. MTBF là một giá trị trung bình cộng của tập hợp các lần hệ thống bị lỗi:

$$\text{MTBF} = \Sigma (\text{bắt đầu thời gian ngừng hoạt động} - \text{bắt đầu thời gian hoạt động trở lại}) / \text{số lần bị lỗi}$$

Thời gian có ý nghĩa cho đến khi bị lỗi (mean time to failure – MTTF) là một biến thể khác của MTBF, là một thước đo được sử dụng một cách phổ biến để thay cho MTBF khi hệ thống được thay thế để sửa chữa. Ngoài

sự khác biệt về ngữ nghĩa, các phép tính là giống nhau, và ý nghĩa về cơ bản là như nhau.



**MÁCH NƯỚC CHO KỲ THI** Mặc dù MTBF và MTTR có vẻ giống nhau nhưng chúng đo lường những điều khác nhau. Các câu hỏi trong bài thi có thể yêu cầu bạn thực hiện các tính toán đơn giản. Các lựa chọn đáp án sai sẽ phản ảnh những sai sót đơn giản về tỷ lệ, vì vậy hãy tính toán một cách cẩn trọng.

### Các Kế hoạch Khôi phục Chức năng

Các tai nạn, thảm họa và gián đoạn đối với các quy trình kinh doanh luôn diễn ra. Đây là lý do tại sao chúng ta có các kế hoạch liên tục kinh doanh (BCPs). Nhưng tiếp theo sẽ là gì? Các *kế hoạch khôi phục chức năng* đại diện cho bước tiếp theo – sự chuyển đổi từ các hoạt động trong [kế hoạch] liên tục kinh doanh sang hoạt động như bình thường. Cũng giống như việc chuyển đổi sang hoạt động liên tục kinh doanh cần phải được lập kế hoạch, kế hoạch khôi phục chức năng cũng vậy. Trong khi việc chuyển tiếp sang hoạt động sau thảm họa là khá nhanh chóng, và việc hoạch định được căn cứ vào quá trình đánh giá đã được ưu tiên về mức độ quan trọng liên quan đến việc tiếp tục hoạt động, cơ sở đối với kế hoạch khôi phục chức năng sẽ khác. Kế hoạch khôi phục chức năng có thể phải được tổ chức và chia giai đoạn chặt chẽ hơn theo thời gian, hoạt động để thúc đẩy tính hiệu quả nhất quán thay vì theo đuổi tốc độ. Việc này có thể được thực hiện theo từng chức năng và được định hướng bởi các nhu cầu về chức năng.

### Điểm Đơn Lỗi

Một nguyên tắc then chốt của bảo mật là chiều sâu của biện pháp phòng thủ. Phương pháp tiếp cận phân lớp này đối với bảo mật được thiết kế để

loại bỏ bất kỳ điểm đơn lỗi cụ thể (single point of failure – SPOF) nào. Một *điểm đơn lỗi* là bất kỳ thành phần hệ thống nào nếu bị lỗi hoặc bị trực tiếp có thể dẫn đến lỗi của toàn bộ hệ thống. Một ví dụ về điểm đơn lỗi sẽ là một kết nối Internet duy nhất – dù tốt cho một doanh nghiệp nhỏ nhưng không tốt đối với một doanh nghiệp lớn với những máy chủ đang cung cấp nội dung nào đó cho các khách hàng. Dự phòng sẽ tốn kém nhưng nếu như chi phí cho biện pháp thay thế không thành công thì việc triển khai các mức độ dự phòng là điều hoàn toàn có thể chấp nhận được. Đối với các hệ thống thiết yếu-đối-với-sứ-mệnh, các điểm đơn lỗi là những hạng mục cần phải được các cấp quản lý quan tâm, với sự diễn giải đầy đủ về rủi ro và chi phí liên quan đến chúng. Trong một số tình huống, việc tránh một điểm đơn lỗi có thể là không khả thi hoặc không thực tế, và trong trường hợp đó, mọi người trong tổ chức đang chịu trách nhiệm quản lý rủi ro nên tìm hiểu bản chất của tình huống và hồ sơ rủi ro dẫn đến [từ tình huống].

### **Kế hoạch Khôi phục sau Thảm họa (DRP)**

Một *kế hoạch khôi phục sau thảm họa (DRP)* là một kế hoạch mà một công ty tạo ra để quản lý sự tác động đến việc kinh doanh của một thảm họa và để khôi phục lại [hoạt động] sau tác động của thảm họa. Chi tiết đối với các kế hoạch khôi phục sau thảm họa được đề cập trong Chương 27, "Các Chính sách và Thủ tục Ứng phó Sự cố".

### **Các Chức năng Thiết-yếu-đối-với-Sứ-mệnh**

Khi kiểm tra rủi ro và những tác động đối với việc kinh doanh, điều quan trọng là phải xác định được các chức năng tối-quan-trọng-đối-với-sứ-mệnh giữa các chức năng nghiệp vụ khác. Trong hầu hết các doanh nghiệp, phần lớn các chức năng hàng ngày, mặc dù rất quan trọng, nhưng không phải là thiết yếu đối với sứ mệnh. Các *chức năng thiết-yếu-đối-với-sứ-mệnh* là những chức năng nếu không diễn ra hoặc không được thực

hiện một cách đúng đắn sẽ gây ảnh hưởng trực tiếp đến sứ mệnh của tổ chức. Nói cách khác, các chức năng thiết-yếu-đối-với-sứ-mệnh là những chức năng phải được khôi phục trước tiên sau một tác động kinh doanh để cho phép tổ chức khôi phục lại hoạt động của mình. Lý do mà việc xác định các chức năng này là rất quan trọng đối với việc quản lý rủi ro rất đơn giản: bạn nên dành phần lớn nỗ lực của mình để bảo vệ các chức năng thiết yếu. Các chức năng khác có thể cần phải được bảo vệ, nhưng sự suy yếu của chúng sẽ không gây ra tác động tức thời như sự suy yếu của chức năng thiết-yếu-đối-với-sứ-mệnh sẽ gây ra.

### **Xác định các Hệ thống Thiết yếu**

Một phần của việc xác định các chức năng thiết-yếu-đối-với-sứ-mệnh là việc xác định các hệ thống và dữ liệu hỗ trợ cho các chức năng. *Xác định các hệ thống thiết yếu* cho phép nhóm bảo mật thiết lập mức ưu tiên thích hợp cho các biện pháp phòng thủ để bảo vệ các hệ thống và dữ liệu theo cách tương xứng với rủi ro có liên quan. Nó cũng cho phép việc thiết lập trình tự hợp lý của việc khôi phục lại các hoạt động để đảm bảo sự khôi phục các dịch vụ một cách phù hợp.

### **Đánh giá Rủi ro của Địa điểm**

Đánh giá rủi ro có thể có những đặc trưng cụ thể tương xứng với các địa điểm khác nhau. Đây chính là cơ sở cho *đánh giá rủi ro của địa điểm*, vốn chỉ đơn giản là một quá trình đánh giá rủi ro được điều chỉnh theo một địa điểm cụ thể. Trong các tổ chức có nhiều vị trí, với các hệ thống và hoạt động khác nhau, việc có được những quá trình đánh giá rủi ro đã được điều chỉnh cụ thể đối với những rủi ro tương ứng với từng địa điểm sẽ cung cấp thêm thông tin cho công ty. Có thể có một số phần tử về tổng thể là cụ thể đối với công ty, nhưng sự phát triển và bao gồm các rủi ro tương ứng với từng địa điểm cung cấp một tài liệu hợp lý và có thể được sử dụng một cách hiệu quả.

## Tóm tắt Chương

Trong chương này, bạn đã làm quen với việc kiểm tra rủi ro từ quan điểm phân tích tác động kinh doanh (BIA). Chương này mở đầu bằng việc kiểm tra các loại rủi ro, bao gồm bên ngoài, bên trong, hệ thống kế thừa, nhiều bên, trộm cắp IP và tuân thủ/cấp phép phần mềm. Phần tiếp theo thảo luận về các chiến lược quản lý rủi ro, trong đó chấp nhận, tránh, chuyển giao (bao gồm cả bảo hiểm an ninh mạng) và giảm nhẹ đều được đề cập.

Chủ đề của phân tích rủi ro hình thành nên phần lớn của chương, trong đó các chủ đề là sổ đăng ký rủi ro, ma trận rủi ro/bản đồ nhiệt, đánh giá biện pháp kiểm soát rủi ro, tự-đánh-giá biện pháp kiểm soát rủi ro và nhận thức rủi ro. Các chủ đề tiếp theo được trình bày là rủi ro cố hữu, rủi ro tồn dư, rủi ro kiểm soát và khẩu vị rủi ro. Những chủ đề này tuân theo các quy định ảnh hưởng đến tình thế rủi ro và các loại đánh giá rủi ro, bao gồm cả định tính và định lượng. Sau đó, phần này chuyển sang tính toán rủi ro định lượng bằng cách sử dụng khả năng xảy ra, tác động, giá-trị-của-tài-sản, tổn-thất-đơn-lẻ dự kiến (SLE), tổn thất hàng năm dự kiến (ALE) và tỷ lệ xuất hiện hàng năm (ARO).

Các thảm họa được đề cập tiếp theo đó, bao gồm cả [thảm họa] môi trường và do-con-người-gây-ra, và các rủi ro bên trong so với bên ngoài đã được kiểm tra.

Chương này kết thúc bằng việc kiểm tra phân tích tác động kinh doanh. Trong phần này, các chủ đề kỹ thuật được đề cập là mục tiêu về thời gian khôi phục (RTO), mục tiêu về thời điểm khôi phục (RPO), thời gian trung bình để sửa chữa (MTTR) và thời gian trung bình giữa các lần hư hỏng (MTBF). Các đề mục tiếp theo được thảo luận là kế hoạch khôi phục chức năng, các điểm lỗi đơn lẻ, kế hoạch khôi phục sau thảm họa (DRP), các chức năng thiết yếu-đối-với-sứ-mệnh, xác định các hệ thống thiết yếu và đánh giá rủi ro của địa điểm.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

1. Tên gọi nào dưới đây thường được sử dụng để mô tả quy trình giải quyết những câu hỏi tương ứng với các nguồn rủi ro, những tác động của chúng, và các bước được thực hiện để giảm nhẹ chúng trong doanh nghiệp?

  - A. Đánh giá rủi ro**
  - B. Phân tích tác động kinh doanh**
  - C. Đánh giá mối đe dọa**
  - D. Kiểm nghiệm xâm nhập.**
2. Những thuật ngữ nào dưới đây được sử dụng để mô tả đích nhắm mục tiêu thời gian được thiết lập để khôi phục lại hoạt động sau một sự cố?

  - A. RPO**
  - B. MTBF**
  - C. RTO**
  - D. MTTR.**
3. Điều nào dưới đây là một thước đo phổ biến về việc mất bao nhiêu thời gian để khắc phục một lỗi nhất định?

  - A. MTTR**
  - B. RTO**
  - C. RPO**
  - D. MTBF.**
4. Thành phần hệ thống nào dưới đây nếu bị lỗi hoặc hoạt động sai có thể dẫn đến lỗi của toàn bộ hệ thống?

  - A. Thời gian trung bình giữa các lần hư hỏng**

- B.** Điểm đơn lối
- C.** Tổn-thất-đơn-lẻ dự kiến
- D.** Khả năng xảy ra.
- 5.** Quá trình nào sau đây là quá trình xác định một cách chủ quan tác động của một sự kiện có ảnh hưởng đến dự án, chương trình hoặc doanh nghiệp?
- A.** Khả năng xảy ra
- B.** Kế hoạch khôi phục chức năng
- C.** Đánh giá rủi ro định tính
- D.** Đánh giá rủi ro định lượng.
- 6.** Câu nào sau đây mô tả các chức năng thiết-yếu-đổi-với-sứ-mệnh? (Chọn tất cả các đáp án đúng).
- A.** Các chức năng mà nếu chúng không diễn ra, sẽ có ảnh hưởng trực tiếp đến sứ mệnh của tổ chức
- B.** Các chức năng, nếu chúng không được thực hiện một cách đúng đắn, sẽ ảnh hưởng trực tiếp đến sứ mệnh của tổ chức
- C.** Các chức năng được coi là thiết yếu đối với tổ chức
- D.** Các chức năng kinh doanh thông thường.
- 7.** Mô tả nào dưới đây là mô tả đúng nhất về rủi ro?
- A.** Chi phí liên quan đến một rủi ro đã hiện thực hóa
- B.** Khả năng một điều gì đó không hoạt động theo kế hoạch
- C.** Thiệt hại do rủi ro không thể khắc phục được
- D.** Mức độ quan tâm của một ai đó chú trọng đến hạnh phúc của con người.
- 8.** Tác động nào sau đây được coi là trọng tài cuối cùng của tất cả các hoạt động theo nhiều cách vì đó là cách chúng ta "giữ điểm"?
- A.** Danh tiếng
- B.** An toàn
- C.** Tài chính

**D. Sinh mạng.**

- 9.** Giá trị nào dưới đây là đại diện cho tần suất của một sự kiện, được đo trong một năm tiêu chuẩn?
- A.** Tổn thất hàng năm dự kiến (ALE)
  - B.** Tỷ lệ xảy ra hàng năm (ARO)
  - C.** Tổn-thất-đơn-lẻ dự kiến (SLE)
  - D.** Tỷ lệ xảy ra hàng năm dự kiến (AEO).
- 10.** Điều nào sau đây thể hiện phương thức chuyển tiếp rủi ro cho bên thứ ba?
- A.** Áp dụng các biện pháp kiểm soát để giảm thiểu tác động của rủi ro
  - B.** Tạo ra một hồ sơ thông tin về các rủi ro đã được xác định
  - C.** Phát triển và chuyển tiếp các kết quả của ma trận rủi ro/bản đồ nhiệt
  - D.** Mua bảo hiểm an ninh mạng.

## Đáp án

- 1. B.** Phân tích tác động kinh doanh (BIA) là tên gọi thường được sử dụng để mô tả một tài liệu đã được tạo ra bằng cách giải quyết những câu hỏi tương ứng với các nguồn rủi ro và các bước được thực hiện để giảm nhẹ chúng trong doanh nghiệp. Đánh giá rủi ro là một phương pháp để phân tích rủi ro tiềm ẩn dựa trên các mô hình thống kê và mô hình toán học. Một phương pháp phổ biến là tính toán tổn thất hàng năm dự kiến (ALE). Một đánh giá mối đe dọa là một phân tích có cấu trúc về các mối đe dọa mà một doanh nghiệp phải đương đầu. Các kiểm nghiệm xâm nhập được sử dụng bởi các tổ chức đang muốn kiểm tra tình hình bảo mật trong-thực-tế của họ.
- 2. C.** Thuật ngữ mục tiêu về thời gian khôi phục (RTO) được sử dụng để mô tả đích nhắm mục tiêu về thời gian được thiết lập để bắt đầu lại hoạt động sau một sự cố. Mục tiêu về thời điểm khôi phục (RPO) thể hiện khoảng thời gian tối đa mà việc tổn thất dữ liệu là có thể chấp nhận được. Thời gian trung bình giữa các lần hư hỏng (MTBF) là một thước đo phổ biến về độ tin cậy của một hệ thống và là một biểu hiện của thời gian trung bình của các lần hư hỏng của hệ thống. Thời gian trung bình để sửa chữa (MTTR) là một thước đo phổ biến về thời gian tiêu tốn để sửa chữa một lỗi nhất định.
- 3. A.** Thời gian trung bình để sửa chữa (MTTR) là thước đo phổ biến để đánh giá thời gian tiêu tốn để sửa chữa một lỗi nhất định. Mục tiêu về thời gian khôi phục (RTO) mô tả đích nhắm mục tiêu thời gian được thiết lập để bắt đầu lại hoạt động sau sự cố. Mục tiêu về thời điểm khôi phục (RPO) thể hiện khoảng thời gian tối đa mà việc mất dữ liệu là có thể chấp nhận được. Thời gian trung bình giữa các lần hư hỏng (MTBF) là thước đo phổ biến về độ tin cậy

của hệ thống và là biểu hiện của thời gian trung bình giữa các lần hư hỏng của hệ thống.

4. **B.** Điểm đơn lỗi là bất kỳ khía cạnh nào của hệ thống, nếu được kích hoạt, có thể gây ra sự cố của toàn bộ hệ thống. Thời gian trung bình giữa các lần hư hỏng (MTBF) là thước đo phổ biến về độ tin cậy của hệ thống và là biểu hiện của thời gian trung bình giữa các lần hư hỏng của hệ thống. Tổn thất đơn lẻ dự kiến (SLE) là tổn thất dự kiến do rủi ro xảy ra đối với một tài sản. Khả năng xảy ra là khả năng mà một rủi ro cụ thể sẽ xảy ra.
5. **C.** Đánh giá rủi ro định tính là quá trình xác định một cách chủ quan tác động của một sự kiện gây ảnh hưởng đến dự án, chương trình hoặc doanh nghiệp. Khả năng xảy ra là khả năng mà một rủi ro cụ thể sẽ xảy ra. Các kế hoạch khôi phục chức năng thể hiện sự chuyển đổi từ hoạt động theo [kế hoạch] liên tục kinh doanh trở lại hoạt động bình thường. Đánh giá rủi ro định lượng là quá trình xác định một cách khách quan tác động của một sự kiện gây ảnh hưởng đến dự án, chương trình hoặc doanh nghiệp.
6. **A, B và C.** Các chức năng thiết-yếu-đối-với-sứ-mệnh là những chức năng mà nếu chúng không xảy ra hoặc không được thực hiện một cách đúng đắn sẽ gây ảnh hưởng trực tiếp đến sứ mệnh của tổ chức. Đây là nơi bạn dành phần lớn nỗ lực của mình - bảo vệ các chức năng thiết yếu. Điều quan trọng là phải tách biệt các chức năng thiết-yếu-đối-với-sứ-mệnh ra khỏi các chức năng nghiệp vụ khác.
7. **B.** Rủi ro là khả năng một điều gì đó không hoạt động như đã được lập kế hoạch và gây ra một tác động bất lợi. Tác động là chi phí liên quan đến rủi ro đã hiện thực hóa. Thiệt hại tài sản có thể là kết quả của rủi ro không thể giảm nhẹ được. An toàn là khi bạn

xem xét mức độ quan tâm của một ai đó đối với mức độ hạnh phúc của con người.

8. **C.** Tài chính, theo nhiều cách, là trọng tài cuối cùng của tất cả các hoạt động bởi vì nó là cách chúng ta giữ điểm. Những điều khác là quan trọng nhưng không được coi là trọng tài cuối cùng.
9. **B.** Tỷ lệ xuất hiện hàng năm (ARO) là đại diện cho tần suất của sự kiện, được đo trong một năm tiêu chuẩn. Tổn thất hàng năm dự kiến (ALE) được tính bằng cách nhân tổn-thất-đơn-lẻ dự kiến (SLE) với khả năng hoặc số lần sự kiện dự kiến sẽ xảy ra trong một năm. SLE được tính bằng cách nhân giá trị tài sản với hệ số tiếp xúc [với rủi ro]. Tỷ lệ xảy ra dự kiến hàng năm (AEO) không phải là một thuật ngữ được sử dụng trong ngành công nghiệp an ninh mạng.
10. **D.** Một phương pháp phổ biến để chuyển rủi ro là mua bảo hiểm an ninh mạng. Bảo hiểm cho phép chuyển rủi ro cho một bên thứ ba đang quản lý các loại rủi ro cụ thể cho nhiều bên, từ đó giảm thiểu được các chi phí riêng lẻ. Việc áp dụng các biện pháp kiểm soát làm giảm tác động của rủi ro mô tả việc giảm nhẹ rủi ro. Số đăng ký rủi ro là "một bản ghi thông tin về các rủi ro đã được xác định," như được định nghĩa trong tài liệu tham khảo *ISO Guide 73:2009 Quản lý rủi ro — Từ vựng*. Ma trận rủi ro/bản đồ nhiệt được sử dụng để hiển thị một cách trực quan các kết quả của phân tích rủi ro định tính.

## Chương 35 Quyền riêng tư

### Quyền riêng tư

Trong chương này, bạn sẽ:

- Khám phá những khái niệm về quyền riêng tư và dữ liệu nhạy cảm,
- Lập mối tương quan giữa những nỗ lực quyền riêng tư với những nỗ lực bảo mật.

Những thực tiễn bảo mật dữ liệu và quyền riêng tư là có mối quan hệ qua lại với nhau bởi vì tiền đề cơ bản để có quyền riêng tư thì bạn phải có bảo mật. Quyền riêng tư được định nghĩa là biện pháp kiểm soát mà bạn thực hiện đối với dữ liệu của bạn, và bảo mật là một phần tử then chốt của biện pháp kiểm soát. Quyền riêng tư dữ liệu trong một tổ chức là sự ngăn chặn việc sử dụng trái phép những dữ liệu đang được nắm giữ bởi tổ chức. Một phương pháp để đảm bảo quyền riêng tư là thông qua việc sử dụng các kỹ thuật tăng-cường-quyền-riêng-tư. Các thành phần hỗ trợ cho những nỗ lực về quyền riêng tư dữ liệu bao gồm việc dán nhãn và xử lý một cách đúng đắn những dữ liệu nhạy cảm, chỉ định trách nhiệm đối với việc bảo vệ dữ liệu, và lưu trữ một cách an toàn những dữ liệu được giữ lại, tất cả đều được đề cập trong chương này.

#### Mục tiêu Chứng nhận

Chương này đề cập đến mục tiêu 5.5 của kỳ thi CompTIA Security+: Diễn giải các khái niệm về quyền riêng tư và dữ liệu nhạy cảm trong mối tương quan với bảo mật.

## Những Hậu quả của việc Vi phạm Quyền Riêng tư đối với Tổ chức

Khi một công ty đánh mất dữ liệu đã được lưu trữ trên hệ thống mạng của mình, thuật ngữ được sử dụng là *vi phạm dữ liệu* (*data breach*). Các vi phạm dữ liệu đã trở thành một mục tin tức hầu như hàng ngày, và kết quả là mọi người trở nên bớt nhạy cảm hơn với sự xuất hiện của chúng. Vi phạm dữ liệu đóng vai trò như một phương tiện thông báo rằng những nỗ lực bảo mật đã thất bại.

Verizon công bố một báo cáo vi phạm dữ liệu thường niên để kiểm tra những loại hình và nguyên nhân của vi phạm dữ liệu trong năm trước đó. Những kết quả này được trình bày dưới nhiều hình thức, phân bổ theo kiểu tấn công, loại người tấn công, ngành, khu vực địa lý, quy mô công ty, và còn nhiều nữa, cung cấp một mức độ phân tích chi tiết đáng kể về các sự cố. Báo cáo này là một khuôn khổ về những gì thực tế đã xảy ra với các công ty trong đời thực với những chương trình bảo mật thực, hoặc bất chấp những chương trình bảo mật của họ. Đây là một bộ sưu tập dữ liệu vô giá, có thể cung cấp những định hướng liên quan đến môi trường mối đe dọa hiện tại và những kết quả của các cuộc tấn công và các lối trong thực tế.

## Tổn hại Danh tiếng

*Tổn hại danh tiếng* là một hình thức thiệt hại gây ra đối với thương hiệu của một công ty. Khách hàng quyết định lựa chọn khi họ tham gia vào một giao dịch thương mại, và các doanh nghiệp dành rất nhiều thời gian và nguồn lực để xây dựng thương hiệu tạo để điều kiện cho quyết định mua hàng đối với công ty của họ. Việc phải thông báo cho tất cả các khách hàng về sự kiện vi phạm/tiết lộ thực sự gây tổn hại cho thương hiệu của một công ty. Một nhà cung cấp máy tính trực tuyến, Egghead, đã gặp phải một sự kiện vi phạm/tiết lộ vào thời điểm gần mùa mua sắm

nghỉ lẽ và họ đã chứng kiến doanh số bán hàng sụt giảm nghiêm trọng trong giai đoạn quan trọng đó và dẫn đến phá sản ngay sau đó.

Target Corporation tiếp tục trở thành ví dụ về kỷ lục cho các vụ vi phạm đầy tốn kém, với một vụ vi phạm trong năm 2013 đã làm tiêu tốn hàng trăm triệu đô-la Mỹ và khiến cho nhiều giám đốc điều hành cấp cao bị mất việc. Facebook đã gia nhập câu lạc bộ này với vụ bê bối Cambridge Analytica năm 2018, khi họ đã thất bại trong việc bảo vệ những thông tin cá nhân của người dùng của họ, và đã phải đổi mới với các yêu cầu pháp lý và quy định giám sát cũng như với việc kích hoạt các biện pháp ứng phó chỉ thị bảo vệ dữ liệu của Liên minh Châu Âu.

### **Đánh cắp Danh tính**

*Đánh cắp danh tính* xảy ra khi một tội phạm, bằng cách sử dụng những thông tin bị đánh cắp, mạo nhận danh tính của một cá nhân khác để có được và sử dụng thẻ tín dụng dưới danh nghĩa của nạn nhân. Nếu như việc tiết lộ dữ liệu dẫn đến những tổn thất trong thông tin cá nhân của khách hàng thì các quy định có thể bắt buộc một công ty chịu trách nhiệm cho việc chia sẻ những rủi ro về việc mất cắp danh tính đối với nạn nhân. Biện pháp ứng phó thông thường của một công ty là mua một chính sách dịch vụ bảo vệ chống lại việc đánh cắp danh tính đối với các cá nhân bị ảnh hưởng bởi vụ vi phạm. Việc này có thể tiêu tốn đến 50 đô-la Mỹ cho mỗi cá nhân bị ảnh hưởng, khiến cho việc vi phạm một triệu hồ sơ trở thành một vấn đề cực kỳ tốn kém.

### **Hình phạt**

Các cơ quan quản lý, chẳng hạn như Ủy ban Thương mại Liên bang (Federal Trade Commission - FTC), có khả năng thu tiền phạt khi các quy định đã không được tuân thủ. Những khoản tiền phạt này không phải là nhỏ. Ở Liên minh Châu Âu, các khoản phạt theo Quy định Chung về Bảo vệ Dữ liệu (General Data Protection Regulation - GDPR) có thể là 4%

doanh thu của một công ty và số tiền phạt lên đến hàng trăm triệu euro đã được thu. Tại Hoa Kỳ, Equifax đã bị phạt gần 700 triệu đô-la Mỹ để bồi thường cho những người dùng bị ảnh hưởng bởi vụ vi phạm dữ liệu của họ.

### **Đánh cắp Tài sản Sở hữu Trí tuệ**

Một trong những đích nhắm của một kẻ tấn công trên một hệ thống là tài sản trí tuệ. *Đánh cắp tài sản trí tuệ* là một hậu quả nghiêm trọng đối với tổ chức khi nó xảy ra, vì khi nó xảy ra, thiệt hại có thể trở nên không rõ ràng cho đến khi các tài liệu được sử dụng bởi một đối thủ cạnh tranh. Trong những tổ chức với các mức độ tài sản trí tuệ đáng kể, đây là một trong những hạng mục quan trọng nhất cần phải được bảo vệ chống lại sự tổn hại. Số năm đầu tư và nhiều năm doanh thu và lợi nhuận tiềm năng có thể nhanh chóng biến mất nếu Tài sản Trí tuệ bị đánh cắp và được sử dụng để chống lại một công ty một cách tích cực.



### **MÁCH NƯỚC CHO KỲ THI**

Hãy nhận thức được những hậu quả đối với tổ chức của việc vi phạm dữ liệu có thể dẫn đến tổn hại về danh tiếng, đánh cắp danh tính, các khoản tiền phạt và trộm cắp Tài sản Trí tuệ.

### **Thông báo Vi phạm**

Trong một thế giới lý tưởng sẽ không bao giờ có bất kỳ vụ vi phạm dữ liệu nào, do đó cũng sẽ không bao giờ cần đến các quy trình trong trường hợp vi phạm dữ liệu. Nhưng đây không phải là một thế giới lý tưởng, và những vi phạm vẫn luôn xảy ra. Và thậm chí ngay cả khi một sự cố chưa xảy ra với công ty của bạn thì hầu như mọi cơ quan tài phán của chính phủ đều ban hành một loạt các đạo luật và quy định về trách nhiệm của công ty trong các trường hợp vi phạm. Việc tìm hiểu và chuẩn bị sẵn sàng

để đưa ra *thông báo* về các vi phạm theo các luật và chỉ thị này là điều rất quan trọng, bởi vì một khi vi phạm xảy ra, thời gian để thực hiện những điều đúng đắn là rất ngắn và các hình phạt có thể sẽ rất đáng kể.

Các đạo luật và quy định về thông báo vi phạm thường có các định nghĩa cụ thể về những gì cấu thành một hành vi vi phạm, những thực thể nào được bảo vệ, các yêu cầu thông báo cụ thể là gì và các yếu tố chính như sự chậm trễ theo yêu cầu của các cơ quan thực thi pháp luật. Do có rất nhiều quy tắc và quy định khác nhau nên thực tiễn tốt nhất thường là tuân theo các quy định nghiêm ngặt nhất, chẳng hạn như quy định về quyền riêng tư của California ở Hoa Kỳ và GDPR ở Liên minh Châu Âu, để đảm bảo phạm vi áp dụng đầy đủ.

### **Leo thang**

Khi một vụ vi phạm dữ liệu xảy ra trong doanh nghiệp, điều quan trọng là có được một quy trình để *leo thang* sự cố lên các cấp bên trong tổ chức của bạn. Hầu hết các vụ vi phạm dữ liệu đều được khám phá như một phần của một số quy trình ứng phó sự cố, và vụ vi phạm cần phải có biện pháp ứng phó tách biệt khỏi sự cố ban đầu. Việc thiết lập chính sách leo thang vi phạm cùng với các thủ tục đi kèm theo sẽ đảm bảo mức quan tâm thích hợp của các cấp quản lý đến quá trình tối quan trọng này. Việc không leo thang vi phạm cho các cơ quan có thẩm quyền thích hợp có thể dẫn đến những rủi ro tài chính và pháp lý bên ngoài, và do đó, cấp quản lý cần phải nhận thức được sự việc và tiến trình thực hiện những trách nhiệm của công ty.

### **Thông báo và Tiết lộ Công khai**

Rất nhiều đạo luật và quy định liên quan đến vi phạm thông tin yêu cầu tiết lộ công khai các vi phạm bảo mật máy tính mà theo đó, thông tin bí mật chưa được mã hóa của bất kỳ cư dân nào có thể đã bị xâm phạm. Các đạo luật này áp dụng cho bất kỳ cá nhân hoặc thực thể nào đang tiến

hành thực hiện việc kinh doanh trong khu vực pháp lý đã được quy định, thậm chí ngay cả khi nằm ngoài tiểu bang và đang sở hữu hoặc cấp phép dữ liệu đã được tin học hóa bao gồm cả thông tin cá nhân. Đây là một yêu cầu của [đạo luật] California SB 1386, là luật mẫu được sử dụng bởi nhiều cơ quan chính phủ khác. Mặc dù không có đạo luật hoặc quy định chung nào trong lĩnh vực này, nhưng hầu hết đều có một số hình thức yêu cầu công bố thông tin công khai.

### Các Kiểu Dữ liệu

Dữ liệu tồn tại dưới nhiều hình thức và được lưu trữ trong các hệ thống để được sử dụng như một phần của các quy trình nghiệp vụ. Quản lý dữ liệu là một tập hợp phức tạp của các nhiệm vụ phục vụ cho mục đích bảo vệ dữ liệu khỏi một loạt các rủi ro khác nhau, bao gồm mất mát dữ liệu. Việc quản lý một lượng lớn và đa dạng các kiểu dữ liệu, thành phần, và các nhu cầu cụ thể của chúng từ quan điểm bảo mật sẽ được thực hiện một cách dễ dàng hơn nếu như dữ liệu được nhóm lại thành một loạt các *kiểu dữ liệu*. Những kiểu [dữ liệu] này có thể bao gồm các nhu cầu bảo vệ cơ bản, hoặc các nguồn của dữ liệu, và do đó không phải là một phép phân loại mà thay vào đó là một tập hợp các nhãn quản lý được sử dụng để cảnh báo người dùng về các yêu cầu cụ thể tương ứng với dữ liệu. Hai kiểu dữ liệu khác nhau sẽ được thảo luận trong những phần dưới đây: một bộ các nhãn xác định các mối quan tâm/hạn chế về quá trình xử lý và việc gán nhãn về các yếu tố xem liệu chúng có thể được truy nguyên đến các cá nhân cụ thể hay không. Mỗi nhãn dán này hỗ trợ cho doanh nghiệp trong việc bảo vệ và xử lý một cách thích hợp những dữ liệu trong suốt vòng đời của chúng.

### Phân loại

Các chương trình *phân loại* dữ liệu hiệu quả bao gồm các biện pháp để đảm bảo việc gán nhãn và xử lý tính nhạy cảm của dữ liệu để từ đó nhận

viên biết được liệu dữ liệu đó có nhạy cảm hay không và hiểu được mức bảo vệ cần thiết. Khi dữ liệu nằm trong một hệ thống xử-lý-thông-tin, các biện pháp bảo vệ nên được thiết kế bên trong hệ thống. Những khi dữ liệu rời khỏi cái kén bảo vệ này, dù là bằng cách in ấn, tải về hoặc sao chép, nó cần phải được bảo vệ liên tục bằng các phương tiện khác. Đây là nơi mà việc gán nhãn về tính nhạy cảm của dữ liệu sẽ hỗ trợ người dùng trong việc hoàn thành trách nhiệm của họ. Việc đào tạo để đảm bảo rằng việc gán nhãn thực sự diễn ra và rằng nó được sử dụng và tuân thủ là điều quan trọng đối với người dùng, những người có những vai trò có thể bị tác động bởi tài liệu này.

Việc gán nhãn đóng một vai trò quan trọng trong việc đảm bảo việc xử lý và tiêu hủy dữ liệu đúng cách. Những nhân viên có liên quan mật thiết đến một số nhiệm vụ cụ thể tương ứng với việc xử lý dữ liệu và phá hủy/tiêu hủy dữ liệu và nếu được đào tạo thích hợp, có thể hoạt động như một kiểm soát bảo mật. Nhân viên không được đào tạo hoặc được đào tạo một cách không đầy đủ sẽ không phải là kiểm soát bảo mật hiệu quả, và trên thực tế, có thể là một nguồn nguy cơ tiềm ẩn.

Một thành phần quan trọng của bảo mật CNTT là việc bảo vệ những thông tin đã được xử lý và lưu trữ trên các hệ thống và mạng máy tính. Các tổ chức xử lý nhiều kiểu thông tin khác nhau, và họ cần phải công nhận rằng không phải mọi thông tin đều có tầm quan trọng hoặc độ nhạy cảm như nhau. Điều này đòi hỏi sự phân loại thông tin thành các thể loại khác nhau, mỗi thể loại có các yêu cầu riêng để quản lý nó. Các yếu tố có ảnh hưởng đến việc phân loại thông tin cụ thể bao gồm giá trị của thông tin đối với tổ chức (tác động sẽ như thế nào đối với tổ chức nếu tổ chức đánh mất thông tin này?), tuổi thọ của thông tin và các đạo luật hoặc quy định chi phối việc bảo vệ thông tin đó. Hệ thống phân loại thông tin được biết đến rộng rãi nhất được triển khai bởi chính phủ Hoa Kỳ (bao

gồm cả quân đội), phân loại thông tin thành các thể loại như Bí mật, Tuyệt mật và Tối mật (Confidential, Secret và Top Secret). Các doanh nghiệp có những mong muốn tương tự để bảo vệ thông tin và thường sử dụng các thể loại [phân loại thông tin] như Bí mật, Riêng tư, Công khai, Độc quyền, PII và PHI. Mỗi chính sách phân loại thông tin nên mô tả cách thức bảo vệ thông tin, ai có thể tiếp cận thông tin, ai có thẩm quyền công bố thông tin và cách thức công bố cũng như cách thức tiêu hủy thông tin như thế nào. Mọi nhân viên của tổ chức nên được đào tạo về các thủ tục xử lý thông tin mà họ được cấp phép truy cập.

## Công khai

Dữ liệu *công khai* là dữ liệu có thể được nhìn thấy bởi công chúng và không cần sự bảo vệ nào liên quan đến tính bảo mật. Điều quan trọng là bảo vệ sự toàn vẹn của dữ liệu công khai, vì e rằng ai đó truyền đạt thông tin không chính xác là đúng. Các trang web công khai, các ấn bản báo chí, các tuyên bố của công ty – tất cả đều là những ví dụ về dữ liệu công khai cần phải được bảo vệ, đặc biệt liên quan đến tính toàn vẹn.

## Riêng tư

Dữ liệu được gán nhãn là *riêng tư* nếu sự tiết lộ của nó cho một bên trái phép sẽ có khả năng gây ra thiệt hại hoặc gián đoạn cho tổ chức. Mật khẩu có thể được xem là [dữ liệu] riêng tư. Thuật ngữ *dữ liệu riêng tư* thường được kết hợp với dữ liệu cá nhân thuộc về một cá nhân và ít thường xuyên hơn đối với các thực thể công ty. Mức độ thiệt hại thường liên quan đến dữ liệu riêng tư sẽ thấp hơn mức bảo mật nhưng vẫn là đáng kể đối với tổ chức.

## Nhạy cảm

Dữ liệu *nhạy cảm* là một thuật ngữ chung thường đại diện cho dữ liệu đã được phân loại là bị hạn chế công bố công khai hoặc công bố chung. Thuật ngữ này thường được sử dụng để thay thế cho dữ liệu bí mật.

## Bí mật

Dữ liệu được gán nhãn *bí mật* nếu việc tiết lộ cho một bên trái phép có thể gây ra tổn hại rất nghiêm trọng cho tổ chức. Dữ liệu này nên được xác định theo chính sách và chính sách đó phải bao gồm các chi tiết về người có thẩm quyền phát hành dữ liệu. Các ví dụ phổ biến về dữ liệu tối quan trọng bao gồm dữ liệu về giá cả và chi phí, dữ liệu khách hàng, kế hoạch kinh doanh nội bộ, v.v..., vì việc tiết lộ những dữ liệu này có thể gây ra những tổn thất đáng kể cho công ty.

## Tối quan trọng

Dữ liệu được gán nhãn là *tối quan trọng* nếu việc tiết lộ dữ liệu đó cho một bên trái phép có thể gây ra tổn hại cực kỳ nghiêm trọng cho tổ chức. Dữ liệu này phải được xác định theo chính sách và chính sách đó phải bao gồm các chi tiết về người có thẩm quyền phát hành dữ liệu. Các ví dụ phổ biến về dữ liệu tối quan trọng bao gồm bí mật thương mại, mã nguồn phần mềm độc quyền và thiết kế sản phẩm mới, vì việc tiết lộ những dữ liệu này có thể dẫn đến tổn thất đáng kể cho công ty. Mức độ thiệt hại từ việc tiết lộ dữ liệu tối quan trọng sẽ là cực kỳ nghiêm trọng đối với doanh nghiệp và có thể gây ra mức độ tổn thất cao nhất.



## MÁCH NƯỚC CHO KỲ THI

Sự khác biệt giữa dữ liệu tối quan trọng và bí mật nằm ở mức độ tổn thất tiềm năng nếu như thông tin bị tiết lộ.

## Độc quyền

Dữ liệu *độc quyền* là dữ liệu bị hạn chế đối với một công ty bởi vì khả năng sử dụng cạnh tranh. Nếu như một công ty có những dữ liệu có thể được sử dụng bởi một đối thủ cạnh tranh vì bất kỳ lý do cụ thể nào (ví dụ, dữ liệu về chi phí và định giá nội bộ) thì nó cần được gán nhãn và xử lý theo một cách thức để bảo vệ nó khỏi sự tiết lộ cho các đối thủ cạnh

tranh. Dữ liệu độc quyền có thể được chia sẻ với một bên-thứ-ba không phải là đối thủ cạnh tranh nhưng khi gán nhãn là “độc quyền”, bạn cảnh báo cho bên-thứ-ba mà bạn đã chia sẻ [dữ liệu] rằng nó không được phép chia sẻ thêm.

---



**MÁCH NƯỚC CHO KỲ THI** Hãy tìm hiểu sự khác biệt giữa các nhãn dán dữ liệu nhạy cảm để bạn có thể so sánh và đối chiếu các thuật ngữ *bí mật, riêng tư, công khai* và *độc quyền*. Sự khác biệt tuy là nhỏ nhưng rất quan trọng để xác định đáp án chính xác.

### **Thông tin Định danh Cá nhân (PII)**

Khi thông tin là về một cá nhân thì việc thất bại trong việc bảo vệ nó có thể có những hậu quả đặc biệt. Những bí mật kinh doanh được bảo vệ thông qua các đạo luật bí mật thương mại, những thông tin chính phủ được bảo vệ thông qua các đạo luật liên quan đến an ninh quốc gia, và các đạo luật về quyền riêng tư bảo vệ những thông tin liên quan đến con người. Một tập hợp các phần tử có thể dẫn đến danh tính cụ thể của một người được gọi là *thông tin định danh cá nhân (PII)*. Theo định nghĩa, PII có thể được sử dụng để nhận dạng một cá nhân cụ thể, thậm chí ngay cả khi toàn bộ tập hợp đã không được tiết lộ.

---



**LƯU Ý** Ngay cả những thông tin nhỏ nhặt như mã ZIP, giới tính và ngày sinh cũng có thể xác định một cá nhân cụ thể.

PII là một thành phần tối quan trọng của rất nhiều giao dịch trực tuyến, nhưng nó cũng có thể bị lạm dụng nếu bị tiết lộ cho các bên trái phép. Vì lý do này, nó nên được bảo vệ trong mọi thời điểm, bởi tất cả các bên

đang sở hữu nó. Và khi PII không còn được sử dụng, nó nên được tiêu hủy theo chính sách tiêu hủy dữ liệu của công ty theo cách thức hoàn chỉnh và không thể đảo ngược.



**MÁCH NƯỚC CHO KỲ THI** PII đề cập đến những thông tin có thể được sử dụng để phân biệt hoặc truy nguyên nhân dạng của một cá nhân, một mình nó hoặc khi được kết hợp với những thông tin cá nhân hoặc thông tin nhận dạng khác được liên kết hoặc có thể liên kết với một cá nhân cụ thể.

### Thông tin về Sức khỏe

Các quy định của Đạo luật về Trách nhiệm giải trình và Cung cấp thông tin Bảo hiểm Y tế (Health Insurance Portability and Accountability Act - HIPAA) định nghĩa *thông tin y tế được bảo vệ (protected health information - PHI)* là “bất kỳ thông tin nào, cho dù bằng miệng hay được ghi lại dưới bất kỳ hình thức hoặc phương tiện nào” mà

*“[được] tạo ra hoặc nhận được bởi nhà cung cấp dịch vụ chăm sóc sức khỏe, chương trình sức khỏe, cơ quan y tế công cộng, người sử dụng lao động, công ty bảo hiểm nhân thọ, trường học hoặc trường đại học hoặc cơ quan thanh toán chăm sóc sức khỏe”* và

*“[liên quan] đến sức khỏe hoặc tình trạng thể chất hoặc tinh thần trong quá khứ, hiện tại hoặc tương lai của một cá nhân, cung cấp dịch vụ chăm sóc sức khỏe cho một cá nhân, hoặc khoản thanh toán trong quá khứ, hiện tại hoặc tương lai cho việc cung cấp dịch vụ chăm sóc sức khỏe cho một cá nhân”.*

Ngôn ngữ của HIPAA được xây dựng dựa trên các khái niệm về PHI và Thông báo về Thực tiễn Quyền riêng tư (Notice of Privacy Practices - CompTIA Security+ - All in One - Exam Guide

NPP). HIPAA mô tả “các pháp nhân được bảo hiểm”, bao gồm các cơ sở y tế, cơ sở thanh toán và cơ sở bảo hiểm (người thanh toán bên-thứ-ba). Bệnh nhân phải có quyền truy cập vào PHI của họ và nên có những kỳ vọng về quyền riêng tư và bảo mật thích hợp liên quan đến hồ sơ y tế [của họ]. HIPAA bắt buộc một loạt các biện pháp bảo vệ an ninh về mặt hành chính, kỹ thuật và vật lý đối với thông tin, bao gồm các yếu tố như đào tạo và nâng cao nhận thức của nhân viên cũng như các mức độ bảo vệ cụ thể đối với PHI khi được sử dụng, lưu trữ hoặc truyền tải giữa các cơ sở.



**MÁCH NƯỚC CHO KỲ THI** Hãy tìm hiểu sự khác biệt giữa PII và PHI và đừng chuyển sang đáp án sai trong kỳ thi.

### Thông tin Tài chính

*Thông tin tài chính* là một nguồn chính của PII. Những khoản mục như các tài khoản ngân hàng, các khoản vay nợ, và tổng số tiền thanh toán, tất cả có thể đều được tận dụng để chống lại các hệ thống xác thực dựa-trên-kiến-thức để có được quyền tiếp cận vào nhiều thông tin hơn, chẳng hạn như các báo cáo tín dụng. Thông tin tài chính là một trong số các loại PII được tìm kiếm nhiều nhất bởi vì nó là loại thông tin dễ kiểm tiền nhất.

### Dữ liệu Chính phủ

Chính phủ Hoa Kỳ cũng như các chính phủ khác trên thế giới thu thập những thông tin như một phần hoạt động của mình. Các quy định chính phủ liên quan đến việc thu thập, lưu trữ và sử dụng những dữ liệu chính phủ tồn tại để hỗ trợ cho các cơ quan chính phủ trong việc quản lý một cách thích hợp dữ liệu trong suốt vòng đời của nó trên các hệ thống của

chính phủ. *Dữ liệu chính phủ* có thể bao gồm PII của mọi người, và thông tin này cần phải được bảo vệ theo các quy tắc và quy định hiện hành.

## **Dữ liệu Khách hàng**

*Dữ liệu khách hàng* là nguồn PII chính yếu trong các hệ thống của một doanh nghiệp. Thông tin này đã được thu thập theo các nhu cầu kinh doanh cụ thể, và nó đòi hỏi mức bảo vệ tương ứng để ngăn chặn sự phát tán hoặc tiết lộ.

## **Các Công nghệ Tăng-cường-Quyền-Riêng-tư**

Một mối liên kết chính yếu giữa bảo mật thông tin và quyền riêng tư là nếu không có bảo mật thông tin, bạn không thể có quyền riêng tư. Nếu quyền riêng tư đã được định nghĩa là khả năng kiểm soát thông tin về bản thân một ai đó, thì các khía cạnh về tính bảo mật, tính toàn vẹn và tính sẵn sàng của bảo mật thông tin trở thành các yếu tố tối quan trọng của quyền riêng tư. Cũng giống như công nghệ đã kích hoạt nhiều vấn đề ảnh-hưởng-đến-quyền-riêng-tư, công nghệ cũng đã cung cấp các phương tiện trong nhiều trường hợp để bảo vệ quyền riêng tư. Một ứng dụng hoặc công cụ hỗ trợ cho việc bảo vệ như vậy được gọi là công nghệ tăng-cường-quyền-riêng-tư (PET).

Mã hóa đứng đầu danh sách của PET để bảo vệ quyền riêng tư và tình trạng nặc danh. Một trong những yếu tố thúc đẩy Phil Zimmerman phát minh ra PGP là mong muốn cho phép những người sống đang trong các nền văn hóa hà khắc có thể giao tiếp một cách an toàn và tự do. Mã hóa có thể giữ bí mật bí mật và là một lựa chọn hàng đầu để bảo vệ thông tin tại bất kỳ giai đoạn nào trong vòng đời của nó. Sự phát triển của định tuyến Tor cho phép giao tiếp ẩn danh, cùng với mã hóa chi-phí-thấp, đảm-bảo-cao đã khiến cho nhiều tương tác web được bảo mật và an toàn khỏi bị nghe trộm.

Các PET khác bao gồm các chương trình ứng dụng nhỏ được gọi là trình cắt cookie được thiết kế để ngăn việc truyền cookie giữa các trình duyệt và máy chủ web. Một số công cụ cắt cookie ngăn chặn tất cả cookie, trong khi những công cụ khác có thể được định cấu hình để chặn một số cookie nhất định. Một số công cụ cắt cookie cũng chặn việc gửi tiêu đề HTTP có thể tiết lộ thông tin cá nhân nhưng có thể không cần thiết để truy cập trang web, cũng như chặn quảng cáo biểu ngữ, các cửa sổ bật lên, đồ họa động hoặc các phần tử web không mong muốn khác. Một số công cụ PET liên quan được thiết kế một cách đặc biệt để tìm kiếm các hình ảnh vô hình thiết lập cookie (được gọi là đèn hiệu web hoặc lỗi web). Các PET khác có sẵn cho người dùng máy tính cá nhân, bao gồm các chương trình mã hóa cho phép người dùng mã hóa và bảo vệ dữ liệu của chính họ, ngay cả trên các khóa USB.

### **Tối thiểu Dữ liệu**

*Tối thiểu dữ liệu* là một trong những công nghệ tăng-cường-quyền-riêng-tư mạnh mẽ nhất. Ngắn gọn, nó liên quan đến việc không giữ lại những gì mà bạn không cần. Việc hạn chế sự thu thập thông tin cá nhân đối với những ai có liên quan trực tiếp và cần thiết để thực hiện một mục đích cụ thể vẫn cho phép các giao dịch được thực hiện, nhưng nó cũng làm giảm thiểu rủi ro do vi phạm và tiết lộ trong tương lai bằng cách không giữ lại những dữ liệu "thừa". Tại Liên minh Châu Âu, các quy tắc về quyền riêng tư được xây dựng dựa trên ý tưởng rằng các cá nhân sở hữu quyền sử dụng lại dữ liệu của họ và trừ khi họ cấp nó cho một công ty, quyền lưu trữ và sử dụng lại dữ liệu nằm ngoài giao dịch tức thời bị cấm. Điều này phục vụ cho một số mục đích, nhưng một kết quả quan trọng là khi một sự kiện vi phạm/tiết lộ xảy ra, mức độ tổn thất PII sẽ bị hạn chế.

Mặc dù bạn có thể cần phải có một lượng PII hợp lý để xử lý và giao đơn đặt hàng, nhưng sau khi quá trình đó kết thúc, bạn có còn cần đến dữ

liệu đó không? Có thể cần một khoảng thời gian hợp lý để trả hàng, yêu cầu bảo hành, v.v..., nhưng khi thời hạn đó đã trôi qua, việc tiêu hủy PII không cần thiết sẽ loại bỏ cơ hội [dữ liệu] bị tiết lộ.

### **Che giấu Dữ liệu**

*Che giấu dữ liệu* bao gồm việc ẩn dữ liệu bằng cách thay thế các giá trị đã được thay đổi. Một phiên bản phản chiếu của cơ sở dữ liệu được tạo và các kỹ thuật sửa đổi dữ liệu chẳng hạn như xáo trộn ký tự, mã hóa và thay thế từ hoặc ký tự được áp dụng để thay đổi dữ liệu. Một hình thức khác là chỉnh sửa vật lý các phần tử bằng cách thay thế một ký hiệu như "\*" hoặc "x". Điều này được thấy trên các biên lai thẻ tín dụng, nơi phần lớn các chữ số bị xóa theo cách này. Việc che giấu dữ liệu khiến cho việc phát hiện hoặc thiết kế ngược không thể thực hiện được.



**MÁCH NƯỚC CHO KỲ THI** Che giấu dữ liệu ẩn đi những dữ liệu cá nhân và nhạy cảm nhưng không khiến cho nó [dữ liệu] trở thành không thể sử dụng được.

### **Mã thông báo (Tokenization)**

*Tokenization* là việc sử dụng một giá trị ngẫu nhiên để thay thế cho một phần tử dữ liệu có ý nghĩa có thể truy nguyên. Một ví dụ điển hình về điều này là khi bạn được phê duyệt thẻ tín dụng, bạn không cần phải ghi lại số thẻ, tên chủ thẻ hoặc bất kỳ dữ liệu nhạy cảm nào liên quan đến mã xác minh thẻ (card verification code - CVC) vì tác nhân giao dịch sẽ trả lại một mã phê duyệt, là mã thông báo (token) duy nhất cho giao dịch đó. Bạn có thể lưu trữ mã phê duyệt này - mã thông báo - trong hệ thống của mình và nếu có lúc nào đó bạn cần tham chiếu đến giao dịch ban đầu, mã thông báo sẽ này cung cấp cho bạn khả năng truy xuất nguồn gốc hoàn chỉnh và nếu bị tiết lộ cho bên ngoài, nó sẽ không tiết lộ gì.

Các mã thông báo được sử dụng mọi thời điểm trong các hệ thống truyền dữ liệu liên quan đến thương mại vì chúng bảo vệ thông tin nhạy cảm không bị tái sử dụng hoặc chia sẻ, nhưng chúng vẫn duy trì các đặc tính không khước từ mong muốn của sự kiện. Tokenization không phải là một bước mã hóa vì dữ liệu được mã hóa có thể được giải mã. Bằng cách thay thế một giá trị ngẫu nhiên không liên quan, tokenization sẽ phá vỡ khả năng cho bất kỳ thực thể bên ngoài nào “đảo ngược” hành động vì không có sự kết nối.

---



**MÁCH NƯỚC CHO KỲ THI** Tokenization chỉ định một giá trị ngẫu nhiên có thể đảo ngược hoặc truy nguyên nguồn gốc đến dữ liệu nguyên thủy.

### **Ẩn danh (Anonymization)**

*Ẩn danh hóa dữ liệu* là quá trình bảo vệ những thông tin cá nhân hoặc nhạy cảm bằng cách loại bỏ các yếu tố nhận dạng kết nối dữ liệu đã được lưu trữ với một cá nhân. Việc tách biệt các yếu tố PII như tên, mã số An sinh Xã hội (Social Security number) và địa chỉ ra khỏi phần dữ liệu còn lại thông qua quy trình ẩn danh dữ liệu sẽ giữ lại dữ liệu hữu ích nhưng giữ cho kết nối với nguồn được ẩn danh. Ẩn danh dữ liệu nói thì dễ hơn thực hiện, bởi vì dữ liệu tồn tại ở rất nhiều nơi dưới rất nhiều hình thức. Điều này cho phép các trình tổng hợp dữ liệu thu thập rất nhiều trường hợp và sau đó, thông qua các thuật toán và đối sánh mẫu, hủy-ẩn-danh dữ liệu thông qua nhiều tham-chiếu-chéo so với nhiều nguồn.

### **Giả Ẩn danh (Pseudo-Anonymization)**

*Giả-ẩn-danh* là một phương pháp khử-nhân-dạng(de-identification) thay thế các yếu tố nhận dạng riêng tư bằng các yếu tố nhận dạng hoặc biệt hiệu giả (ví dụ: thay thế giá trị của từ định danh tên “Mark Sands” bằng

"John Doe"). Không phải tất cả các trường nhận dạng duy nhất đều bị thay đổi bởi vì một số trường, chẳng hạn như ngày sinh, có thể cần phải được giữ nguyên để duy trì tính chính xác của thống kê. Tín hiệu gây nhiễu có thể được thêm vào một số trường để loại bỏ các kết nối trực tiếp, nhưng vẫn duy trì giá trị gần đúng, ví dụ, cộng hoặc trừ ngẫu nhiên ba ngày thêm/bớt vào ngày sinh thực tế sẽ giữ nguyên tuổi nhưng khử-nhân-dạng từ hồ sơ gốc. Thuật ngữ giả danh duy trì tính chính xác thống kê và tính toàn vẹn của dữ liệu, cho phép dữ liệu đã sửa đổi được sử dụng để đào tạo, phát triển, thử nghiệm và phân tích trong khi vẫn bảo vệ được quyền riêng tư của dữ liệu.



**MÁCH NƯỚC CHO KỲ THI** Hãy chắc chắn rằng bạn có thể xác định được những công nghệ tăng-cường-quyền-riêng-tư khác nhau. Hãy hiểu được những gì chúng thực hiện và cách mà chúng được triển khai như thế nào.

### Vai trò và Trách nhiệm

Rất nhiều nhân viên trong một tổ chức được liên kết với các biện pháp kiểm soát và quản trị hành chính của dữ liệu. Những *vai trò dữ liệu* này bao gồm chủ sở hữu dữ liệu, người kiểm soát dữ liệu, người xử lý dữ liệu, người bảo quản/bảo vệ dữ liệu và người dùng. Từng vai trò trong số này đều chịu trách nhiệm cho việc bảo vệ và kiểm soát dữ liệu. Lãnh đạo của nỗ lực này được đặt dưới sự bảo trợ của chuyên viên về quyền riêng tư dữ liệu.

### Chủ Sở hữu Dữ liệu

Tất cả những thành phần dữ liệu trong một tổ chức nên có những yêu cầu được xác định đối với tính bảo mật, quyền riêng tư, lưu giữ, và các

chức năng nghiệp vụ khác. Đây là trách nhiệm của *chủ sở hữu dữ liệu* đã được chỉ định để xác định những yêu cầu này.

### **Người Kiểm soát Dữ liệu**

*Người kiểm soát dữ liệu* là cá nhân chịu trách nhiệm cho việc quản lý cách thức và lý do tại sao dữ liệu sẽ được sử dụng bởi tổ chức. Trong kỵ nguyên của GDPR và các đạo luật và quy định về quyền riêng tư khác, đây là một vị trí tối quan trọng bởi vì, theo GDPR và các đạo luật về quyền riêng tư khác, người kiểm soát dữ liệu là vị trí chịu trách nhiệm cho việc bảo vệ quyền riêng tư và những quyền hạn của chủ thể của dữ liệu, chẳng hạn như người dùng của một trang web. Bất kể dữ liệu là dữ liệu chính hay dữ liệu từ bên-thứ-ba, người kiểm soát dữ liệu vẫn có trách nhiệm cho việc chỉ định cách thức dữ liệu sẽ được sử dụng và xử lý cả bên trong nội bộ lẫn bên ngoài tổ chức. Có thể có rất nhiều người kiểm soát dữ liệu trong một tổ chức, chịu trách nhiệm cho các bộ dữ liệu khác nhau.



**MÁCH NƯỚC CHO KỲ THI** Tại Liên minh Châu Âu (EU), Quy định Bảo vệ Dữ liệu Chung (GDPR) phân loại người kiểm soát dữ liệu là người quản lý dữ liệu (data manager). Nói cách khác, người kiểm soát dữ liệu sẽ quản lý dữ liệu.

Đối với những dữ liệu liên quan đến quyền riêng tư, theo hầu hết các quy định về quyền riêng tư và GDPR, người kiểm soát dữ liệu chịu trách nhiệm cho việc quyết định những điều sau đây:

- Dữ liệu nào sẽ được thu thập
- Dữ liệu được sử dụng ở đâu và như thế nào
- Dữ liệu được chia sẻ với ai và như thế nào

- Dữ liệu được giữ trong bao lâu và nó sẽ được tiêu hủy như thế nào khi kết thúc vòng đời (end of life – EOL).

### **Người Xử lý Dữ liệu**

*Người xử lý dữ liệu* là thực thể đang xử lý dữ liệu được cung cấp bởi người kiểm soát dữ liệu. Người xử lý dữ liệu không sở hữu dữ liệu cũng như không kiểm soát dữ liệu đó. Vai trò của họ là thao tác dữ liệu như một phần của các quy trình nghiệp vụ. Người xử lý dữ liệu có thể là nhân viên hoặc các hệ thống, một ví dụ về hệ thống là việc sử dụng Google Analytics để thao tác các phần tử nhất định của dữ liệu, khiến cho chúng trở nên hữu ích đối với các chuyên gia phân tích nghiệp vụ.

Đối với dữ liệu có liên quan đến quyền riêng tư, theo hầu hết các quy định về quyền riêng tư và GDPR, người xử lý dữ liệu chịu trách nhiệm về những điều sau đây:

- Phát triển và triển khai các quy trình và hệ thống CNTT để quản lý dữ liệu cá nhân
- Triển khai các biện pháp bảo mật để bảo vệ dữ liệu cá nhân
- Sử dụng các công cụ và chiến lược để xử lý dữ liệu cá nhân một cách đúng đắn.

### **Người Bảo quản/Bảo vệ Dữ liệu**

*Một người bảo quản dữ liệu* hoặc *người bảo vệ dữ liệu* là vài trò chịu trách nhiệm cho việc chăm sóc dữ liệu hàng ngày. Chủ sở hữu dữ liệu xác lập nên các chính sách có liên quan, và người bảo vệ hoặc bảo quản đảm bảo rằng chúng [các chính sách] được tuân thủ.

### **Chuyên gia về Quyền Riêng tư Dữ liệu (DPO)**

*Chuyên gia về quyền riêng tư dữ liệu (DPO)* là nhân sự điều hành cấp độ-C, người chịu trách nhiệm cho việc thiết lập và củng cố chính sách quyền riêng tư dữ liệu và giải quyết các vấn đề pháp lý và tuân thủ đối

với quyền riêng tư dữ liệu. Các sáng kiến tối thiểu dữ liệu cũng là trách nhiệm của chuyên gia về quyền riêng tư dữ liệu. Việc lưu trữ những dữ liệu không có bất kỳ giá trị kinh doanh thực tế nào chỉ làm gia tăng tỷ lệ của việc tiết lộ. Chuyên gia về quyền riêng tư dữ liệu chịu trách nhiệm cho việc xác định khoảng cách giữa những thực tiễn về quyền riêng tư của một công ty và các hành động bắt buộc để thu hẹp khoảng cách đó đến mức đã được phê duyệt. Việc này được gọi là phân tích tác động đến quyền riêng tư.

Chuyên gia về quyền riêng tư dữ liệu cũng đóng một vai trò quan trọng nếu như những thông tin về khách hàng người châu Âu có liên quan vì Liên minh Châu Âu có các quy định nghiêm ngặt về bảo vệ dữ liệu (quyền riêng tư). Chuyên gia về quyền riêng tư chịu trách nhiệm giải trình cho sự bảo vệ dữ liệu người tiêu dùng từ Liên minh Châu Âu phải đảm bảo tuân thủ các quy định của Liên minh Châu Âu.



## MÁCH NƯỚC CHO KỲ THI

Chuyên gia về quyền riêng tư dữ liệu chịu trách nhiệm cho việc đảm bảo sự tuân thủ về mặt pháp lý đối với các quy định về quyền riêng tư dữ liệu.

### Vòng đời của Thông tin

Thông tin có một vòng đời – một khởi đầu, ở giữa và tại một số thời điểm, kết thúc. Việc hiểu được vòng đời của tài sản thông tin - từ thời điểm thu thập, sử dụng và lưu trữ cũng như cách thức tài sản được chia sẻ, bảo vệ và cuối cùng là tiêu hủy - là điều quan trọng nếu bạn muốn xử lý thông tin một cách đúng đắn. Không phải tất cả thông tin đều có cùng khoảng thời gian, hoặc thậm chí ngay cả các bước, được liên kết với nó, vì vậy các vòng đời là duy nhất cho các nguồn và phần tử

thông tin khác nhau. Vòng đời hình thành nền nếp tảng cho việc quản lý thông tin.

### **Đánh giá Tác động**

Một *đánh giá tác động quyền riêng tư* (*privacy impact assessment – PIA*) là một phương pháp tiếp cận có cấu trúc để xác định những khoảng cách giữa hoạt động quyền riêng tư mong muốn và hoạt động quyền riêng tư trong thực tế. Một PIA là một quá trình phân tích về cách mà PII được xử lý thông qua các quy trình nghiệp vụ và là một quá trình đánh giá về những rủi ro đối với PII trong suốt quá trình lưu trữ, sử dụng và truyền thông. Một PIA cung cấp một phương tiện để đánh giá tính hiệu quả của quy trình liên quan đến các yêu cầu tuân thủ và để xác định những vấn đề cần phải được giải quyết. Một PIA được cơ cấu với một loạt các bước để đảm bảo một đánh giá toàn diện về các điều kiện đối với quyền riêng tư.



### **MÁCH NƯỚC CHO KỲ THI**

Các tổ chức thu thập, sử dụng hoặc xử lý những thông tin cá nhân được yêu cầu phải tiến hành một đánh giá tác động quyền riêng tư.

Các bước dưới đây cấu thành nên một phương pháp luận và phương pháp tiếp cận cao-cấp để tiến hành một PIA:

1. *Xác lập phạm vi của PIA*. Xác định các bộ phận liên quan và những đại diện thích hợp. Xác định những ứng dụng và quy trình nghiệp vụ nào cần được đánh giá. Xác định những đạo luật và quy định có thể áp dụng tương ứng với các mối quan tâm của doanh nghiệp và mối quan tâm về quyền riêng tư.

2. Nhận diện các bên liên quan. Nhận diện tất cả các đơn vị kinh doanh đang sử dụng PII. Kiểm tra các chức năng nhân sự như Nhân sự, Pháp chế, CNTT, Mua hàng, và Kiểm soát Chất lượng.
3. Lập thành tài liệu tất cả liên hệ với PII:
  - Việc thu thập, đánh giá, sử dụng, chia sẻ và tiêu hủy PII
  - Các quy trình và thủ tục, chính sách, bảo vệ, các sơ đồ luồng-dữ-liệu, và bất kỳ dữ liệu đánh giá rủi ro nào khác
  - Các chính sách trang web, hợp đồng Nhân sự và quản lý hành chính đối với PII khác.
4. Xem xét các yêu cầu pháp lý và quy định, bao gồm bất kỳ hợp đồng thương nguồn (upstream contract) nào. Có rất nhiều nguồn, nhưng một số vẫn đề thường hay bị bỏ qua là các thỏa thuận với các nhà cung cấp và khách hàng về quyền hạn chia-sẻ-thông-tin.
5. Lập thành tài liệu những khoảng cách và vấn đề tiềm ẩn giữa các yêu cầu và thực tiễn. Tất cả những khoảng cách và vấn đề nên được ánh xạ so với nơi mà vấn đề đã được khám phá và cơ sở (yêu cầu hoặc quy định) mà khoảng cách đang ánh xạ đến.
6. Xem xét những phát hiện cùng với các bên liên quan để xác định tính chính xác và làm rõ bất kỳ vấn đề nào. Trước khi báo cáo sau cùng được viết ra, bất kỳ vấn đề hoặc thông tin sai lệch nào đều nên được làm rõ với các bên liên quan thích hợp để đảm bảo một báo cáo công bằng và chính xác.
7. Tạo ra báo cáo sau cùng cho cấp quản lý.

### Các Điều khoản Thỏa thuận

Mô tả pháp lý về các điều khoản thỏa thuận (thường được gọi là các điều khoản và điều kiện) là một tập hợp các hạng mục mà cả hai bên đã đồng ý trước một số hoạt động chung. Điều này được sử dụng trong mọi thời điểm với bất kỳ tương tác bên ngoài nào, nơi bạn yêu cầu bên phản hồi đồng ý với tài liệu thỏa thuận điều khoản đã được lập trước khi cấp cho

họ quyền truy cập hoặc xử lý các phần tử dữ liệu của họ. Một văn bản thỏa thuận điều khoản điển hình bao gồm các điều khoản, quy tắc, hướng dẫn về hành vi có thể được chấp nhận và các phần hữu ích khác mà người dùng phải đồng ý để sử dụng hoặc truy cập vào tài nguyên CNTT, chẳng hạn như trang web, ứng dụng dành cho thiết bị di động, trang đặt hàng, v.v.... Các hạng mục quan trọng trong tài liệu văn bản thỏa thuận bao gồm các điều khoản pháp lý, luật điều chỉnh, thỏa thuận đối với các quy tắc hoạt động, những dịch vụ nào được cung cấp và theo những điều kiện kinh doanh nào, nghĩa vụ pháp lý, các biện pháp khắc phục những bất đồng (ví dụ: trọng tài) và các điều khoản kinh doanh như quyền hủy bỏ, bồi hoàn, thỏa thuận mức dịch vụ, v.v.... Điều này trở thành giấy phép ràng buộc các bên với các điều khoản mà doanh nghiệp muốn thực thi.

### **Thông báo Quyền Riêng tư**

Một *thông báo quyền riêng tư* là một tuyên bố hướng ra bên ngoài mô tả cách thức tổ chức thu thập, sử dụng, lưu giữ và công bố thông tin cá nhân như thế nào. Thông báo về quyền riêng tư cũng được coi là một tuyên bố về quyền riêng tư hoặc một tuyên bố xử lý công bằng. Các thông báo đặc biệt về quyền riêng tư cũng được bắt buộc bởi các luật về quyền riêng tư cụ thể, và một ví dụ phổ biến về những thông báo đó là tuyên bố công bố về cookie được thấy trên các trang web có sử dụng cookie. Các thành phần phổ biến của một thông báo về quyền riêng tư bao gồm:

- Khi bạn thu thập thông tin cá nhân
- Lý do tại sao bạn thu thập thông tin cá nhân
- Thông tin nào sẽ được thu thập
- Thông tin sẽ được bảo vệ như thế nào
- Khi nào thì thông tin có thể hoặc sẽ được chia sẻ
- Ai là người để liên hệ và nơi những thắc mắc nên được định hướng liên quan đến thông báo

- Cách thức để chọn không tham gia hoặc tham gia
- Ngày có hiệu lực của tài liệu

Một ví dụ về thông báo cookie web sẽ là, "Chúng tôi đang sử dụng cookie để cung cấp các dịch vụ trực tuyến của chúng tôi. Các chi tiết về cookie và các công nghệ theo dõi khác mà chúng tôi đang sử dụng và hướng dẫn về cách vô hiệu hóa chúng được nêu trong Chính sách Cookie của chúng tôi. Bằng cách sử dụng trang web này, bạn đồng ý với việc sử dụng cookie của chúng tôi".

---



## **MÁCH NƯỚC CHO KỲ THI**

Khái niệm then chốt cần lưu ý là rằng một chính sách về quyền riêng tư được tập trung vào nội bộ, cho nhân viên biết rằng những gì họ có thể thực hiện với những thông tin cá nhân, trong khi một thông báo về quyền riêng tư lại hướng ra bên ngoài, cho khách hàng, cơ quan quản lý và các bên liên quan khác biết được tổ chức đang làm gì với những thông tin cá nhân.

## Tóm tắt Chương

Chương này bắt đầu bằng việc giải thích các khái niệm về quyền riêng tư và dữ liệu nhạy cảm có liên quan đến bảo mật. Phần đầu tiên mở đầu bằng việc xem xét những hậu quả của tổ chức do vi phạm quyền riêng tư, bao gồm thiệt hại về danh tiếng, trộm cắp danh tính, tiền phạt và hành vi trộm cắp tài sản trí tuệ. Tiếp theo là cuộc thảo luận về các yêu cầu thông báo xung quanh các vi phạm, bao gồm cả việc leo thang. Phần này đã kết thúc với các chủ đề về yêu cầu công bố và thông báo công khai.

Chủ đề chính tiếp theo được thảo luận là các loại dữ liệu, được chia thành hai phần phụ: phân loại và thông tin nhận dạng cá nhân (PII). Theo phân loại dữ liệu, các chủ đề [dữ liệu] công khai, riêng tư, nhạy cảm, bí mật, tối quan trọng và độc quyền đã được trình bày. Trong PII, các chủ đề về thông tin sức khỏe, thông tin tài chính, dữ liệu chính phủ và dữ liệu khách hàng đã được đề cập đến.

Các công nghệ tăng-cường-quyền-riêng-tư đã được trình bày, bao gồm tối thiểu dữ liệu, ẩn dữ liệu, mã thông báo, ẩn danh và giả-ẩn-danh. Chương này sau đó chuyển sang vai trò và trách nhiệm của các nỗ lực về quyền riêng tư của dữ liệu. Trong phần này, nhiệm vụ của chủ sở hữu dữ liệu, người kiểm soát dữ liệu, người xử lý dữ liệu, người bảo quản/bảo vệ dữ liệu và chuyên gia về quyền riêng tư dữ liệu đã được xác định và giải thích.

Chương này kết thúc bằng việc kiểm tra các chủ đề về vòng đời của thông tin, đánh giá tác động, các điều khoản thỏa thuận và thông báo về quyền riêng tư.

## Câu hỏi

Để giúp bạn chuẩn bị thêm cho kỳ thi CompTIA Security+, và để kiểm tra mức độ chuẩn bị của bạn, hãy trả lời những câu hỏi dưới đây và sau đó kiểm tra đáp án của bạn so với những câu trả lời chính xác ở cuối mỗi chương.

- 1. Điều gì dưới đây không phải là PII?**
  - A. Tên khách hàng**
  - B. Mã số ID (nhân dạng) của khách hàng**
  - C. Số An sinh Xã hội của khách hàng hoặc mã định danh người nộp thuế**
  - D. Ngày sinh của khách hàng.**
- 2. Đánh giá tác động quyền riêng tư sẽ thực hiện điều gì?**
  - A. Nó xác định khoảng cách giữa những thực tiễn về quyền riêng tư của một công ty và những hành động cần thiết.**
  - B. Nó xác định tổn thất gây ra bởi một vi phạm quyền riêng tư.**
  - C. Nó xác định những gì công ty nắm giữ những thông tin về một cá nhân cụ thể.**
  - D. Nó là một thủ tục phối hợp để bảo vệ PII.**
- 3. Quyền riêng tư là gì?**
  - A. Khả năng kiểm soát thông tin về bản thân một người nào đó**
  - B. Có khả năng giữ bí mật thông tin của một ai đó**
  - C. Khiến cho việc chia-sẻ-dữ-liệu trở nên bất hợp pháp mà không có sự chấp thuận của người dùng**
  - D. Thứ gì đó đã lỗi thời trong thời đại Internet.**
- 4. Ai chịu trách nhiệm cho việc xác định những dữ liệu nào là cần thiết bởi doanh nghiệp?**
  - A. Người bảo vệ dữ liệu**
  - B. Chuyên gia về quyền riêng tư dữ liệu**
  - C. Người bảo quản dữ liệu**

- D.** Chủ sở hữu dữ liệu.
- 5.** Dữ liệu đã được gán nhãn là “riêng tư” thường thích hợp với thể loại nào?
- A.** Dữ liệu độc quyền
  - B.** Thông tin bí mật
  - C.** Thông tin pháp lý
  - D.** Thông tin cá nhân.
- 6.** Dữ liệu đã được gán nhãn là “độc quyền” thường thích hợp với thể loại nào?
- A.** Thông tin được lưu giữ hợp pháp
  - B.** Thông tin cần phải được bảo vệ bởi các đối tác kinh doanh vì nó chứa những bí mật kinh doanh
  - C.** Dữ liệu cá nhân
  - D.** PHI cùng với PII.
- 7.** Thông tin có thể tiết lộ nhân dạng của một khách hàng được gọi là gì?
- A.** Thông tin nhân dạng khách hàng (CII)
  - B.** Thông tin nhân dạng cá nhân (PII)
  - C.** Thông tin được bảo vệ quyền riêng tư (PPI)
  - D.** Thông tin nhạy cảm về khách hàng (SCI)
- 8.** Những gì sau đây không phải là công nghệ tăng-cường-quyền-riêng-tư?
- A.** Tối thiểu dữ liệu
  - B.**Ẩn giấu dữ liệu
  - C.** Tiết lộ dữ liệu
  - D.** Mã thông báo.
- 9.** Thuật ngữ nào thông báo cho khách hàng về chính sách quyền riêng tư của bạn và tác động của nó đến những thông tin của họ [khách hàng]?

- A. Phân tích tác động**
  - B. Thông báo công khai về sự tiết lộ**
  - C. Thông báo quyền riêng tư**
  - D. Các điều khoản thỏa thuận.**
- 10.** Điều nào dưới đây là rất quan trọng để đảm bảo các mối quan tâm về phát hành quyền riêng tư được xử lý một cách đúng đắn khi được khám phá ra bởi một đội ứng phó sự cố?
- A. Leo thang**
  - B. Phân tích tác động quyền riêng tư**
  - C. Các công nghệ tăng-cường-quyền-riêng-tư**
  - D. Thông báo và tiết lộ công khai.**

## Đáp án

1. **B.** Một mã định danh khách hàng được tạo ra bởi một công ty để theo dõi một hồ sơ khách hàng chỉ có ý nghĩa khi ở trong công ty và nói chung không được xem là thông tin định danh cá nhân (PII). Hãy lưu ý rằng điều quan trọng là không sử dụng mã số An sinh Xã hội cho việc này, vì những lý do hiển nhiên.
2. **A.** Một đánh giá tác động quyền riêng tư (PIA) xác định khoảng cách giữa những gì mà một công ty đang thực hiện với PII và những gì mà các chính sách, quy tắc và quy định của công ty nêu rõ những gì họ nên thực hiện.
3. **A.** Mặc dù tất cả các câu trả lời khả dĩ đều chứa các yếu tố của sự thật đối với chúng, nhưng quyền riêng tư là kiểm soát thông tin của một người, không chỉ là tích trữ thông tin đó.
4. **D.** Chủ sở hữu dữ liệu xác định nhu cầu của doanh nghiệp. Chuyên gia về quyền riêng tư đảm bảo rằng các luật lệ và quy định được tuân theo và người bảo quản/bảo vệ sẽ duy trì dữ liệu.
5. **D.** Dữ liệu cá nhân (private) thường đề cập đến dữ liệu thuộc về một cá nhân nào đó (personal).
6. **B.** Dữ liệu độc quyền có thể được chia sẻ với bên thứ ba không phải là đối thủ cạnh tranh, nhưng khi đã gán nhãn dữ liệu là "độc quyền", bạn cảnh báo cho bên mà bạn đã chia sẻ rằng dữ liệu không được chia sẻ thêm nữa.
7. **B.** Bất kỳ thông tin nào có thể được sử dụng để xác định danh tính đều được gọi chung là thông tin nhận dạng cá nhân (PII).
8. **C.** Tiết lộ dữ liệu không phải là công nghệ tăng-cường-quyền-riêng-tư, chúng là hậu quả của việc kẻ tấn công có quyền truy cập vào dữ liệu nhạy cảm trên một hệ thống.

9. **C.** Thông báo quyền riêng tư là phương tiện được sử dụng để thông báo cho khách hàng về những ảnh hưởng của chính sách bảo mật của một công ty đối với dữ liệu của họ (khách hàng).
10. **A.** Leo thang là điều quan trọng để đảm bảo rằng các nhóm thích hợp đang ứng phó với một sự cố liên-quan-đến-quyền-riêng-tư.

## Phần VI

### Phụ lục và Chú giải thuật ngữ

- Phụ lục A Mô hình OSI và các Giao thức Internet
- Phụ lục B Về Nội dung Trực tuyến
- Chú giải thuật ngữ

## Phụ lục A Mô hình OSI và các Giao thức Internet

### Mô hình OSI và các Giao thức Internet

Trong phụ lục này, bạn sẽ:

- Tìm hiểu về mô hình OSI,
- Xem xét các giao thức mạng tương ứng với Internet.

Các hệ thống mạng là các nhóm bao gồm nhiều máy tính và những phần cứng đặc biệt kết nối với nhau được thiết kế để tạo điều kiện cho sự truyền tải dữ liệu từ thiết bị này sang thiết bị khác. Chức năng cơ bản của hệ thống mạng là để cho phép máy móc và thiết bị giao tiếp với nhau một cách có trật tự.

### Các Khuôn khổ và Giao thức Kết nối mạng

Mạng ngày nay cấu thành từ nhiều loại và kích cỡ thiết bị từ rất nhiều nhà cung cấp khác nhau. Để đảm bảo việc truyền tải thông tin hiệu quả và hiệu quả giữa các thiết bị, thỏa thuận về cách thức truyền tải giữa các nhà cung cấp là điều cần thiết.

Thuật ngữ *giao thức* đề cập đến một bộ các quy tắc tiêu chuẩn được phát triển để tạo điều kiện cho một mức chức năng cụ thể. Trong việc kết nối mạng, một loạt các giao thức đã được phát triển - một số giao thức độc quyền và một số công khai - để tạo điều kiện giao tiếp giữa các máy. Cũng giống như người nói cần một ngôn ngữ chung để giao tiếp hoặc ít nhất phải hiểu ngôn ngữ của nhau, máy tính và mạng phải thống nhất về một giao thức chung.

Giao tiếp đòi hỏi tất cả các bên đều phải có sự hiểu biết chung về đối tượng đang được thảo luận. Nếu đối tượng là vô hình hoặc không hiện

diện, mỗi bên cần một số phương pháp tham chiếu các đề mục theo cách thức mà bên kia hiểu được. *Mô hình* là một công cụ được sử dụng như một khuôn khổ để cung cấp cho mọi người những điểm tham chiếu chung khi thảo luận về các đề mục. Các mô hình toán học rất phổ biến trong khoa học, vì chúng cung cấp cho mọi người khả năng so sánh các câu trả lời và kết quả. Theo cách tương tự, các mô hình được sử dụng trong rất nhiều lĩnh vực để tạo điều kiện giao tiếp. Các mô hình mạng đã được phát triển bởi rất nhiều công ty như một cách để giao tiếp giữa các kỹ sư về chức năng cụ thể đang diễn ra khi nào và ở đâu trong hệ thống mạng.

Khi Internet hình thành, một loạt các giao thức là cần thiết để đảm bảo khả năng tương tác qua lại trên toàn bộ cấu trúc mạng chung này. Giao thức Kiểm soát Truyền tải (TCP), Giao thức Dữ liệu Người dùng (UDP) và Giao thức Internet (IP) là ba trong số các giao thức được sử dụng phổ biến cho phép truyền tải dữ liệu trên Internet. Vì các giao thức này hoạt động phối hợp với nhau, bạn thường thấy TCP/IP hoặc UDP/IP là các cặp giao thức được sử dụng. Một hiểu biết cơ bản về các thuật ngữ và cách sử dụng các giao thức và mô hình là điều cần thiết để thảo luận về chức năng kết nối mạng vì nó cung cấp các điểm tham chiếu cần thiết để hiểu điều gì đang xảy ra ở đâu và khi nào trong dòng hoạt động phức tạp có liên quan đến kết nối mạng.

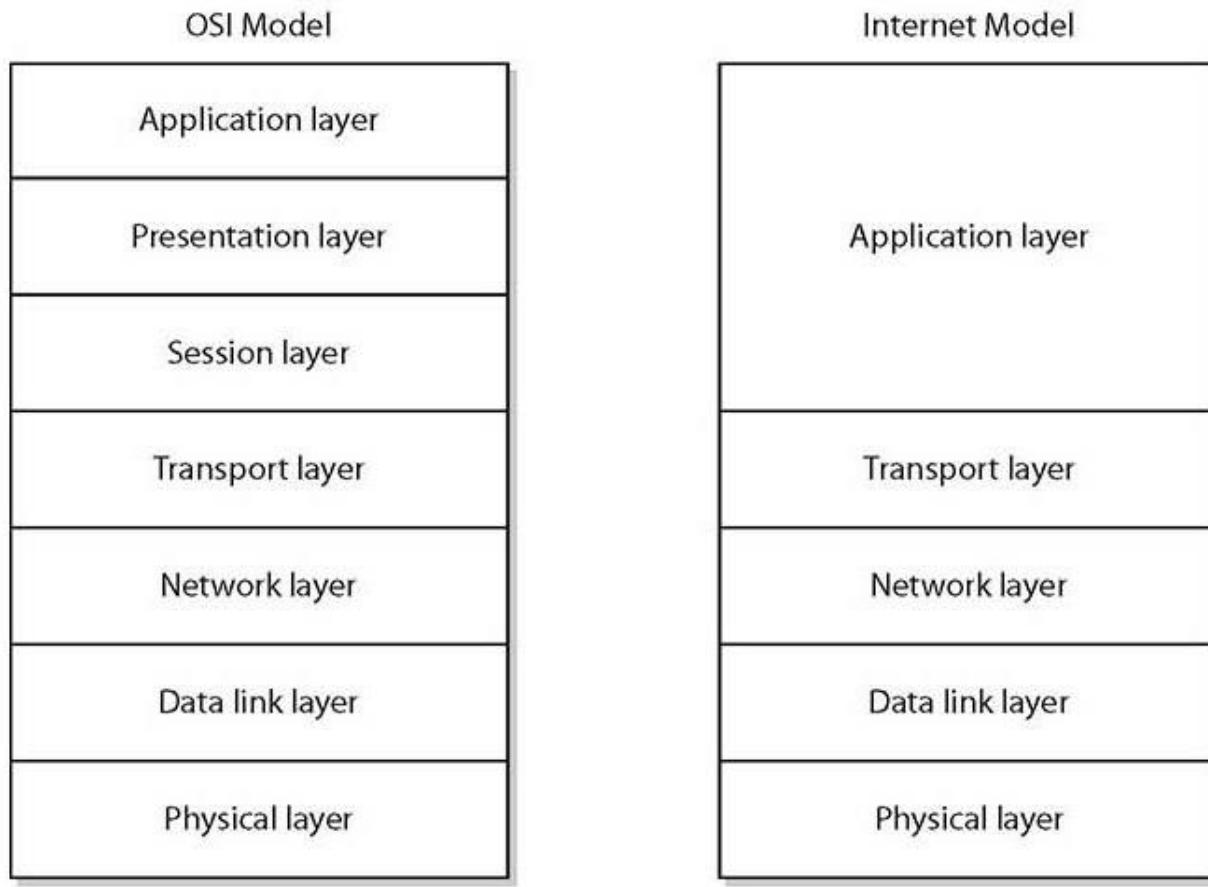
## **Mô hình OSI**

Để tạo điều kiện giao tiếp giữa-các-nhà-cung-cấp và đa công ty, vào năm 1984, Tổ chức Tiêu chuẩn hóa Quốc tế (ISO) đã tạo ra mô hình Kết nối Hệ thống Mở (OSI) cho mạng. Mô hình OSI có lẽ là mô hình được tham chiếu và thảo luận rộng rãi nhất trong kết nối mạng. Mặc dù nó chưa bao giờ được hiểu đầy đủ ở Bắc Mỹ nhưng các phần của nó đã được chấp nhận làm điểm tham chiếu, thậm chí đến mức được kết hợp vào tên công ty. Lớp 2, lớp 3, lớp mạng, mức 3 - đây là tất cả các tham chiếu đến các

phần của mô hình OSI. Những tham chiếu này cho phép mọi người giao tiếp theo một cách rõ ràng và không mơ hồ khi nói về các vấn đề trừu tượng và nằm-ngoài-ngữ-cảnh. Những tài liệu tham chiếu này cung cấp ngữ cảnh đến từng chi tiết trong lĩnh vực phức tạp về kết nối mạng. Các thuật ngữ *cấp độ (level)* và *lớp (layer)* đã được sử dụng thay thế cho nhau để mô tả các phần của mô hình OSI, mặc dù lớp là thuật ngữ phổ biến hơn.

Mô hình OSI bao gồm bảy lớp được xếp chồng theo kiểu tuyến tính. Các lớp này là, từ trên xuống dưới, ứng dụng (application), trình diễn (presentation), phiên (session), truyền tải (transport), mạng (network), liên kết dữ liệu (data link) và vật lý (physical). Bạn có thể sử dụng một cách ghi nhớ để ghi nhớ chúng [các lớp]: Tất cả Mọi người Có vẻ Cần Xử lý Dữ liệu (All People Seem To Need Data Processing). Mỗi lớp có chức năng đã được xác định và sự tách biệt được thiết kế để cho phép nhiều giao thức hoạt động cùng nhau theo một cách được phối hợp.

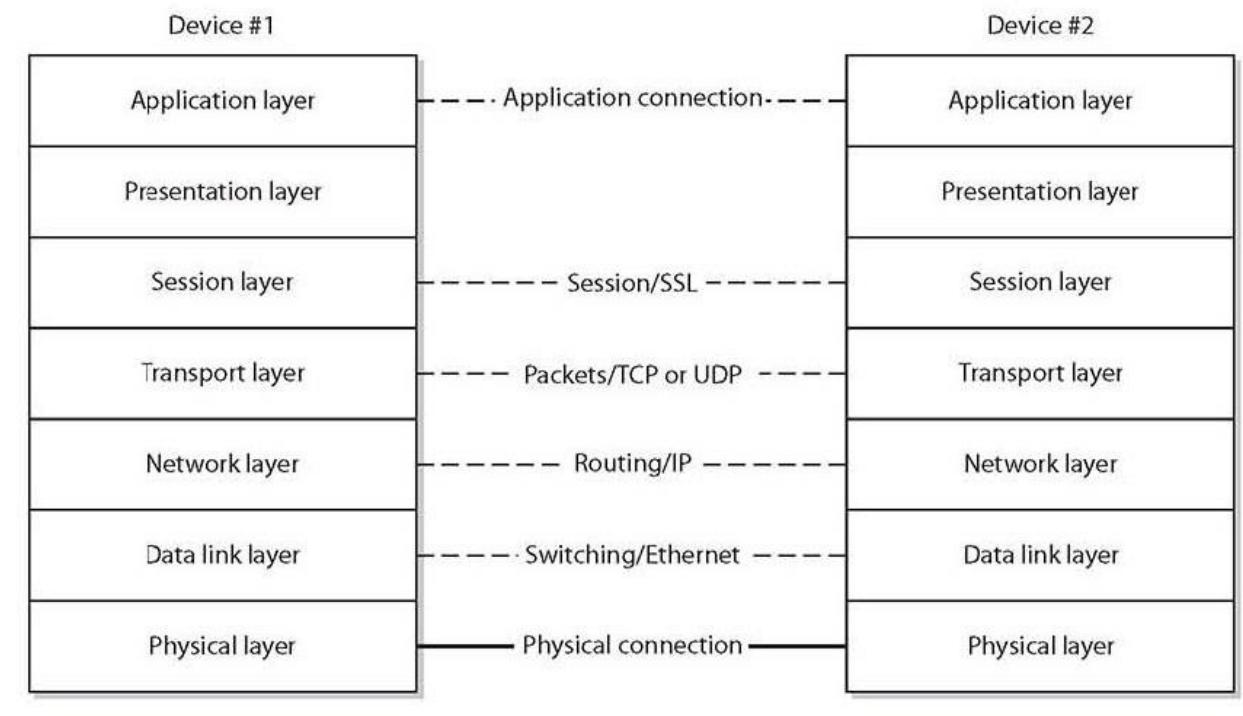
Mặc dù mô hình OSI có lẽ là mô hình mạng tiêu chuẩn và được tham chiếu nhiều nhất, nhưng một mô hình phổ biến hơn - mô hình Internet - đã vươn lên thống trị Internet. Mô hình OSI có vị thế là một tiêu chuẩn quốc tế chính thức và được xác định, trong khi mô hình Internet chưa bao giờ được định nghĩa một cách chính thức. Mô hình Internet về cơ bản giống với mô hình OSI, với ba lớp OSI trên cùng được kết hợp thành một lớp ứng dụng duy nhất, để lại tổng cộng năm lớp trong mô hình Internet. Cả hai mô hình được thể hiện trong Hình A-1.



**Hình A-1** Các mô hình mạng OSI và Internet

Một khía cạnh của các mô hình này là chúng cho phép các mức chức năng cụ thể được chia nhỏ và thực hiện theo trình tự. Sự phân định này cũng xác định những lớp nào có thể giao tiếp với những lớp khác. Tại mỗi lớp, các biểu mẫu và giao thức dữ liệu cụ thể có thể tồn tại, khiến cho chúng tương thích với các giao thức và biểu mẫu dữ liệu tương tự trên các máy khác tại cùng một lớp. Điều này làm cho nó có vẻ như mỗi lớp đang giao tiếp với đối tác của nó trên cùng một lớp trong một máy tính khác, mặc dù đây chỉ là một kết nối ảo. Kết nối thực sự duy nhất giữa các hộp là ở lớp vật lý của các mô hình này. Tất cả các kết nối khác đều là ảo - mặc dù chúng có vẻ là thật đối với người dùng, nhưng chúng không thực sự tồn tại trong thực tế.

Giao tiếp thực sự giữa các lớp xảy ra theo chiều dọc, lên và xuống - mỗi lớp chỉ có thể giao tiếp với người hàng xóm trực tiếp của nó ở bên trên và bên dưới. Trong Hình A-2, một đường dẫn truyền thông tin trực tiếp được thể hiện như một đường kẻ đậm giữa hai lớp vật lý. Tất cả dữ liệu giữa các hộp đi qua đường này. Các đường đứt nét giữa các lớp cao hơn đại diện cho các kết nối ảo, các hoạt động và giao thức liên quan cũng được liệt kê đối với hầu hết các lớp (các giao thức cũng được liệt kê trong Bảng A-1). Những đường đứt nét này là ảo - dữ liệu không thực sự đi qua chúng, mặc dù nó xuất hiện như thể dữ liệu thực sự đi qua nó. Đường dẫn thực của dữ liệu đi xuống lớp vật lý và sao lưu vào cùng lớp trên một máy khác.



**Hình A-2** Các đường dẫn giao tiếp của mô hình mạng

Lớp	Các Giao thức Được sử dụng Phổ biến
Ứng dụng	HTTP(S), SNMP, SMTP, FTP(S), Telnet, SSH, DNS
Trình diễn	XDR, SSL, TLS, IMAP, SSH
Phiên	NetBIOS, RTP, PPTP
Truyền tải	TCP, UDP, SCTP
Mạng	IP, IPSec, ICMP, IGMP, RIP, OSPF
Liên kết dữ liệu	IEEE 802.3 (Ethernet), IEEE 802.5 (Token Ring), ARP, RARP, PPP, SLIP
Vật lý	Phần cứng IEEE 802.3 (Ethernet), phần cứng IEEE 802.5 (Token Ring), USB, Bluetooth, IEEE 802.11

**Bảng A-1** Các Giao thức phổ biến theo Lớp OSI

### **Lớp Ứng dụng (Application Layer)**

Lớp ứng dụng là giao diện điển hình của ứng dụng thực tế đang được sử dụng. Đây là lớp của ngăn xếp giao tiếp thường chịu trách nhiệm khởi tạo nên yêu cầu giao tiếp. Ví dụ, các trình duyệt là các chương trình ứng dụng hoạt động trong lớp ứng dụng sử dụng [giao thức] HTTP để di chuyển dữ liệu giữa các hệ thống. Lớp này đại diện cho quyền truy cập của người dùng vào hệ thống và mạng. Mặc dù có vẻ như ứng dụng đang giao tiếp trực tiếp với một ứng dụng trên máy khác, nhưng đây thực chất là một kết nối ảo. Lớp ứng dụng đôi khi cũng được gọi là lớp 7 trong mô hình OSI. Một số giao thức thường được tìm thấy trong lớp ứng dụng, bao gồm Giao thức Truyền tải Siêu văn bản (Hypertext Transfer Protocol - HTTPS), Giao thức Truyền Thư Đơn giản (Simple Mail Transfer Protocol

- SMTP) và Giao thức Quản lý Mạng Đơn giản (Simple Network Management Protocol - SNMP).

Trong mô hình OSI, lớp ứng dụng thực sự chỉ giao tiếp với lớp trình diễn trên máy tính của chính nó. Trong mô hình Internet, mức ngay bên dưới lớp ứng dụng là lớp truyền tải và đây là lớp duy nhất được gọi trực tiếp bởi lớp ứng dụng trong mô hình này. Do các lớp trình diễn và phiên “bị thiếu” trong mô hình Internet, chức năng của các lớp OSI này được thực hiện bởi lớp ứng dụng.

Chức năng lớp phiên hiện diện trong lớp ứng dụng của mô hình Internet bao gồm việc khởi tạo, duy trì và kết thúc các phiên logic giữa các điểm đầu cuối trong giao tiếp mạng. Chức năng lớp phiên cũng bao gồm các dịch vụ kế toán và mã hóa cấp-phiên. Chức năng lớp trình diễn của mô hình OSI cũng được bao gồm trong lớp ứng dụng của mô hình Internet, cụ thể là chức năng định dạng các tham số hiển thị của dữ liệu đang được nhận. Bất kỳ chức năng nào khác không được bao gồm cụ thể trong các lớp dưới của mô hình Internet đều được bao gồm một cách cụ thể trong lớp ứng dụng.

### **Lớp Trình diễn (Presentation Layer)**

Lớp trình diễn có tên gọi của nó từ chức năng chủ yếu của nó: chuẩn bị trình bày dữ liệu. Lớp này chịu trách nhiệm cho việc chuẩn bị dữ liệu cho các tương tác khác nhau trên các kiểu thiết bị đầu cuối hoặc thiết bị hiển thị khác nhau để lớp ứng dụng không phải xử lý nhiệm vụ này. Nén dữ liệu, diễn giải bộ ký tự, và mã hóa được tìm thấy ở lớp này.

Lớp trình diễn chỉ giao tiếp với hai lớp khác – lớp ứng dụng bên trên nó và lớp phiên bên dưới nó. Lớp trình diễn còn được gọi là lớp 6 của mô hình OSI.

## Lớp Phiên (Session Layer)

Trách nhiệm chính của lớp phiên là quản lý các phiên giao tiếp giữa các máy. Các chức năng quản lý bao gồm khởi đầu, duy trì và kết thúc phiên. Việc quản lý một phiên có thể được so sánh với việc thực hiện một cuộc gọi điện thoại thông thường. Khi bạn quay số, bạn khởi đầu một phiên. Phiên phải được duy trì ở trạng thái mở trong suốt cuộc gọi. Khi kết thúc cuộc gọi, bạn cúp máy và mạch phải được ngắt. Vì mỗi phiên có thể có các tham số riêng nên lớp phiên chịu trách nhiệm thiết lập chúng, bao gồm bảo mật, mã hóa và các chức năng thanh toán hoặc kế toán.

Lớp phiên giao tiếp độc quyền với lớp trình diễn bên trên nó và lớp truyền tải bên dưới nó. Lớp phiên còn được gọi là lớp 5 của mô hình OSI.

## Lớp Truyền tải (Transport Layer)

Tầng truyền tải chịu trách nhiệm xử lý việc truyền tải dữ liệu từ đầu đến cuối đi qua kết nối mạng. Để thực hiện nhiệm vụ này, lớp truyền tải xử lý dữ liệu vào và ra khỏi mạng thông qua các kết nối luân lý. Nó có thể bổ sung thêm và sử dụng thông tin địa-chỉ-cụ-thể, chẳng hạn như các cổng, để hoàn thành nhiệm vụ này. *Cổng* là một phần mở rộng địa-chỉ-cụ-thể cho phép thực hiện nhiều giao tiếp đồng thời giữa các máy tính. Nếu việc truyền tải dữ liệu quá lớn đối với việc truyền tải một gói-đơn-lẻ, lớp truyền tải sẽ quản lý việc chia nhỏ luồng dữ liệu thành nhiều phần và sau đó tổng hợp lại. Nó đảm bảo rằng tất cả các gói đã được truyền đi và được nhận, đồng thời nó có thể yêu cầu [truyền lại] các gói bị mất và loại bỏ các gói trùng lặp. Việc kiểm tra lỗi cũng có thể được thực hiện ở mức này, mặc dù chức năng này thường được thực hiện ở lớp liên kết dữ liệu.

Các giao thức có thể là định hướng kết nối hoặc không có kết nối. Nếu giao thức được định hướng kết nối, lớp truyền tải quản lý thông tin kết

nối. Trong trường hợp TCP, lớp truyền tải quản lý các yêu cầu truyền lại gói bị thiếu thông qua thuật toán cửa sổ trượt.

Lớp truyền tải giao tiếp độc quyền với lớp phiên bên trên nó và lớp mạng bên dưới nó. Lớp truyền tải còn được gọi là lớp 4 của mô hình OSI.

### **Lớp Mạng (Network Layer)**

Lớp mạng chịu trách nhiệm cho việc định tuyến các gói tin đi qua mạng. Các chức năng định tuyến xác định đích đến tốt nhất kế tiếp đối với một gói tin và sẽ xác định địa chỉ đầy đủ của máy tính đích nếu cần thiết. Các giao thức phổ biến tại mức này bao gồm IP và Giao thức Kiểm soát Thông điệp Internet (ICMP).

Lớp mạng giao tiếp độc quyền với lớp truyền tải bên trên nó và lớp liên kết dữ liệu bên dưới nó. Lớp mạng còn được gọi là lớp 3 của mô hình OSI.

### **Lớp Liên kết dữ liệu (Data link Layer)**

Lớp liên kết dữ liệu chịu trách nhiệm cho việc chuyển giao và nhận dữ liệu từ phần cứng trong lớp 1, lớp vật lý. Lớp 1 chỉ thao tác với một luồng các bit, do đó lớp liên kết dữ liệu phải chuyển đổi các gói tin từ lớp mạng thành các luồng bit dưới dạng có thể được hiểu bởi lớp vật lý. Để đảm bảo truyền tải chính xác, lớp liên kết dữ liệu bổ sung thêm các điểm đánh dấu kết-thúc-thông-điệp vào mỗi gói tin và đồng thời quản lý các chức năng phát hiện lỗi, sửa lỗi và truyền tải lại. Lớp này cũng thực hiện chức năng truy-cập-phương-tiện, xác định thời điểm gửi và nhận dữ liệu dựa trên lưu lượng mạng. Tại lớp này, về mặt kỹ thuật, các gói dữ liệu được gọi là các *khung* (frame), mặc dù rất nhiều người hành nghề sử dụng *gói* (packet) theo nghĩa chung.

Lớp liên kết dữ liệu giao tiếp độc quyền với lớp mạng bên trên nó và lớp vật lý bên dưới nó. Lớp liên kết dữ liệu cũng được gọi là lớp 2 của mô

hình OSI, và đây là nơi việc chuyển mạch mạng LAN (LAN switching) dựa trên địa-chỉ-máy diễn ra.

## Lớp Vật lý (Physical Layer)

Lớp vật lý là lĩnh vực về giao tiếp phần cứng và phần mềm, nơi [các bit] 1 và 0 trở thành sóng ánh sáng, các mức điện áp, chuyển pha và các thực thể vật lý khác như đã được xác định bởi tiêu chuẩn truyền dẫn cụ thể. Lớp này xác định phương thức truyền tín hiệu vật lý giữa các máy xét về mặt các đặc tính điện và quang học. Lớp vật lý là điểm kết nối với thế giới bên ngoài thông qua các bộ kết nối tiêu chuẩn, một lần nữa được xác định bởi loại tín hiệu và giao thức.

Lớp vật lý giao tiếp với lớp vật lý trên các máy khác thông qua dây cáp, sợi quang học hoặc sóng vô tuyến. Lớp vật lý cũng giao tiếp với lớp liên kết dữ liệu bên trên nó. Lớp vật lý còn được gọi là lớp 1 của [mô hình] OSI.

## Các Giao thức Internet

Để tạo điều kiện cho giao tiếp giữa các sản phẩm của nhiều-nhà-cung-cấp, các giao thức đã được áp dụng cho các phương pháp tiêu chuẩn. Internet đã bổ sung thêm một số giao thức mới, và một vài trong số đó được sử dụng phổ biến trong việc định tuyến thông tin. Hai giao thức được sử dụng tại lớp truyền tải là TCP và UDP, trong khi IP được sử dụng tại lớp mạng. Trong từng phiên, một giao thức lớp truyền tải và một giao thức lớp mạng được sử dụng, tạo thành các cặp [giao thức] TCP/IP và UDP/IP.

### TCP

Giao thức Kiểm soát Truyền tải (Transmission Control Protocol – TCP) là giao thức truyền tải chủ yếu được sử dụng trên Internet ngày nay, chiếm đến hơn 80% số lượng gói tin trên Internet.

TCP khởi đầu bằng cách thiết lập một kết nối ảo thông qua một cơ chế được gọi là *bắt tay* TCP. Quá trình bắt tay này liên quan đến 3 tín hiệu: một tín hiệu SYN được gửi đến đích đến, một tín hiệu SYN/ACK được trả về để phản hồi và sau đó một ACK được gửi trở lại mục tiêu để hoàn thành mạch [kết nối]. Điều này thiết lập một kết nối ảo giữa các máy mà dữ liệu sẽ được truyền qua đó, và đó là lý do tại sao TCP được gọi là *định hướng kết nối* (*connection oriented*).

TCP được phân loại là một giao thức đáng tin cậy và sẽ đảm bảo rằng các gói được gửi, nhận và sắp xếp theo trình tự bằng cách sử dụng số thứ tự. Một số chi phí tương ứng với trình tự sắp xếp các gói và duy trì trình tự này, nhưng đối với rất nhiều giao tiếp, điều này là cần thiết, chẳng hạn như trong truyền tải email, HTTP, và những thứ tương tự.

TCP có các phương tiện để thực hiện hoàn thành các chức năng cần thiết của lớp truyền tải. TCP có các cơ chế kiểm-soát-luồng và kiểm-soát-tắc-nghẽn để báo cáo về sự tắc nghẽn và các thông tin liên-quan-đến-lưu-lượng khác trở lại người gửi để giúp quản-lý-mức-lưu-lượng. Nhiều kết nối TCP có thể được thiết lập giữa các máy thông qua một cơ chế được gọi là *các cổng*. Các cổng TCP được đánh số từ 0 đến 65,535, mặc dù các cổng thấp hơn 1024 thường được dành riêng cho các chức năng cụ thể. Các cổng TCP là các thực thể tách biệt với cổng UDP và có thể được sử dụng cùng một lúc.

## **UDP**

Giao thức Sơ đồ dữ liệu Người dùng (User Datagram Protocol – UDP) là một hình thức đơn giản hơn của giao thức truyền tải so với TCP. UDP thực hiện mọi chức năng cần thiết của lớp truyền tải, nhưng nó không thực hiện các chức năng duy trì và kiểm tra của TCP. UDP không thiết lập một kết nối và không sử dụng các số thứ tự. Các gói tin UDP được gửi đi thông qua phương pháp “nỗ lực tốt nhất”, thường được gọi là “cháy và

quên (fire and forget)", bởi vì các gói tin hoặc là đến được đích đến của chúng hoặc chúng sẽ mất đi mãi mãi. Nó không cung cấp cơ chế truyền lại, và đó là lý do tại sao UDP được gọi là một giao thức không đáng tin cậy.

UDP không có các chức năng quản-lý-lưu-lượng hay quản-lý-luồng như TCP. Điều này dẫn đến việc chi phí thấp hơn và khiến cho UDP lý tưởng hơn đối với việc phát trực tuyến các luồng dữ liệu, chẳng hạn như lưu lượng âm thanh và hình ảnh, khi độ trễ giữa các gói tin có thể là một vấn đề. Các dịch vụ thiết yếu như Giao thức Cấu hình Máy chủ Động (DHCP) và Dịch vụ Tên Miền (DNS) sử dụng UDP, chủ yếu bởi vì chi phí thấp. Khi các gói tin bị mất – điều hiếm hoi trong các mạng hiện đại – chúng có thể được truyền lại.

Nhiều kết nối UDP có thể được thiết lập giữa các máy thông qua các cổng. Các cổng UDP được đánh số từ 0 đến 65,535, mặc dù các cổng dưới 1024 thường được dành riêng cho các chức năng cụ thể. Các cổng UDP là các thực thể riêng biệt với các cổng TCP và có thể được sử dụng cùng một lúc.

## IP

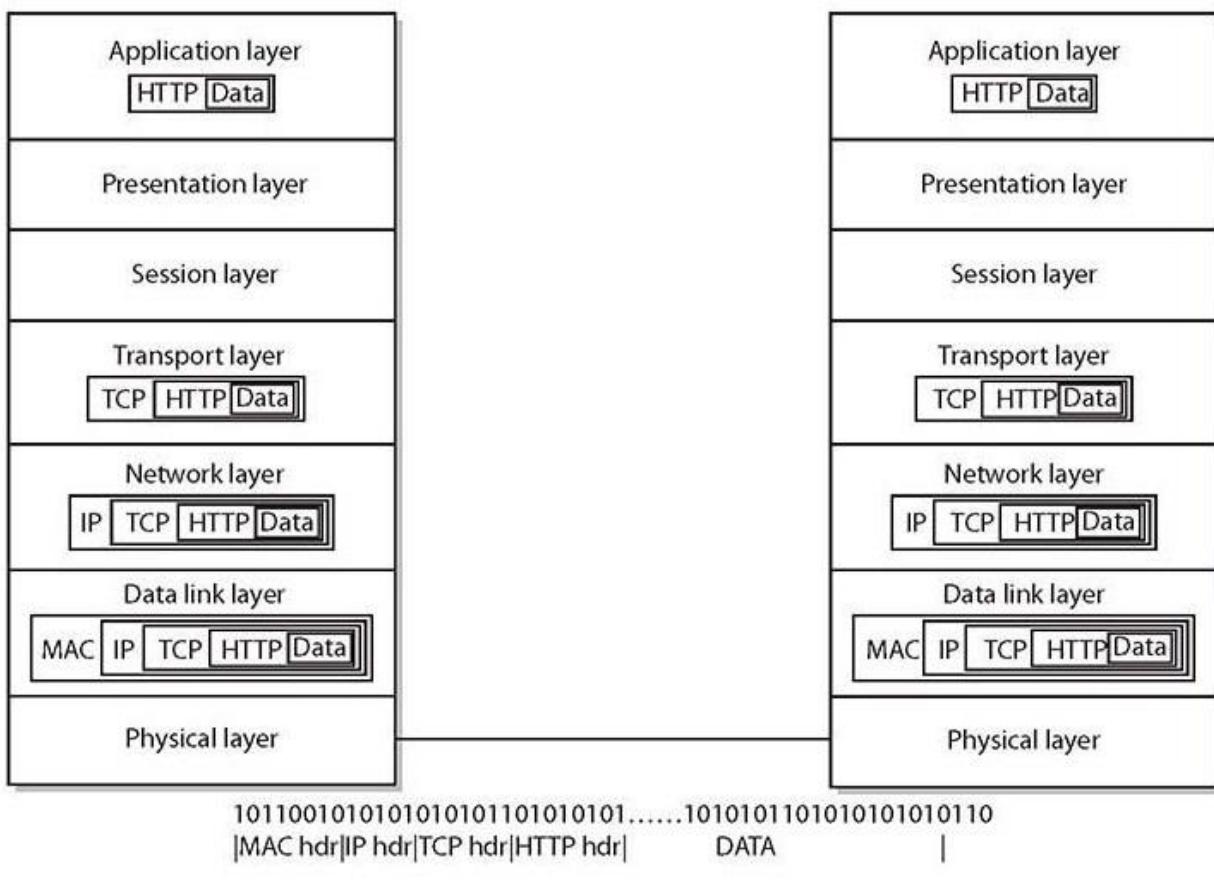
Giao thức Internet (IP) là một giao thức không kết nối (connectionless) được sử dụng để định tuyến thông điệp trên Internet. Mục đích chính của nó là đánh địa chỉ các gói tin bằng các địa chỉ IP, cả địa chỉ đích lẫn địa chỉ nguồn, và sử dụng các địa chỉ này để xác định bước tiếp theo mà gói tin sẽ được truyền đi. Vì IP là *không kết nối*, các gói tin IP có thể đi theo các tuyến đường khác nhau tại các thời điểm khác nhau giữa các máy chủ giống nhau, tùy thuộc vào điều kiện giao thông. IP cũng duy trì một số thông tin quản-lý-lưu-lượng, chẳng hạn như thời-gian-tồn-tại (time-to-live) (một chức năng cung cấp cho các gói tin một thời gian tồn tại bị

giới hạn) và kiểm soát phân mảnh (một cơ chế để chia nhỏ các gói trên tuyến đường, nếu cần).

Phiên bản hiện tại của IP là phiên bản 4, còn được gọi là IPv4 và sử dụng không gian địa chỉ 32 bit. Giao thức IPv6 mới hơn bổ sung thêm các cấp độ chức năng quan trọng, chẳng hạn như bảo mật, không gian địa chỉ được mở rộng lên 128 bit và một loạt các tùy chọn quản-lý-lưu-lượng phức tạp. Địa chỉ IPv4 được viết dưới dạng bốn bộ số ở dạng v.x.y.z, với mỗi giá trị này nằm trong khoảng từ 0 đến 255. Vì điều này sẽ rất khó nhớ nên một hệ thống đặt tên cho máy chủ đã được phát triển xung quanh các miền, và máy chủ DNS chuyển đổi tên máy chủ, chẳng hạn như www.ietf.org, thành các địa chỉ IP, chẳng hạn như 4.17.168.6.

## **Đóng gói Thông điệp**

Khi một thông điệp truyền qua mạng từ một ứng dụng trên một máy vật chủ, đi xuống qua mô hình OSI, đi ra ngoài qua lớp vật lý và đi lên mô hình OSI của máy khác, dữ liệu được đóng gói ở mỗi lớp. Đây có thể được xem như là một lược đồ phong-bì-trong-một-phong-bì. Vì chỉ những phong bì cụ thể được xử lý ở mỗi lớp nên chỉ có những thông tin cần thiết cho lớp đó mới được thể hiện trên phong bì. Tại mỗi lớp, thông tin bên trong phong bì không có liên quan và các phong bì trước đó đã bị loại bỏ - chỉ có thông tin trên phong bì hiện tại được sử dụng. Điều này giúp phân tách chức năng hiệu quả giữa các lớp. Khái niệm này được minh họa trong Hình A-3.



**Hình A-3** Đóng gói thông điệp OSI

Khi một thông điệp truyền qua mô hình OSI từ lớp ứng dụng đến lớp vật lý, các phong bì được đặt bên trong các phong bì lớn hơn. Điều này làm gia tăng kích thước của gói tin, nhưng sự gia tăng này được biết đến và tính đến bởi các giao thức cấp-cao-hơn. Ở mỗi cấp, một tiêu đề được bổ sung thêm vào giao diện người dùng (front-end) và nó hoạt động để đóng gói lớp trước đó dưới dạng dữ liệu. Ở mức vật lý, các bit được chuyển thành tín hiệu vật lý và được truyền đến trạm tiếp theo.

Tại trạm nhận, các bit được chuyển thành một gói tin lớn, đại diện cho khái niệm phong-bì-trong-một-phong-bì ban đầu. Sau đó, mỗi phong bì được xử lý ở một mức độ thích hợp. Sự đóng gói này tồn tại ở lớp truyền tải và thấp hơn, vì đây là lĩnh vực của một gói tin gói trong một phiên.

## **Chỉ định Cổng Phổ biến**

Có một tập hợp các chỉ định gán cổng TCP và UDP phổ biến (xem Bảng A-2) cần được cam kết đưa vào bộ nhớ dành cho kỳ thi. Một số cổng trong số này phục vụ cho nhiều dịch vụ, ví dụ: tất cả các giao thức bảo mật SSH đều đi qua cổng TCP 22. Các giao thức bảo mật SSL/TLS sử dụng nhiều cổng TCP, khác nhau đối với từng giao thức liên quan. Hãy lưu ý rằng tất cả các giao thức được bảo mật đều sử dụng TCP, vì quá trình bắt tay và sắp xếp gói tin là điều thiết yếu đối với các giao thức đã được mã hóa.

TCP Port Number	UDP Port Number	Keyword	Protocol
20		FTP-Data	File Transfer (Default Data)
21		FTP	File Transfer Control
22		SSH	Secure Shell Login
22		SCP	SCP uses SSH
22		SFTP	SFTP uses SSH
23		TELNET	Telnet
25		SMTP	Simple Mail Transfer
53	53	DNS	Domain Name Server
80		HTTP	Web
110		POP3	E-mail
139		NetBIOS	NetBIOS
143		IMAP	E-mail
161		SNMP	SNMP
162		SNMP	SNMP
443		HTTPS	HTTPS
465		Encrypted SMTP	SMTP over SSL/TLS
636		LDAPS	LDAPS
989		FTPS	FTPS
990		FTPS	FTPS
993		Secure IMAP	Secure IMAP over SSL/TLS
995		Secure POP3	Secure POP3 over SSL/TLS
3269		LDAPS	LDAPS
3389	3389	RDP	Remote Desktop Protocol

**Bảng A-3** Chỉ định Cổng TCP/UDP Phổ biến

### Đánh giá

Để giúp các hệ thống khác nhau hiểu được chức năng được thực hiện trong giao tiếp mạng, một khuôn khổ chung là điều cần thiết. Khuôn khổ này được cung cấp bởi các mô hình OSI và mô hình mạng Internet, vốn chỉ định những chức năng nào xảy ra, theo trình tự như thế nào, trong

việc truyền tải dữ liệu từ một ứng dụng sang một ứng dụng khác trên một hệ thống mạng.

Sự hiểu biết về mô hình OSI và từ đó, về trạng thái mà theo đó, dữ liệu tồn tại khi nó truyền qua mạng cho phép hiểu sâu hơn về các vấn đề liên quan đến bảo mật. Việc hiểu được rằng SSL xuất hiện trước TCP và IP cho phép bạn hiểu cách thức SSL bảo vệ TCP và IP khỏi sự dòm ngó từ bên ngoài như thế nào. Việc hiểu các giao thức khác nhau và điều gì xảy ra với việc mất dữ liệu sẽ giúp bạn hiểu rõ hơn về cách thức một số loại tấn công nhất định được thực hiện như thế nào.

Bản chất của một khuôn khổ là cho phép nâng cao hiểu biết về các mối quan hệ và các mô hình mạng này thực hiện chức năng này cho các chuyên gia về hệ thống mạng.

## **Phụ lục B      Nói về Nội dung Trực tuyến**

Quyển sách này đi kèm với phần mềm thực hành luyện thi có thể tùy chỉnh TotalTesterOnline với 250 đề thi thực hành.

### **Yêu cầu Hệ thống**

Các phiên bản chính hiện tại và trước đây của các trình duyệt máy tính để bàn sau đây được khuyến nghị và được hỗ trợ: Chrome, Microsoft Edge, Firefox và Safari. Các trình duyệt này cập nhật thường xuyên và đôi khi bản cập nhật có thể gây ra sự cố tương thích với TotalTester Online hoặc nội dung khác được lưu trữ trên Trung tâm Đào tạo. Nếu bạn gặp sự cố khi sử dụng một trong các trình duyệt này, vui lòng thử sử dụng trình duyệt khác cho đến khi sự cố được giải quyết.

### **Tài khoản trên Trung tâm Đào tạo Hội thảo Tổng của bạn**

Để truy cập vào nội dung trực tuyến, bạn sẽ cần phải tạo một tài khoản trên Trung tâm Đào tạo Hội Thảo Tổng (Total Seminars Training Hub). Việc đăng ký hoàn toàn miễn phí, và bạn sẽ có thể theo dõi tất cả những nội dung trực tuyến của bạn bằng cách sử dụng tài khoản của mình. Bạn cũng có thể chọn tham gia vào nếu bạn muốn nhận những thông tin tiếp thị từ McGraw Hill hoặc Total Seminars, nhưng điều này là không bắt buộc để bạn có quyền truy cập vào nội dung trực tuyến.

### **Thông báo Quyền riêng tư**

McGraw Hill tôn trọng quyền riêng tư của bạn. Hãy đảm bảo rằng bạn đã đọc Thông báo về Quyền riêng tư có sẵn trong quá trình đăng ký để xem xét cách thức mà thông tin bạn đã cung cấp sẽ được sử dụng như thế nào. Bạn có thể xem xét Chính sách Bảo mật Khách hàng Doanh nghiệp (Corporate Customer Privacy Policy) của chúng tôi bằng cách truy cập Trung tâm Bảo mật McGraw Hill. Hãy truy cập trang mheducation.com và nhấp vào mục Quyền riêng tư ở cuối trang.

## **Điều khoản và Điều kiện của Giấy phép Người dùng Đơn**

Quyền truy cập trực tuyến vào nội dung kỹ thuật số đi kèm với quyển sách này được điều chỉnh bởi Thỏa thuận Cấp phép McGraw Hill được nêu dưới đây. Bằng cách sử dụng nội dung kỹ thuật số này, bạn đồng ý với các điều khoản của giấy phép đó.

**Truy cập** Để đăng ký và kích hoạt tài khoản Total Seminars Training Hub của bạn, chỉ cần làm theo các bước đơn giản sau.

1. Truy cập URL: hub.totalsem.com/mheclaim
2. Để đăng ký và tạo một tài khoản Trung tâm Đào tạo mới, hãy nhập địa chỉ email, tên và mật khẩu của bạn vào tab **Đăng ký**. Không cần bổ sung thêm thông tin cá nhân (chẳng hạn như số thẻ tín dụng) để tạo tài khoản. Nếu bạn đã có tài khoản Total Seminars Training Hub, hãy nhập địa chỉ email và mật khẩu của bạn vào tab **Đăng nhập**.
3. Nhập Khóa sản phẩm của bạn: pkf0-0b2x-747g
4. Nhấp để chấp nhận các điều khoản cấp phép người dùng.
5. Đối với người dùng mới, hãy nhấp vào nút **Đăng ký và Xác nhận** để tạo tài khoản của bạn. Đối với người dùng hiện tại, hãy nhấp vào nút **Đăng nhập và Xác nhận**.

Bạn sẽ được đưa đến Trung tâm đào tạo và có quyền truy cập vào nội dung cho quyển sách này.

**Thời hạn của Giấy phép** Quyền truy cập vào nội dung trực tuyến của bạn thông qua Trung tâm Đào tạo Hội thảo Tổng sẽ hết hạn sau một năm kể từ ngày nhà xuất bản tuyên bố cuốn sách không còn bản in.

Việc bạn mua sản phẩm McGraw Hill này, bao gồm cả mã truy cập của nó, thông qua một cửa hàng bán lẻ phải tuân theo chính sách hoàn tiền của cửa hàng đó.

Nội dung là tác phẩm có bản quyền của McGraw Hill và McGraw Hill bảo lưu mọi quyền trong và đối với Nội dung. Tác phẩm là © 2021 bởi McGraw Hill.

**Giới hạn chuyển giao** Người dùng chỉ nhận được quyền hạn chế để sử dụng Nội dung cho mục đích sử dụng nội bộ và cá nhân của chính người dùng, tùy thuộc vào việc mua và tiếp tục sở hữu quyền sách này. Người dùng không được sao chép, chuyển tiếp, sửa đổi, tạo các tác phẩm phái sinh dựa trên, truyền tải, phân phối, phổ biến, bán, xuất bản hoặc cấp phép lại cho Nội dung hoặc theo bất kỳ cách nào để trộn lẫn Nội dung với nội dung của bên-thứ-ba khác mà không có sự đồng ý của McGraw Hill.

**Bảo hành có Giới hạn** Nội dung McGraw Hill được cung cấp trên cơ sở "nguyên trạng". Cả McGraw Hill và người cấp phép của McGraw Hill đều không đưa ra bất kỳ bảo đảm hoặc bảo hành nào dưới bất kỳ hình thức nào, dù rõ ràng hay ngụ ý, bao gồm, nhưng không giới hạn, bảo đảm ngụ ý về khả năng bán được hoặc tính phù hợp cho một mục đích cụ thể hoặc việc sử dụng đối với bất kỳ Nội dung McGraw Hill nào hoặc thông tin trong đó hoặc bất kỳ bảo đảm nào về tính chính xác, đầy đủ, đúng đắn hoặc kết quả thu được từ, truy cập vào hoặc sử dụng Nội dung McGraw Hill, hoặc bất kỳ tài liệu nào được đề cập đến trong Nội dung đó hoặc bất kỳ thông tin nào được người dùng hoặc người khác và/hoặc bất kỳ tài liệu nào đưa vào sản phẩm của bên được cấp phép có sẵn trên hoặc có thể được truy cập thông qua sản phẩm của bên được cấp phép (bao gồm thông qua bất kỳ siêu liên kết nào hoặc hình thức nào khác) hoặc không-vi-phạm quyền của bên-thứ-ba. Mọi bảo đảm dưới bất kỳ hình thức nào, dù rõ ràng hay ngụ ý, đều bị từ chối. Bất kỳ tài liệu hoặc dữ liệu nào thu được thông qua việc sử dụng Nội dung McGraw Hill là tùy theo quyết định và rủi ro của riêng bạn và người dùng hiểu rằng họ sẽ tự chịu trách nhiệm

về bất kỳ thiệt hại nào gây ra cho hệ thống máy tính của mình hoặc mất mát dữ liệu.

McGraw Hill hoặc người cấp phép của McGraw Hill sẽ không chịu trách nhiệm pháp lý đối với bất kỳ người đăng ký nào hoặc bất kỳ người dùng nào hoặc bất kỳ ai khác về bất kỳ sự không chính xác, chậm trễ, gián đoạn dịch vụ, lỗi hoặc thiếu sót, bất kể nguyên nhân hoặc bất kỳ thiệt hại nào gây ra từ đó.

Trong mọi trường hợp, McGraw Hill hoặc người cấp phép của McGraw Hill sẽ không chịu trách nhiệm pháp lý đối với bất kỳ thiệt hại gián tiếp, đặc biệt hoặc tổn thất do hậu quả nào, bao gồm nhưng không giới hạn, mất thời gian, mất tiền, mất lợi nhuận hoặc thiện chí, cho dù theo hợp đồng, vi phạm, trách nhiệm pháp lý nghiêm ngặt hoặc cách nào khác, và cho dù những thiệt hại đó có thể thấy trước hay không lường trước được đối với bất kỳ việc sử dụng Nội dung McGraw Hill nào.

## **TotalTester Online**

TotalTester Online cung cấp cho bạn một mô phỏng của kỳ thi CompTIA Security+. Các bài kiểm tra có thể được thực hiện trong Chế độ Thực hành hoặc Chế độ Kiểm tra. Chế độ Thực hành cung cấp một cửa sổ hỗ trợ với các gợi ý, tài liệu tham khảo đến quyển sách, giải thích về các câu trả lời đúng và sai, và tùy chọn để kiểm tra câu trả lời của bạn khi bạn làm bài kiểm tra. Chế độ Kiểm tra cung cấp một mô phỏng của kỳ thi thực tế. Số lượng câu hỏi, loại câu hỏi và thời gian cho phép nhằm thể hiện chính xác môi trường thi. Tùy chọn để tùy chỉnh bài kiểm tra của bạn cho phép bạn tạo ra các bài kiểm tra tùy chỉnh từ các lĩnh vực hoặc chương đã chọn và bạn có thể tùy chỉnh bổ sung thêm số lượng câu hỏi và thời gian cho phép.

Để làm bài kiểm tra, hãy làm theo hướng dẫn được cung cấp trong phần trước để đăng ký và kích hoạt tài khoản Trung tâm Đào tạo Hội thảo Tổng của bạn. Khi bạn đăng ký, bạn sẽ được đưa đến Trung tâm Đào tạo Hội thảo Tổng. Từ Trang chủ của Trung tâm Đào tạo, chọn **CompTIA Security+ All-in-One Exam Guide, 6e (SY0-601)** từ trình đơn thả-xuống Study ở đầu trang hoặc từ danh sách Chủ đề của bạn trên Trang chủ. Sau đó, bạn có thể chọn tùy chọn để tùy chỉnh bài kiểm tra của mình và bắt đầu tự kiểm tra ở Chế độ Thực hành hoặc Chế độ Kiểm tra. Tất cả các bài kiểm tra đều cung cấp điểm tổng thể và điểm được chia nhỏ theo lĩnh vực.

## Hỗ trợ Kỹ thuật

Với những thắc mắc liên quan đến TotalTester hoặc hoạt động của Trung tâm Đào tạo, hãy ghé thăm trang [www.totalsem.com](http://www.totalsem.com) hoặc gửi email đến địa chỉ [support@totalsem.com](mailto:support@totalsem.com).

Đối với những thắc mắc liên quan đến nội dung của quyển sách này, hãy ghé thăm trang [www.mheducation.com/customerservice](http://www.mheducation.com/customerservice).

## Chú giải thuật ngữ

Thuật ngữ	Định nghĩa
<b>A</b>	
<b>3DES</b>	Mã hóa DES ba lần – ba vòng mã hóa DES được sử dụng để tăng cường bảo mật.
<b>802.11</b>	Một họ tiêu chuẩn để mô tả các giao thức mạng dành cho các thiết bị không dây.
<b>802.1X</b>	Một tiêu chuẩn IEEE để thực hiện việc xác thực trên các mạng.
<b>AAA</b>	Xem xác thực, cấp phép và tính toán.
<b>ABAC</b>	Xem kiểm soát truy cập dựa-trên-thuộc-tính.
<b>acceptable use policy (AUP)</b>	Một chính sách truyền đạt cho người dùng về những cách sử dụng tài nguyên máy tính cụ thể nào được chấp thuận.
<b>access</b>	Khả năng của một đối tượng để thực hiện những hoạt động cụ thể trên một đối tượng chẳng hạn như một tập tin. Các cấp độ truy cập điển hình bao gồm đọc, ghi, thực thi, và xóa.

<b>access controls</b>	Các cơ chế hoặc phương pháp được sử dụng để xác định những quyền truy cập nào mà các chủ thể (chẳng hạn như người dùng) có đối với các đối tượng cụ thể (chẳng hạn như các tập tin).
<b>access control list (ACL)</b>	Một danh sách tương ứng với một đối tượng (chẳng hạn như một tập tin) để xác định mức truy cập nào mà từng chủ thể (chẳng hạn như một người dùng) đã có cũng như những gì họ có thể thực hiện đối với đối tượng (chẳng hạn như đọc, ghi, hoặc thực thi).
<b>access point (AP)</b>	Từ viết tắt của điểm truy cập không dây, thiết bị cho phép các thiết bị kết nối tới một mạng không dây.
<b>Active Directory (AD)</b>	Phần dịch vụ thư mục của hệ điều hành Windows lưu trữ thông tin về các thực thể dựa-trên-mạng (chẳng hạn như các ứng dụng, tập tin, máy in và con người) và cung cấp một cách thức nhất quán và có cấu trúc để đặt tên, mô tả, định vị, truy cập và quản lý các tài nguyên này.
<b>Active Server Pages (ASP)</b>	Một khuôn khổ tập lệnh phía-máy-chủ cũ hơn dành cho các máy chủ web được giới thiệu bởi Microsoft. Đã được thay thế bằng ASP.NET trong 2002.
<b>ActiveX</b>	Công nghệ không còn sử dụng nữa của Microsoft tạo điều kiện cho các ứng dụng Internet phong phú và do đó mở rộng và nâng cao chức năng của Microsoft Internet Explorer. Giống như Java, ActiveX cho phép phát triển nội dung tương tác. Khi trình

	duyệt nhận-biết-ActiveX gặp một trang web có tính năng không được hỗ trợ, trình duyệt này có thể tự động cài đặt ứng dụng thích hợp để có thể sử dụng tính năng này.
<b>AD</b>	Xem Active Directory.
<b>Address Resolution Protocol (ARP)</b>	Một giao thức trong bộ đặc tả thông số kỹ thuật TCP/IP được sử dụng để ánh xạ một địa chỉ IP với một địa chỉ Kiểm soát Truy cập Phương tiện (Media Access Control – MAC).
<b>Address Space Layout Randomization (ASLR)</b>	Một tiến trình bảo-vệ-bộ-nhỏ được sử dụng bởi hệ điều hành trong đó không gian bộ nhớ được khóa ngẫu nhiên để bảo vệ chống lại các lần chèn tập lệnh có chủ đích từ các cuộc tấn công tràn-bộ-nhỏ-đệm.
<b>Advanced Encryption Standard (AES)</b>	Tiêu chuẩn hiện hành của Chính phủ Hoa Kỳ dành cho mã hóa đối xứng, được sử dụng rộng rãi trong tất cả các ngành.
<b>Advanced Encryption Standard 256-bit</b>	Một triển khai AES sử dụng một khóa 256-bit.
<b>advanced persistent threat (APT)</b>	Một véc-tơ mối đe dọa mà mục tiêu chính là ẩn náu trong hệ thống, với trích lọc dữ liệu là nhiệm vụ thứ cấp.

<b>Adversarial Techniques, Common Knowledge (ATT&amp;CK)</b>	Một khuôn khổ được phát triển bởi MITRE để mô tả các phương pháp được sử dụng bởi những kẻ tấn công.
<b>adware</b>	Phần mềm hỗ-trợ-quảng-cáo tự động phát, hiển thị hoặc tải xuống các quảng cáo sau khi phần mềm được cài đặt hoặc trong khi ứng dụng đang được sử dụng.
<b>AEAD</b>	<i>Xem</i> Authenticated Encryption with Associated Data.
<b>AES</b>	<i>Xem</i> Advanced Encryption Standard.
<b>AES256</b>	<i>Xem</i> Advanced Encryption Standard 256-bit.
<b>AH</b>	<i>Xem</i> Authentication Header.
<b>AI</b>	Từ viết tắt của trí tuệ nhân tạo.
<b>air gap</b>	Sự tách biệt cưỡng bức của các mạng, dẫn đến "khoảng cách" giữa các hệ thống. Truyền thông qua một khe hở không khí đòi hỏi một nỗ lực thủ công để di chuyển dữ liệu từ mạng này sang mạng khác, vì không có kết nối mạng nào tồn tại giữa hai mạng.
<b>AIS</b>	<i>Xem</i> Automated Indicator Sharing.

<b>algorithm</b>	Một thủ tục từng-bước – điển hình là một phép tính đã được thiết lập để giải quyết một vấn đề trong phạm vi một số bước.
<b>amplification</b>	Một hành động tận dụng công nghệ để khuếch đại một cuộc tấn công, chẳng hạn như ping một địa chỉ mạng để yêu cầu tất cả các thiết bị được kết nối vào mạng gửi lại phản hồi.
<b>annual loss expectancy (ALE)</b>	Một sự kiện dự kiến sẽ gây thiệt hại bao nhiêu cho doanh nghiệp mỗi năm như thế nào, với chi phí tính bằng đô-la của tổn thất và tần suất nó có khả năng xảy ra. ALE = dự báo tổn thất đơn lẻ × tỷ lệ xuất hiện hàng năm.
<b>annualized rate of occurrence (ARO)</b>	Tần suất mà theo đó, một sự kiện được dự kiến sẽ xảy ra trên cơ sở hàng năm.
<b>anomaly</b>	Một điều gì đó không phù hợp với hình mẫu đã được dự kiến.
<b>antivirus (AV)</b>	Một chương trình phần mềm được thiết kế để phát hiện, giảm nhẹ, hoặc loại bỏ phần mềm độc hại và vi-rút máy tính khỏi một hệ thống hoặc một mạng.
<b>Anything as a Service (XaaS)</b>	Một thuật ngữ mô tả một loạt các dịch vụ có thể được cung cấp cho người dùng từ đám mây.
<b>AP</b>	Xem Access Point.

<b>application</b>	Một chương trình hoặc một nhóm chương trình được thiết kế để cung cấp các chức năng người dùng cụ thể, chẳng hạn như trình xử lý văn bản hoặc máy chủ web.
<b>application programming interface (API)</b>	Một tập hợp các hướng dẫn về cách tương tác với chương trình máy tính để các nhà phát triển có thể truy cập các giao diện đã được xác định trong một chương trình.
<b>application service provider (ASP)</b>	Một công ty cung cấp cho các thực thể quyền truy cập vào các ứng dụng và dịch vụ qua Internet.
<b>APT</b>	Xem advanced persistent threat.
<b>ARP</b>	Xem Address Resolution Protocol.
<b>ARP Poisoning</b>	Một cuộc tấn công vào bảng ARP nơi các giá trị bị thay đổi dẫn đến lưu lượng truy cập bị định hướng sai.
<b>ASLR</b>	Xem Address Space Layout Randomization.
<b>ASN.1</b>	Tóm tắt Cú pháp Ký hiệu số một là một ký hiệu chính thức được sử dụng để mô tả việc truyền dữ liệu trong các giao thức viễn thông.
<b>asset</b>	Một nguồn lực hoặc thông tin mà tổ chức cần để tiến hành hoạt động kinh doanh của mình.

<b>asset value (AV)</b>	Giá trị của một tài sản đang chịu rủi ro.
<b>asymmetric encryption</b>	Còn được gọi là mã hóa khóa công khai, một hệ thống mã hóa dữ liệu sử dụng hai khóa toán học để mã hóa và giải mã một tin nhắn - một khóa công khai, khả dụng cho tất cả mọi người và một khóa riêng tư, chỉ dành cho chủ sở hữu của khóa.
<b>ATT&amp;CK</b>	Xem Adversarial Tactics, Techniques, and Common Knowledge.
<b>attribute-based access control (ABAC)</b>	Một cơ chế kiểm soát truy cập để cấp quyền truy cập dựa trên các thuộc tính của người dùng.
<b>audit trail</b>	Một tập hợp các bản ghi hoặc sự kiện, thường được tổ chức theo thứ tự thời gian, ghi lại những hoạt động nào đã xảy ra trên một hệ thống. Các bản ghi này (thường là các tập tin máy tính) thường được sử dụng để cỗ gắng tái tạo lại những gì đã diễn ra khi sự cố bảo mật xảy ra và chúng cũng có thể được sử dụng để phát hiện những kẻ xâm nhập khả dĩ.
<b>auditing</b>	Các hành động hoặc quy trình được sử dụng để xác minh các đặc quyền và quyền đã được chỉ định của người dùng hoặc bất kỳ năng lực nào được sử dụng để tạo ra và duy trì hồ sơ cho thấy ai đã truy cập vào một hệ thống cụ thể và họ đã thực hiện những hành động nào.

<b>Authenticated Encryption with Associated Data (AEAD)</b>	Một phương pháp mã hóa cho phép người nhận kiểm tra tính toàn vẹn của cả thông tin được mã hóa và không được mã hóa trong một thông điệp.
<b>authentication</b>	Tiến trình mà theo đó, nhân dạng của một chủ thể (chẳng hạn như của một người dùng) được xác minh.
<b>authentication, authorization and accounting (AAA)</b>	Ba chức năng phổ biến được thực hiện khi đăng nhập vào hệ thống. Xác thực và cấp phép hầu như luôn xảy ra, với tính toán thì ít phổ biến hơn. Xác thực và cấp phép là một phần của hệ thống kiểm soát truy cập.
<b>Authentication Header (AH)</b>	Một phần của giao thức bảo mật IPSec cung cấp các dịch vụ xác thực và khả năng phát-hiện-phát-lại. AH có thể được sử dụng bởi chính nó hoặc với Tải trọng Bảo mật Đóng gói (Encapsulation Security Payload - ESP). Tham khảo RFC 2402.
<b>Automated Indicator Sharing (AIS)</b>	Sử dụng STIX và TAXII để chia sẻ những thông tin về các mối đe dọa giữa các hệ thống.
<b>AV</b>	Xem antivirus hoặc asset value.
<b>B</b>	
<b>backdoor</b>	Một phương pháp ẩn giấu được sử dụng để truy cập vào hệ thống máy tính, mạng hoặc ứng dụng. Thường được sử dụng bởi các nhà phát triển phần mềm để đảm

	bảo quyền truy cập không hạn chế vào hệ thống mà họ tạo ra. Đồng nghĩa với <i>cửa sập (trapdoor)</i> .
<b>backup</b>	Đề cập đến việc sao chép và lưu trữ dữ liệu ở một vị trí thứ cấp và tách biệt với bản gốc để bảo toàn dữ liệu trong trường hợp bản gốc bị mất, bị hư hỏng hoặc bị phá hủy.
<b>baseline</b>	Một hệ thống hoặc phần mềm khi nó được xây dựng và hoạt động tại một thời điểm cụ thể. Đóng vai trò là nền tảng để so sánh hoặc đo lường, cung cấp tính minh bạch cần thiết để kiểm soát sự thay đổi.
<b>BASH</b>	Xem Bourne Again Shell
<b>Basic Input/Output System (BIOS)</b>	Một phần tử của firmware của hệ thống máy tính cung cấp giao diện tương tác giữa phần cứng và phần mềm hệ thống với các thiết bị và thiết bị ngoại vi. BIOS đã được thay thế bằng Giao diện Phần mềm Mở rộng Hợp nhất (Unified Extensible Firmware Interface - UEFI), một hệ thống phức tạp hơn và có năng lực hơn.
<b>Basic Service Set Identifier (BSSID)</b>	Mã định danh của một điểm truy cập (AP) trong một WLAN, thường là địa chỉ MAC của AP.
<b>BCP</b>	Xem business continuity plan.
<b>BGP</b>	Xem Border Gateway Protocol.

<b>BIA</b>	Xem business impact analysis.
<b>biometrics</b>	Được sử dụng để xác minh danh tính của một cá nhân đối với hệ thống hoặc mạng bằng cách sử dụng thông tin nào đó duy nhất về cá nhân đó, chẳng hạn như dấu vân tay, cho quá trình xác minh. Các ví dụ bao gồm dấu vân tay, quét võng mạc, hình học bàn tay và khuôn mặt, và phân tích giọng nói.
<b>BIOS</b>	Xem Basic Input/Output System.
<b>birthday attack</b>	Một phương pháp tấn công dựa trên các sự kết hợp chứ không phải xác suất tuyến tính. Ví dụ, trong một căn phòng có 30 người, một người không nhất thiết phải khớp với một ngày sinh cụ thể mà có thể có hai ngày sinh bất kỳ trong cùng một căn phòng, khiến cho vấn đề trở thành một khớp tổ hợp, vốn có nhiều khả năng xảy ra hơn.
<b>Blowfish</b>	Một bản triển khai miễn phí của mật mã khối đối xứng, được phát triển bởi Bruce Schneier để thay thế cho DES và IDEA. Nó có lược đồ độ-dài-bit-thay-đổi từ 32 đến 448 bit, dẫn đến các mức độ bảo mật khác nhau.
<b>bluebugging</b>	Sử dụng thiết bị được-Bluetooth-hỗ-trợ để nghe trộm cuộc trò chuyện của người khác bằng cách sử dụng điện thoại Bluetooth của người đó làm thiết bị phát. Ứng dụng bluebug âm thầm khiến thiết bị Bluetooth thực hiện cuộc gọi đến một thiết bị

	khác, khiến điện thoại hoạt động như một thiết bị phát và cho phép người nghe nghe trộm cuộc trò chuyện của nạn nhân trong đời thực.
<b>bluejacking</b>	Việc gửi các tin nhắn không mong muốn thông qua Bluetooth tới các thiết bị hỗ trợ Bluetooth như điện thoại di động, máy tính bảng hoặc máy tính xách tay.
<b>bluesnarfing</b>	Truy cập trái phép thông tin từ thiết bị được-Bluetooth-hỗ-trợ thông qua kết nối Bluetooth, thường là giữa điện thoại di động, máy tính để bàn, máy tính xách tay và máy tính bảng.
<b>Border Gateway Protocol (BGP)</b>	Giao thức định tuyến liên miền được triển khai trong mạng Giao thức Internet (IP) để cho phép định tuyến giữa các hệ thống độc lập.
<b>botnet</b>	Một tập hợp các rô bốt phần mềm, hoặc các <i>bots</i> , chạy độc lập và tự động và thường là ẩn dưới nền [chạy ngầm]. Thuật ngữ này thường được kết hợp với phần mềm độc hại, nhưng nó cũng có thể để cập đến mạng máy tính sử dụng phần mềm máy tính phân tán.
<b>Bourne Again Shell (BASH)</b>	Một ngôn ngữ lệnh dành cho hệ thống Linux.

<b>bridge protocol data unit (BPDU)</b>	BPDU là một kiểu thông điệp dữ liệu được trao đổi qua các thiết bị chuyển mạch trong một mạng LAN mở rộng sử dụng cấu trúc liên kết Giao thức Cây Mở rộng (Spanning Tree Protocol - STP).
<b>bring your own device (BYOD)</b>	Một thuật ngữ được sử dụng để mô tả một môi trường nơi người dùng mang những thiết bị thuộc sở hữu cá nhân của họ vào doanh nghiệp và tích hợp chúng vào hệ thống của doanh nghiệp.
<b>buffer overflow</b>	Một loại lỗi mã lập trình phần mềm cụ thể cho phép đầu vào của người dùng làm tràn vùng lưu trữ đã được cấp phát và gây gián đoạn chương trình đang chạy.
<b>business availability center (BAC)</b>	Một nền tảng phần mềm cho phép doanh nghiệp tối ưu hóa tính khả dụng, hiệu suất và hiệu quả của các dịch vụ và ứng dụng nghiệp vụ.
<b>business continuity plan (BCP)</b>	Kế hoạch mà một doanh nghiệp phát triển để tiếp tục các hoạt động quan trọng trong trường hợp xảy ra một sự gián đoạn nghiêm trọng.
<b>business impact analysis</b>	Phân tích tác động đối với hoạt động kinh doanh của một sự kiện cụ thể.
<b>business partnership agreement (BPA)</b>	Một thỏa thuận bằng văn bản xác định các điều khoản và điều kiện của một mối quan hệ đối tác kinh doanh.
<b>BYOD</b>	Xem bring your own device.

**C**

<b>CA</b>	Xem certificate authority.
<b>cache</b>	Việc lưu trữ tạm thời thông tin trước khi sử dụng, thường được sử dụng để tăng tốc các hệ thống. Trong bối cảnh Internet, bộ nhớ đệm đề cập đến việc lưu trữ các trang web thường được truy cập, các tập tin đồ họa và nội dung khác một cách cục bộ trên máy tính cá nhân của người dùng hoặc trên máy chủ web. Bộ nhớ đệm giúp giảm thiểu thời gian tải xuống và bảo toàn băng thông cho các trang web được truy cập thường xuyên, đồng thời giúp giảm tải trên máy chủ web.
<b>Capability Model (CMM)</b>	<b>Maturity</b> Một phương pháp có cấu trúc giúp cho các tổ chức cải thiện mức độ trưởng thành của các quy trình phần mềm của họ bằng cách cung cấp một lộ trình tiến hóa từ các quy trình đột xuất đến các quy trình quản lý phần mềm có kỷ luật. Được phát triển tại Viện Kỹ thuật Phần mềm của Đại học Carnegie Mellon (Carnegie Mellon University's Software Engineering Institute).
<b>CAPTCHA</b>	Kiểm tra Turing Công cộng Hoàn toàn Tự động (Completely Automated Public Turing Test) để phân biệt máy tính và con người. Phần mềm được thiết kế để đặt ra các bài kiểm tra yêu cầu khả năng giải quyết của con người, ngăn không cho rô bốt điền thông tin và gửi đến các trang web.
<b>CASB</b>	Xem Cloud Access Security Broker.

<b>CBC</b>	Xem Cipher Block Chaining.
<b>centralized management</b>	Một kiểu quản lý đặc quyền đưa quyền hạn và trách nhiệm quản lý và duy trì các quyền và đặc quyền vào một nhóm, vị trí hoặc khu vực.
<b>CERT</b>	Xem Computer Emergency Response Team.
<b>certificate</b>	Một đối tượng được ký bằng mật mã có chứa một danh tính và khóa công khai được liên kết với danh tính này. Chứng chỉ có thể được sử dụng để xác lập danh tính, tương tự như một tài liệu văn bản đã được công chứng.
<b>certificate authority (CA)</b>	Một thực thể chịu trách nhiệm cho việc cấp và thu hồi chứng chỉ. CA thường không được liên kết với công ty yêu cầu chứng chỉ, mặc dù chúng cũng tồn tại để sử dụng trong nội bộ công ty (chẳng hạn như Microsoft). Thuật ngữ này cũng được áp dụng cho phần mềm máy chủ cung cấp các dịch vụ này. Thuật ngữ <i>cơ quan cấp chứng chỉ (certificate authority)</i> được sử dụng thay thế cho <i>cơ quan cấp chứng chỉ (certification authority)</i> .
<b>Certificate Enrollment Protocol (CEP)</b>	Ban đầu được phát triển bởi VeriSign dành cho Hệ thống Cisco để hỗ trợ việc cấp phát, phân phối và thu hồi chứng chỉ bằng cách sử dụng các công nghệ hiện có.
<b>certificate revocation list (CRL)</b>	Một đối tượng được ký điện tử liệt kê tất cả các chứng chỉ hiện tại nhưng đã bị thu hồi bởi một cơ quan cấp chứng chỉ nhất định cấp. Điều này cho phép người dùng xác minh xem chứng chỉ hiện có hợp lệ hay không ngay cả khi nó chưa hết hạn.

	CRL tương tự như một danh sách các mã số thẻ tín dụng bị đánh cắp cho phép các cửa hàng từ chối thẻ tín dụng xấu.
<b>certificate signing request (CSR)</b>	Một thông điệp được gửi từ một người đăng ký đến cơ quan cấp chứng chỉ để đăng ký chứng chỉ nhận dạng kỹ thuật số.
<b>chain of custody</b>	Các quy tắc về lập hồ sơ, xử lý và bảo vệ bằng chứng để đảm bảo rằng không có những thay đổi không lường trước được đối với bằng chứng.
<b>Challenge Handshake Authentication Protocol (CHAP)</b>	Được sử dụng để cung cấp xác thực qua các liên kết điểm-đến-điểm bằng cách sử dụng Giao thức Điểm-đến-điểm (Point-to-Point Protocol - PPP).
<b>change (configuration) management</b>	Một phương pháp luận tiêu chuẩn để thực hiện và ghi nhận lại những thay đổi trong quá trình phát triển và vận hành phần mềm.
<b>change control board (CCB)</b>	Một cơ quan giám sát quá trình quản lý thay đổi và cho phép cấp quản lý giám sát và điều phối các dự án.
<b>channel service unit (CSU)</b>	Một thiết bị được sử dụng để liên kết các mạng cục bộ (LAN) thành một mạng diện rộng (WAN) sử dụng các dịch vụ của nhà cung cấp dịch vụ viễn thông.
<b>CHAP</b>	Xem Challenge Handshake Authentication Protocol.

<b>chief security officer (CSO)</b>	Người được bổ nhiệm để giám sát các chức năng an ninh trong một doanh nghiệp.
<b>chief technology officer (CTO)</b>	Người được bổ nhiệm giám sát các chức năng về công nghệ khoa học trong doanh nghiệp.
<b>choose your own device (CYOD)</b>	Một phương pháp triển khai thiết bị di động trong đó mỗi người chọn loại thiết bị của riêng họ.
<b>CIA of security</b>	Đề cập đến tính bảo mật, tính toàn vẹn và tính sẵn sàng - các chức năng cơ bản của bất kỳ hệ thống bảo mật nào.
<b>cipher</b>	Một hệ thống mật mã chấp nhận đầu vào là văn bản rõ ràng (plaintext) và sau đó xuất ra bản mã theo thuật toán và khóa bên trong của nó.
<b>Cipher Block Chainint (CPB)</b>	Một phương pháp bổ sung sự thêm ngẫu nhiên vào các khối, trong đó mỗi khối văn bản rõ ràng được XOR với khối bản mã trước đó trước khi được mã hóa.
<b>cipher feedback (CFB)</b>	Một phương pháp để biến một mật mã khối thành một mật mã luồng tự-đồng-bộ-hóa.
<b>ciphertext</b>	Đầu ra của một thuật toán mã hóa - dữ liệu được mã hóa.

<b>CIRT</b>	<i>Xem Computer Emergency Response Team.</i>
<b>clickjacking</b>	Một cuộc tấn công chống lại giao diện người dùng trong đó người dùng nhấp vào thứ gì đó mà không biết về nó, ví dụ: một mục bị ẩn hoặc không nhìn thấy, kích hoạt một hành động trình duyệt mà người dùng không biết vào thời điểm đó.
<b>closed circuit television (CCTV)</b>	Một hệ thống truyền hình riêng tư thường được nối cứng trong các ứng dụng an ninh để ghi lại những thông tin hình ảnh.
<b>Cloud Access Security Broker (CASB)</b>	Một cơ chế thực thi chính sách bảo mật giữa người dùng đám mây và nhà cung cấp dịch vụ đám mây.
<b>cloud computing</b>	Việc cung cấp tự động các tài nguyên tính toán theo yêu cầu trên một mạng.
<b>cloud service provider (CSP)</b>	Một công ty cung cấp các dịch vụ mạng, cơ sở hạ tầng hoặc các ứng dụng nghiệp vụ dựa-trên-đám-mây.
<b>CMS</b>	<i>Xem content management system.</i>
<b>CN</b>	<i>Xem Common Name.</i>
<b>codec</b>	Một hệ thống cung cấp các dịch vụ mã hóa và giải mã, được sử dụng trong phát trực tuyến đa phương tiện.

<b>cold site</b>	Một hình thức địa điểm dự phòng rẻ tiền không bao gồm tập hợp dữ liệu hiện tại tại mọi thời điểm. Một địa điểm lạnh mất nhiều thời gian hơn để khôi phục hệ thống hoạt động, nhưng nó ít tốn kém hơn đáng kể so với địa điểm ấm hoặc nóng.
<b>collision</b>	Được sử dụng trong phân tích mật mã băm, một xung đột là tình huống kết quả xảy ra khi một thuật toán băm sẽ tạo ra cùng một giá trị băm từ hai tập hợp dữ liệu khác nhau.
<b>Common Access Card (CAC)</b>	Một thẻ thông minh được sử dụng để truy cập các hệ thống máy tính liên bang của Hoa Kỳ và cũng hoạt động như một thẻ ID.
<b>Common Name (CN)</b>	Một trường đặc trưng trong Tên Phân biệt (Distinguished Name - DN).
<b>Common Vulnerability and Exposure (CVE)</b>	Một bản liệt kê các lỗ hổng bảo mật đã biết.
<b>Common Vulnerability Scoring System (CVSS)</b>	Một khuôn khổ để chấm điểm mức độ nghiêm trọng của lỗ hổng.
<b>Computer Emergency Response Team (CERT)</b>	Nhóm chịu trách nhiệm điều tra và ứng phó với các vi phạm bảo mật, vi-rút [máy tính] và các sự cố thảm khốc có thể xảy ra khác. Còn được gọi là Nhóm ứng phó sự cố máy tính (Computer Incident Response Team - CIRT).

<b>computer security</b>	Nói chung là các phương pháp, kỹ thuật và công cụ được sử dụng để đảm bảo rằng một hệ thống máy tính được bảo mật.
<b>computer software configuration item</b>	Xem configuration item.
<b>confidentiality</b>	Một phần của CIA về bảo mật, tính bí mật đề cập đến nguyên tắc bảo mật tuyên bố rằng thông tin không được tiết lộ cho các cá nhân trái phép.
<b>configuration auditing</b>	Quá trình xác minh rằng các đơn vị cấu hình đã được xây dựng và duy trì theo các yêu cầu, tiêu chuẩn hoặc các thỏa thuận hợp đồng.
<b>configuration control</b>	Quá trình kiểm soát các thay đổi đối với các đơn vị [cấu hình] đã được lập đường cơ sở.
<b>configuration identification</b>	Quá trình xác định những tài sản nào cần phải được quản lý và kiểm soát.
<b>configuration item</b>	Dữ liệu và phần mềm (hoặc các tài sản khác) được xác định và quản lý như một phần của quy trình quản lý thay đổi phần mềm. Còn được gọi là <i>đơn vị cấu hình phần mềm máy tính</i> ( <i>computer software configuration item</i> ).
<b>configuration status accounting</b>	Các thủ tục theo dõi và duy trì dữ liệu liên quan đến từng đơn vị cấu hình trong đường cơ sở.

<b>content management system (CMS)</b>	Một hệ thống quản lý để quản lý nội dung cho một hệ thống cụ thể, chẳng hạn như một trang web.
<b>contingency planning (CP)</b>	Hành động tạo ra các quy trình và thủ tục được sử dụng trong những điều kiện đặc biệt (dự phòng).
<b>continuity of operations planning (COOP)</b>	Việc tạo ra các kế hoạch liên quan đến việc tiếp tục các hoạt động kinh doanh thiết yếu sau bất kỳ sự gián đoạn nghiêm trọng nào.
<b>controller area network (CAN)</b>	Một tiêu chuẩn bus để sử dụng trên các phương tiện để kết nối vi điều khiển.
<b>cookie</b>	Thông tin được máy chủ web lưu trữ trên máy tính của người dùng để duy trì trạng thái kết nối với máy chủ web. Được sử dụng chủ yếu để các thông tin tùy chọn hoặc thông tin đã được sử dụng trước đó có thể được gọi lại khi có các yêu cầu tới máy chủ trong tương lai.
<b>COOP</b>	Xem continuity of operations planning.
<b>corporate owned, personally enabled (COPE)</b>	Một hình thức quản lý/sở hữu thiết bị di động trong đó công ty cung cấp các thiết bị di động cho nhân viên và cho phép họ sử dụng thiết bị như thẻ họ [nhân viên] đang sở hữu chúng.

<b>corrective action report (CAR)</b>	Một báo cáo được sử dụng để ghi lại các hành động khắc phục được thực hiện trên một hệ thống.
<b>Counter Mode (CTM)</b>	Biến mật mã khối thành mật mã luồng.
<b>Counter Mode with Cipher Block Chaining – Message Authentication Code Protocol (CCMP)</b>	Một cơ chế đóng gói mã hóa dữ liệu nâng cao dựa trên Chế độ Bộ đếm (Counter Mode) với CBC-MAC từ AES, được thiết kế để sử dụng qua mạng LAN không dây.
<b>countermeasure</b>	<i>Xem</i> security controls.
<b>cracking</b>	Một thuật ngữ được một số người sử dụng để chỉ hành vi tin tặc độc hại, trong đó một cá nhân cố gắng truy cập trái phép vào hệ thống máy tính hoặc mạng. <i>Xem</i> thêm tin tặc (hacking).
<b>CRC</b>	<i>Xem</i> cyclic redundancy check.
<b>CRL</b>	<i>Xem</i> certificate revocation list.
<b>cross-site request forgery (CSRF hoặc XSRF)</b>	Một phương pháp tấn công hệ thống bằng cách gửi đầu vào độc hại đến hệ thống và dựa vào bộ phân tích cú pháp và các phần tử thực thi để thực hiện các hành động được yêu cầu, từ đó khởi tạo cuộc tấn công. XSRF khai thác độ tin cậy của một trang web trong trình duyệt của người dùng.

<b>cross-site scripting (XSS)</b>	Một phương pháp tấn công hệ thống bằng cách gửi các lệnh kịch bản tới đầu vào của hệ thống và dựa vào bộ phân tích cú pháp và các phần tử thực thi để thực hiện các hành động theo kịch bản được yêu cầu, từ đó khởi tạo cuộc tấn công. XSS khai thác sự tin tưởng của người dùng đối với trang web.
<b>cryptanalysis</b>	Quá trình cố gắng phá vỡ một hệ thống mật mã.
<b>cryptography</b>	Nghệ thuật viết bí mật để cho phép một cá nhân ẩn nội dung của một thông điệp hoặc tập tin với tất cả trừ người nhận đã được dự định.
<b>crypto-malware</b>	Phần mềm độc hại sử dụng mật mã để mã hóa tập tin để tống tiền.
<b>CSO</b>	<i>Xem</i> chief security officer.
<b>CRT</b>	<i>Xem</i> Counter Mode - một cách viết tắt thay thế.
<b>CVE</b>	<i>Xem</i> Common Vulnerabilities Exposure.
<b>CVSS</b>	<i>Xem</i> Common Vulnerabilities Scoring System.
<b>cyclic redundancy check (CRC)</b>	Một kỹ thuật phát hiện lỗi sử dụng một chuỗi hai ký tự kiểm tra khối 8-bit để đại diện cho toàn bộ khối dữ liệu. Những ký tự kiểm tra khối này được kết hợp vào khung truyền tải và sau đó được kiểm tra tại đầu nhận tín hiệu.

**D**

<b>DAC</b>	Xem discretionary access control
<b>data encryption key (DEK)</b>	Một khóa mã hóa có chức năng mã hóa và giải mã dữ liệu.
<b>Data Encryption Standard (DES)</b>	Một thuật toán mã hóa khóa cá nhân đã được chính phủ Hoa Kỳ thông qua như một tiêu chuẩn để bảo vệ những thông tin nhạy cảm nhưng chưa được phân loại. Thường được sử dụng trong 3DES, trong đó ba vòng được áp dụng để cung cấp bảo mật cao hơn.
<b>data execution prevention (DEP)</b>	Một tính năng bảo mật của Hệ điều hành có thể được điều khiển bởi phần mềm, phần cứng hoặc cả hai, được thiết kế để ngăn chặn việc thực thi mã phần mềm từ các khối dữ liệu trong bộ nhớ.
<b>data loss prevention (DLP)</b>	Công nghệ, quy trình và thủ tục được thiết kế để phát hiện khi nào thì việc xóa trái phép dữ liệu khỏi hệ thống đã xảy ra. DLP thường hoạt động, ngăn ngừa sự mất mát bằng cách ngăn chặn việc truyền tải hoặc ngắt kết nối.
<b>data protection officer</b>	Người phụ trách về quyền riêng tư/bảo vệ dữ liệu tại Liên minh Châu Âu theo GDPR.
<b>data service unit</b>	Xem channel service unit.

<b>datagram</b>	Một gói dữ liệu có thể được truyền tải qua hệ thống chuyển mạch gói ở chế độ không kết nối.
<b>decision tree</b>	Một cấu trúc dữ liệu trong đó mỗi phần tử được gắn với một hoặc nhiều cấu trúc ngay bên dưới nó.
<b>demilitarized zone (DMZ)</b>	Một phân đoạn mạng tồn tại trong một khu vực được bảo vệ giữa Internet và mạng tin cậy an toàn bên trong.
<b>denial-of-service (DoS)</b>	Một cuộc tấn công trong đó các hành động được thực hiện để tước quyền truy cập của các cá nhân đã được cấp phép vào hệ thống, tài nguyên của hệ thống, dữ liệu mà nó lưu trữ hoặc xử lý, hoặc mạng mà nó được kết nối.
<b>Destination Network Address Translation (DNAT)</b>	Một biến dịch tĩnh 1-1 từ địa chỉ đích công khai sang địa chỉ riêng tư.
<b>DES</b>	Xem Data Encryption Standard.
<b>DHCP</b>	Xem Dynamic Host Configuration Protocol.
<b>Diffie-Hellman</b>	Một phương pháp mật mã để thiết lập khóa được chia sẻ trên một phương tiện không an toàn theo cách thức an toàn.

<b>Diffie-Hellman Ephemeral (DHE)</b>	Một phương pháp mã hóa thiết lập khóa chia sẻ trên một phương tiện không an toàn theo cách an toàn bằng cách sử dụng khóa tạm thời để cho phép bảo mật chuyển tiếp hoàn hảo.
<b>digital forensics and investigation response (DFIR)</b>	Một tên gọi khác của quy trình ứng phó sự cố.
<b>digital signature</b>	Một tạo tác dựa-trên-mật-mã là thành phần chính của việc triển khai cơ sở hạ tầng khóa công khai (public key infrastructure - PKI). Chữ ký điện tử có thể được sử dụng để chứng minh danh tính vì nó được tạo bằng phần khóa riêng tư của cặp khóa công khai/khóa riêng tư. Người nhận có thể giải mã chữ ký và bằng cách đó, nhận được sự đảm bảo rằng dữ liệu phải đến từ người gửi và dữ liệu đã không bị thay đổi.
<b>Digital Signature Algorithm (DSA)</b>	Một tiêu chuẩn của chính phủ Hoa Kỳ để triển khai chữ ký kỹ thuật số.
<b>direct-sequence spread spectrum (DSSS)</b>	Một phương pháp phân phối thông tin liên lạc qua nhiều tần số để tránh nhiễu và tránh bị phát hiện.
<b>disassociation</b>	Một cuộc tấn công vào mạng không dây theo đó kẻ tấn công gửi một khung hủy xác thực trong một kết nối không dây, để phá vỡ một kết nối hiện có.

<b>disaster recovery plan (DRP)</b>	Một kế hoạch bằng văn bản được phát triển để xác định cách thức một tổ chức sẽ phản ứng với thảm họa tự nhiên hoặc nhân tạo nhằm đảm bảo tính liên tục của hoạt động kinh doanh. Liên quan đến khái niệm về kế hoạch liên tục kinh doanh (BCP).
<b>discretionary access control (DAC)</b>	Một cơ chế kiểm soát truy cập trong đó chủ sở hữu đối tượng (chẳng hạn như tập tin) có thể quyết định chủ thể nào khác (chẳng hạn như người dùng khác) có thể có quyền truy cập vào đối tượng cũng như quyền truy cập nào (đọc, ghi, thực thi) mà những chủ thể này có thể có.
<b>Distinguished Encoding Rules (DER)</b>	Một phương pháp cung cấp chính xác một cách để biểu diễn bất kỳ giá trị ASN.1 nào dưới dạng chuỗi octet.
<b>Distinguished Name (DN)</b>	Tên gọi để phân biệt một mục nhập trong một hệ thống đặt tên.
<b>distributed denial-of-service (DDoS)</b>	Một kiểu tấn công DoS đặc biệt, trong đó kẻ tấn công gây ra tình trạng hỗ trợ nói chung không sẵn sàng của các hệ thống khác để khởi động một cuộc tấn công rất-nhiều-chỗng-lại-một.
<b>diversity of defense</b>	Phương pháp tiếp cận tạo ra các lớp bảo mật khác nhau để kẻ xâm nhập có thể xâm phạm một lớp sẽ phải đổi mặt với một bộ phòng thủ hoàn toàn khác ở lớp tiếp theo.

<b>DLL injection</b>	Một cuộc tấn công sử dụng việc chèn một DLL vào một hệ thống, làm thay đổi quá trình xử lý của một chương trình về bản chất là lập trình lại nó [chương trình].
<b>DNS</b>	<i>Xem Domain Name Service/Server.</i>
<b>DNS poisoning</b>	Việc thay đổi dữ liệu trong một bảng DNS để gây ra việc đánh địa chỉ sai các gói.
<b>DNSSEC</b>	<i>Xem Domain Name System Security Extentions.</i>
<b>domain hijacking</b>	Hành động thay đổi đăng ký tên miền mà không được phép của người đăng ký ban đầu.
<b>Domain Message Authentication Reporting and Conformance (DMARC)</b>	Một giao thức xác thực, chính sách và báo cáo email.
<b>Domain Name Service/Server (DNS)</b>	Dịch vụ biên dịch tên miền Internet (chẳng hạn như <a href="http://www.mhprofessional.com">www.mhprofessional.com</a> ) thành địa chỉ IP.
<b>Domain Name Service System Security Extensions (DNSSEC)</b>	Phần mở rộng của DNS sử dụng các yêu cầu và câu trả lời đã được ký bằng mật mã.

<b>DRP</b>	Xem disaster recovery plan.
<b>DSSS</b>	Xem direct-sequence spread spectrum.
<b>dumpster diving</b>	Tiến hành tìm kiếm trong thùng rác để phát hiện các tài liệu đã được vứt bỏ mang tính nhạy cảm, vẫn chưa được tiêu hủy hoặc băm nhỏ.
<b>Dynamic Host Configuration Protocol (DHCP)</b>	Đặc tả thông số kỹ thuật Giao thức Internet (IP) của Lực lượng Đặc nhiệm Kỹ thuật Internet (IETF) để tự động phân bổ địa chỉ IP và thông tin cấu hình khác dựa trên địa chỉ bộ điều hợp mạng (card mạng). Nó cho phép phân bổ và nhóm địa chỉ, đồng thời đơn giản hóa việc cài đặt và quản trị TCP / IP.
<b>dynamic link library (DLL)</b>	Một chức năng thư viện chia sẻ được sử dụng trong môi trường Microsoft Windows.
<b>E</b>	
<b>EAP</b>	Xem Extensible Authentication Protocol.
<b>electromagnetic interference (EMI)</b>	Sự gián đoạn hoặc nhiễu của thiết bị điện tử do trường điện từ.
<b>electromagnetic pulse (EMP)</b>	Sự gián đoạn hoặc nhiễu của thiết bị điện tử do một trường điện từ cường độ cao đột ngột dưới dạng một xung đột ngột hoặc xung.

<b>Electronic Code Book (ECB)</b>	Một chẽ độ mật mã khối trong đó thông điệp được chia thành các khối, và mỗi khối được mã hóa một cách riêng biệt.
<b>electronic serial number (ESN)</b>	Một mã số nhận dạng duy nhất được các nhà sản xuất nhúng vào vi mạch trong điện thoại không dây.
<b>elliptic curve cryptography (ECC)</b>	Một phương pháp mã hóa khóa công khai dựa trên cấu trúc đại số của đường cong elliptic trên các trường hữu hạn.
<b>Elliptic Curve Diffie-Hellman Ephemeral (ECDHE)</b>	Một phương pháp mã hóa sử dụng ECC để thiết lập khóa chia sẻ trên một phương tiện không an toàn theo cách an toàn bằng cách sử dụng khóa tạm thời để cho phép bảo mật chuyển tiếp hoàn hảo.
<b>Elliptic Curve Digital Signature Algorithm (ECDSA)</b>	Một phương pháp mã hóa sử dụng ECC để tạo ra một chữ ký điện tử.
<b>Encapsulating Security Payload (ESP)</b>	Một phần của việc triển khai IPSec để cung cấp tính bảo mật của dữ liệu với các dịch vụ xác thực và phát-hiện-phát-lại tùy chọn. ESP hoàn toàn đóng gói dữ liệu người dùng trong lược đồ dữ liệu và có thể được sử dụng bởi chính nó hoặc kết hợp với Tiêu đề Xác thực (Authentication Header) cho các mức độ khác nhau của dịch vụ IPSec.

<b>Encrypted File System (EFS)</b>	Một tính năng bảo mật của Windows, kể từ Windows 2000 trở đi, cho phép mã hóa/giải mã minh bạch các tập tin trên hệ thống.
<b>end of life (EOL)</b>	Một thuật ngữ được sử dụng để biểu thị rằng một cái gì đó đã hết "vòng đời hữu ích" của nó.
<b>end of service life (EOSL)</b>	Một thuật ngữ được sử dụng để biểu thị thời điểm nhà sản xuất ngừng bán một mặt hàng. Trong hầu hết các trường hợp, nhà sản xuất không còn cung cấp các dịch vụ bảo trì hoặc cập nhật.
<b>escalation auditing</b>	Quá trình tìm kiếm sự gia tăng các đặc quyền, chẳng hạn như khi một người dùng bình thường có được các đặc quyền của cấp quản trị viên.
<b>ESSID</b>	Xem Extended Service Set Identifier.
<b>evidence</b>	Các tài liệu, lời khai và đối tượng vật chất có thể được chấp nhận trước tòa án pháp luật.
<b>evil twin</b>	Một cuộc tấn công liên quan đến một bộ định tuyến do kẻ-tấn-công-sở-hữu trong hệ thống không dây, được thiết lập cấu hình để khớp với một bộ định tuyến hợp pháp.
<b>exposure factor (EF)</b>	Một thước đo mức độ tổn thất của một tài sản. Được sử dụng trong tính toán tổn thất đơn lẻ dự kiến (SLE).

<b>Extended Service Set Identifier (ESSID)</b>	Tập hợp tất cả các BSSID trên một mạng WLAN, trên thực tế tương tự như SSID.
<b>Extensible Authentication Protocol (EAP)</b>	Một khuôn khổ xác thực chung được sử dụng trong các mạng không dây và kết nối điểm-đến-điểm. Nó được định nghĩa trong RFC 3748 và đã được cập nhật bởi RFC 5247.
<b>Extensible Markup Language (XML)</b>	Một ngôn ngữ đánh dấu dữ liệu dựa-trên-văn-bản, con-người-có-thể-đọc-được.
<b>F</b>	
<b>false acceptance rate (FAR)</b>	Tỷ lệ dương tính giả được hệ thống chấp nhận.
<b>false positive</b>	Thuật ngữ được sử dụng khi một hệ thống bảo mật mắc lỗi và báo cáo không chính xác về sự tồn tại của đối tượng được tìm kiếm. Các ví dụ bao gồm hệ thống phát hiện xâm nhập xác định nhầm lưu lượng truy cập lành tính là thù địch, một chương trình chống vi-rút báo cáo sự tồn tại của vi-rút trong phần mềm thực sự không bị nhiễm và hệ thống sinh trắc học cho phép một cá nhân trái phép truy cập vào hệ thống.

<b>false rejection rate (FRR)</b>	Mức độ chấp nhận được của những người dùng hợp pháp bị hệ thống từ chối.
<b>FDE</b>	Xem full disk encryption.
<b>FHSS</b>	Xem frequency-hopping spread spectrum.
<b>field programmable gate array (FPGA)</b>	Một mạch logic có thể lập trình được trong phần cứng.
<b>file system access control list (FACL)</b>	Việc triển khai các biện pháp kiểm soát truy cập như một phần của hệ thống tập tin.
<b>File Transfer Protocol (FTP)</b>	Một giao thức ở lớp ứng dụng được sử dụng để truyền tập tin qua kết nối mạng.
<b>File Transfer Protocol Secure (FTPS)</b>	Một giao thức lớp ứng dụng được sử dụng để truyền tập tin qua kết nối mạng, sử dụng FTP qua kết nối SSL hoặc TLS.
<b>firewall</b>	Một thiết bị mạng được sử dụng để tách riêng lưu lượng truy cập dựa trên các quy tắc.
<b>flood guard</b>	Một thiết bị mạng ngăn chặn các cuộc tấn công DoS/DDoS kiểu lũ lụt, thường là một phần của IDS/IPS.

<b>forensics (hoặc computer forensics)</b>	Việc lưu giữ, nhận dạng, lập tài liệu và diễn giải dữ liệu máy tính để sử dụng trong tố tụng pháp lý.
<b>FPGA</b>	Xem field programmable gate array.
<b>free space</b>	Các khu vực (sector) trên phương tiện lưu trữ đang sẵn sàng để hệ điều hành sử dụng.
<b>frequency-hopping spread spectrum</b>	Một phương pháp phân phối thông tin liên lạc qua nhiều tần số theo thời gian để tránh nhiễu và tránh bị phát hiện.
<b>full disk encryption</b>	Ứng dụng mã hóa toàn bộ đĩa cứng, bảo vệ tất cả nội dung trong một vùng chứa.
<b>G</b>	
<b>Galois Counter Mode (GCM)</b>	Một phương thức vận hành dành cho mã hóa khối mật mã khóa đối xứng đã được áp dụng rộng rãi vì nó có thể được vận hành song song để gia tăng hiệu quả và hiệu suất.
<b>General Data Protection Regulation (GDPR)</b>	Quy định về quyền riêng tư của dữ liệu của Liên minh Châu Âu (EU).
<b>Generic Routing Encapsulation (GRE)</b>	Một giao thức đường hầm được thiết kế để đóng gói nhiều gói tin lớp mạng bên trong các gói tin đường hầm IP.

<b>Global Positioning System (GPS)</b>	Một dạng dịch vụ định vị và tiêu chuẩn hóa thời gian dựa-trên-vệ-tinh.
<b>Gnu Privacy Guard (GPG)</b>	Một chương trình ứng dụng tuân theo tiêu chuẩn OpenPGP để mã hóa.
<b>GPG</b>	<i>Xem Gnu Privacy Guard.</i>
<b>GPO</b>	<i>Xem Group Policy Object.</i>
<b>graphic procesing unit (GPU)</b>	Một con chip được thiết kế để quản lý các chức năng đồ họa trong hệ thống.
<b>Group Policy Object (GPO)</b>	Một phương pháp được Windows sử dụng để áp dụng những thiết lập của hệ điều hành trong toàn doanh nghiệp.
<b>H</b>	
<b>hacking</b>	Thuật ngữ được giới truyền thông sử dụng để chỉ quá trình chiếm được sự truy cập trái phép vào hệ thống máy tính và mạng. Thuật ngữ này cũng đã được sử dụng để chỉ quá trình nghiên cứu sâu về mã và các giao thức được sử dụng trong hệ thống máy tính và mạng. <i>Xem thêm bẻ khóa (cracking).</i>
<b>hard disk drive (HDD)</b>	Một thiết bị cơ học được sử dụng để lưu trữ dữ liệu kỹ thuật số dưới dạng từ tính.

<b>hardware security module (HSM)</b>	Một thiết bị vật lý được sử dụng để bảo vệ nhưng vẫn cho phép sử dụng các khóa mã hóa. Nó được tách biệt với máy vật chủ.
<b>hash</b>	Một dạng mã hóa tạo ra một bản tóm tắt dữ liệu được đưa vào thuật toán. Các thuật toán này được gọi là thuật toán mật chiềng vì không có cách nào khả thi để giải mã những gì đã được mã hóa.
<b>hash value</b>	Xem message digest.
<b>hashed message authentication code (HMAC)</b>	Sử dụng hàm băm mật mã và mã xác thực thông điệp để đảm bảo tính toàn vẹn và tính xác thực của thông điệp.
<b>HĐ</b>	Xem hard disk drive.
<b>heating, ventilation, air conditioning (HVAC)</b>	Các hệ thống được sử dụng để sưởi ấm và làm mát không khí trong một tòa nhà hoặc một cấu trúc.
<b>HIDS</b>	Xem host-based intrusion detection system.
<b>high availability (HA)</b>	Một thiết kế hệ thống để mang lại tính sẵn sàng được đảm bảo.
<b>HIPS</b>	Xem host-based intrusion prevention system.

<b>HMAC-based one-time password (HOTP)</b>	Một phương pháp tạo ra mật khẩu dùng một lần bằng các hàm HMAC.
<b>homomorphic cryptography</b>	Một dạng hệ thống mật mã trong đó các phép toán có thể được thực hiện trực tiếp trên dữ liệu đã được mã hóa.
<b>honeypot</b>	Một hệ thống máy tính hoặc một phần của mạng đã được thiết lập để thu hút những kẻ xâm nhập tiềm năng, với hy vọng rằng chúng sẽ để yên cho các hệ thống khác. Vì không có người dùng hợp pháp nào của hệ thống này, bất kỳ nỗ lực nào để truy cập vào hệ thống đều là dấu hiệu của hoạt động trái phép và cung cấp một cơ chế dễ dàng để phát hiện các cuộc tấn công.
<b>host-based intrusion detection system (HIDS)</b>	Một hệ thống tìm kiếm sự xâm nhập vào máy tính bằng cách giám sát hoạt động trên một hoặc nhiều máy tính cá nhân hoặc máy chủ riêng lẻ.
<b>host-based intrusion prevention system (HIPS)</b>	Một hệ thống tự động ứng phó với sự xâm nhập vào máy tính bằng cách giám sát hoạt động trên một hoặc nhiều máy tính cá nhân hoặc máy chủ riêng lẻ và ứng phó dựa trên một bộ quy tắc.
<b>hot site</b>	Một địa điểm sao lưu được cấu hình đầy đủ với thiết bị và dữ liệu và sẵn sàng chấp nhận ngay việc chuyển giao quá trình vận hành trong trường hợp hệ thống vận hành bị lỗi.

<b>HSM</b>	<i>Xem hardware security module.</i>
<b>Hypertext Markup Language (HTML)</b>	Một giao thức được sử dụng để đánh dấu văn bản để sử dụng trên HTTP.
<b>Hypertext Transfer Protocol (HTTP)</b>	Một giao thức để truyền tải tài liệu qua Internet có chứa các liên kết đến tài liệu bổ sung.
<b>Hypertext Transfer Protocol over SSL/TLS (HTTPS)</b>	Một giao thức để truyền tài liệu qua Internet có chứa các liên kết đến tài liệu bổ sung được chuyển qua một đường hầm an toàn thông qua SSL hoặc TLS.
<b>I</b>	
<b>IaaS</b>	<i>Xem Infrastructure as a Service.</i>
<b>IAM</b>	<i>Xem Identity and Access Management.</i>
<b>ICMP</b>	<i>Xem Internet Control Message Protocol.</i>
<b>ICS</b>	<i>Xem industrial control system.</i>
<b>identification (ID)</b>	Bước đầu tiên trong quá trình xác thực, trong đó người dùng xác lập một bí mật với hệ thống xác thực và bị ràng buộc với ID người dùng.

<b>Identity and Access Management</b>	Các chính sách và thủ tục được sử dụng để quản lý kiểm soát truy cập.
<b>identity provider (IdP)</b>	Một hệ thống tạo ra, duy trì và quản lý thông tin nhận dạng, bao gồm cả các dịch vụ xác thực.
<b>IEEE</b>	Xem Institute of Electrical and Electronics Engineers.
<b>IETF</b>	Xem Internet Engineering Task Force.
<b>impact</b>	Kết quả của việc một lỗ hổng bị lợi dụng bởi một mối đe dọa, dẫn đến một tổn thất.
<b>impersonation</b>	Một kỹ thuật kỹ thuật xã hội có thể xảy ra trực tiếp, qua điện thoại hoặc trực tuyến, trong đó kẻ tấn công đảm nhận một vai trò được nhận ra bởi người bị tấn công và khi giả định vai trò đó, kẻ tấn công sử dụng thành kiến của nạn nhân tiềm năng để chống lại phán đoán tốt hơn của họ để tuân theo các thủ tục.
<b>incident response</b>	Quá trình ứng phó với, đóng gói, phân tích và khôi phục từ một sự cố liên-quan-đến-máy-tính.
<b>incident response plan</b>	Kế hoạch được sử dụng để ứng phó, đóng gói, phân tích và phục hồi sau một sự cố liên-quan-đến-máy-tính.

<b>indicators of compromise (IOC)</b>	Một tập hợp các giá trị, nếu được tìm thấy trong bộ nhớ hoặc bộ lưu trữ tập tin, chỉ ra một sự kiện thỏa hiệp cụ thể.
<b>industrial control system (ICS)</b>	Thuật ngữ được sử dụng để mô tả phần cứng và phần mềm điều khiển các hệ thống vật lý mạng.
<b>information security</b>	Thường được sử dụng một cách đồng nghĩa với bảo mật máy tính (computer security), nhưng tập trung vào việc bảo vệ thông tin mà hệ thống đang xử lý và lưu trữ, thay vì tập trung vào phần cứng và phần mềm cấu thành nên hệ thống.
<b>infrared (IR)</b>	Một tập hợp các bước sóng vượt qua đầu màu đỏ của dải quang phổ khả kiến, được sử dụng làm phương tiện liên lạc.
<b>Infrastructure as a Service (IaaS)</b>	Việc cung cấp tự động và theo yêu cầu về các phần tử cơ sở hạ tầng, hoạt động như một dịch vụ, một yếu tố chung của điện toán đám mây.
<b>initialization vector (IV)</b>	Một giá trị dữ liệu được sử dụng để bắt đầu một thuật toán mật mã, cung cấp một thước đo về sự ngẫu nhiên.
<b>instant messaging (Quản lý Sự cố)</b>	Một phương thức giao tiếp dựa-trên-văn-bản qua Internet.

<b>Institute of Electrical and Electronics Engineers (IEEE)</b>	Một học viện kỹ thuật, chuyên nghiệp và phi lợi nhuận liên kết với các nghiên cứu, tiêu chuẩn và hội nghị về máy tính.
<b>intangible asset</b>	Là tài sản khó hoặc không thể xác định được một giá trị tiền tệ tương đương. Các ví dụ bao gồm sự công nhận thương hiệu và thiện chí.
<b>integrity</b>	Một phần của CIA về bảo mật, nguyên tắc bảo mật yêu cầu thông tin đó không được sửa đổi ngoại trừ các cá nhân được phép làm như vậy.
<b>interconnection security agreement (ISA)</b>	Một thỏa thuận giữa các bên nhằm thiết lập các thủ tục cộng tác và phối hợp lẫn nhau giữa các bên liên quan đến các yêu cầu bảo mật liên quan đến dự án chung của họ.
<b>intermediate distribution frame (IDF)</b>	Một giá đỡ gắn-tường hoặc cố-định để quản lý và kết nối cáp viễn thông giữa các thiết bị của người-dùng-đầu-cuối và khung phân phối chính (MDF).
<b>internal segmentation firewall (ISFW)</b>	Một thiết bị tường lửa được đặt trong mạng để phân đoạn các phần của mạng.
<b>International Data Encryption Algorithm (IDEA)</b>	Một thuật toán mã hóa đối xứng được sử dụng trong nhiều hệ thống cho các dịch vụ mã hóa số lượng lớn.

<b>Internet Numbers (IANA)</b>	<b>Assigned Authority</b>	Trung tâm điều phối ấn định các giá trị tham số duy nhất cho các giao thức Internet. IANA được Hiệp hội Internet (ISOC) thuê để hoạt động như cơ quan thanh toán bù trừ để chỉ định và điều phối việc sử dụng một lượng lớn tham số giao thức Internet.
<b>Internet Message Control Protocol (ICMP)</b>	<b>Control Protocol</b>	Một trong những giao thức cốt lõi của bộ giao thức TCP/IP, được sử dụng để báo cáo lỗi và thông báo trạng thái.
<b>Internet Engineering Task Force (IETF)</b>	<b>Engineering</b>	Một cộng đồng quốc tế lớn bao gồm các nhà thiết kế, điều hành, nhà cung cấp và nhà nghiên cứu mạng quốc tế, mở cửa cho bất kỳ cá nhân quan tâm nào liên quan đến sự phát triển của kiến trúc Internet và sự vận hành trơn tru của Internet. Công việc kỹ thuật thực tế của IETF được thực hiện trong các nhóm công việc của nó, được tổ chức theo chủ đề thành một số lĩnh vực (chẳng hạn như định tuyến, truyền tải và bảo mật). Phần lớn công việc được xử lý thông qua danh sách gửi thư, với các cuộc họp được tổ chức ba lần mỗi năm.
<b>Internet Key Exchange (IKE)</b>	<b>Key Exchange</b>	Một giao thức trao đổi khóa tiêu chuẩn được sử dụng trên Internet, một triển khai của thuật toán Diffie-Hellmann.
<b>Internet Message Access Protocol version 4 (IMAP4)</b>	<b>Message Access Protocol</b>	Một trong hai giao thức chuẩn Internet phổ biến để truy xuất email (giao thức còn lại là POP3).

<b>Internet of Things (IoT)</b>	Mạng kết nối của một số lượng lớn các thiết bị thông qua Internet để đạt được một mục đích kinh doanh.
<b>Internet Protocol (IP)</b>	Giao thức lớp mạng được Internet sử dụng để định tuyến các gói tin qua mạng.
<b>Internet Protocol Security (IPSec)</b>	Một giao thức được sử dụng để bảo mật các gói IP trong quá trình truyền qua mạng. IPSec cung cấp các dịch vụ xác thực, toàn vẹn và bảo mật đồng thời sử dụng Tiêu đề Xác thực (AH) và Đóng gói Tải trọng Bảo mật (ESP) để thực hiện chức năng này.
<b>Internet Relay Chat (IRC)</b>	Một giao thức lớp ứng dụng hỗ trợ giao tiếp dưới dạng văn bản trên Internet.
<b>Internet Security Association and Key Management Protocol (ISAKMP)</b>	Một khuôn khổ giao thức để xác định cơ chế triển khai giao thức trao đổi khóa và thương lượng về một chính sách bảo mật.
<b>Internet Service Provider (ISP)</b>	Một công ty viễn thông cung cấp quyền truy cập vào Internet.
<b>intrusion detection system (IDS)</b>	Một hệ thống để xác định những hoạt động đáng ngờ, độc hại hoặc không mong muốn chỉ ra một sự vi phạm bảo mật máy tính.

<b>IOCs</b>	Xem indicators of compromise.
<b>IPSec</b>	Xem Internet Protocol Security.
<b>ISA</b>	Xem interconnection security agreement.
<b>IT contingency plan (ITCP)</b>	Kế hoạch được sử dụng để quản lý các hoạt động dự phòng trong một môi trường CNTT.
<b>K</b>	
<b>Kerberos</b>	Một giao thức xác thực mạng được MIT thiết kế để sử dụng trong môi trường máy khách/máy chủ.
<b>key</b>	Trong mã hóa, đây là một chuỗi các ký tự hoặc bit được sử dụng bởi một thuật toán để mã hóa hoặc giải mã một thông điệp.
<b>key distribution center (KDC)</b>	Một thành phần của hệ thống xác thực Kerberos quản lý việc phân phối khóa an toàn.
<b>key encrypting key (KEK)</b>	Khóa mã hóa có chức năng mã hóa và giải mã khóa mã hóa dữ liệu (data encryption key - DEK).
<b>keyspace</b>	Toàn bộ tập hợp tất cả các khóa có thể có đổi với một thuật toán mã hóa cụ thể.

**L**

<b>Layer 2 Tunneling Protocol (L2TP)</b>	Một giao thức chuyển mạch của Cisco hoạt động ở lớp liên kết dữ liệu.
<b>LDAP</b>	Xem Lightweight Directory Access Protocol.
<b>least privilege</b>	Một nguyên tắc bảo mật trong đó người dùng được cung cấp tập hợp các quyền và đặc quyền tối thiểu cần thiết để thực hiện các chức năng được yêu cầu của họ. Mục đích là hạn chế những thiệt hại tiềm ẩn mà bất kỳ người dùng nào cũng có thể gây ra.
<b>lightweight cryptography</b>	Các hệ thống mật mã được thiết kế để sử dụng trong các hệ thống công-suất-thấp, tính-toán-thấp.
<b>Lightweight Directory Access Protocol (LDAP)</b>	Một giao thức ứng dụng được sử dụng để truy cập các dịch vụ thư mục trên mạng TCP/IP.
<b>Lightweight Extensible Authentication Protocol (LEAP)</b>	Một phiên bản của EAP được phát triển bởi Cisco trước 802.11i để thúc đẩy việc áp dụng 802.1X và WEP.
<b>load balancer</b>	Một thiết bị mạng phân phối năng lực tính toán trên nhiều máy tính.

<b>local area network (LAN)</b>	Một nhóm các máy tính trong một cấu trúc mạng được giới hạn trong một khu vực giới hạn và sử dụng các giao thức cụ thể, chẳng hạn như Ethernet để định địa chỉ lưu lượng OSI Lớp 2.
<b>Local Security Authority Subsystem Service (LSASS)</b>	Tiến trình trong hệ điều hành Microsoft Windows chịu trách nhiệm cho việc thực thi chính sách bảo mật trên hệ thống.
<b>logic bomb</b>	Một dạng mã độc hoặc phần mềm được kích hoạt bởi một sự kiện hoặc điều kiện cụ thể. <i>Xem thêm</i> time bomb.
<b>loop protection</b>	Yêu cầu ngăn chặn vòng lặp cầu nối ở cấp độ Lớp 2, vốn thường được giải quyết bằng cách sử dụng thuật toán Cây Mở rộng (Spanning Tree) trên các thiết bị chuyển mạch.
<b>LSASS</b>	<i>Xem</i> Local Security Authority Subsystem Service.
<b>M</b>	
<b>MAC</b>	<i>Xem</i> mandatory access control, Media Access Control, <i>hoặc</i> message authentication code.
<b>machine learning (ML)</b>	Một dạng trí tuệ nhân tạo trong đó các thuật toán máy học tập bằng cách kiểm tra các trường hợp thử nghiệm và các giải pháp.

<b>main distribution frame (MDF)</b>	Thiết bị điện thoại để kết nối thiết bị của khách hàng với thiết bị của nhà cung cấp dịch vụ thuê bao.
<b>man-in-the-browser attack (MITB)</b>	Một cuộc tấn công người trung gian (man-in-the-middle) liên quan đến các đối tượng trợ giúp trình duyệt và các trình duyệt để tiến hành cuộc tấn công.
<b>man-in-the-middle attack (MITM)</b>	Bất kỳ cuộc tấn công nào cố gắng sử dụng một nút mạng làm trung gian giữa hai nút khác. Mỗi nút điểm cuối nghĩ rằng nó đang nói chuyện trực tiếp với nhau, nhưng mỗi nút thực sự đang nói chuyện với nút trung gian.
<b>managed security service provider (MSSP)</b>	Một bên-thứ-ba quản lý các khía cạnh bảo mật của một hệ thống theo một số hình thức thỏa thuận dịch vụ.
<b>managed service provider (MSP)</b>	Một bên-thứ-ba quản lý các khía cạnh của một hệ thống theo một số hình thức thỏa thuận dịch vụ.
<b>mandatory access control (MAC)</b>	Một cơ chế kiểm soát truy cập trong đó cơ chế bảo mật kiểm soát quyền truy cập vào tất cả các đối tượng (tập tin) và các chủ thể riêng lẻ (quy trình hoặc người dùng) không thể thay đổi quyền truy cập đó.
<b>master boot record (MBR)</b>	Một dải dữ liệu trên ổ cứng trong hệ thống Windows có nghĩa là dẫn đến các chức năng hoặc nhận dạng ban đầu cụ thể.

<b>maximum transmission unit (MTU)</b>	Là thước đo tải trọng lớn nhất mà một giao thức cụ thể có thể mang trong một gói tin trong một trường hợp cụ thể.
<b>MD5</b>	Message Digest 5, một thuật toán băm và một phương pháp cụ thể để tạo ra một thông báo thông báo.
<b>mean time between failures (MTBF)</b>	Khoảng thời gian được xác định theo thống kê giữa các lần hỏng hóc của hệ thống.
	thời gian thất bại trung bình (MTTF) Thời gian được xác định theo thống kê cho đến lần hỏng hóc tiếp theo.
<b>mean time to repair/recover (MTTR)</b>	Một thước đo phổ biến về thời gian để sửa chữa một lỗi nhất định. Đây là thời gian trung bình, và có thể có hoặc không bao gồm thời gian cần thiết để có được các bộ phận.
<b>Media Access Control (MAC)</b>	Một giao thức được sử dụng trong lớp liên kết dữ liệu để đánh địa chỉ mạng cục bộ.
<b>memorandum of agreement (MOA)</b>	Một tài liệu được thực hiện giữa hai bên để xác định một số hình thức thỏa thuận.
<b>memorandum of understanding (MOU)</b>	Một văn bản được thực hiện giữa hai bên để xác định một số hình thức thỏa thuận.

<b>message authentication code (MAC)</b>	Một đoạn dữ liệu ngắn được sử dụng để xác thực thông điệp. Xem hashed message authentication code.
<b>message digest</b>	Kết quả của việc áp dụng một hàm băm cho dữ liệu. Đôi khi còn được gọi là giá trị băm. Xem hash.
<b>Measurement Systems Analysis (MSA)</b>	Đánh giá quá trình đo lường để xác định độ nhạy và nguồn lỗi.
<b>metropolitan area network (MAN)</b>	Một tập hợp các mạng được kết nối với nhau trong một khu vực đô thị và thường được kết nối với Internet.
<b>Microsoft Challenge Handshake Authentication Protocol (MS-CHAP)</b>	Một biến thể của Giao thức xác thực bắt tay thử thách (CHAP) được Microsoft phát triển.
<b>mitigation</b>	Hành động được thực hiện để làm giảm khả năng xảy ra mối đe dọa.
<b>mobile device management (MDM)</b>	Một ứng dụng được thiết kế để cung cấp chức năng cấp-doanh-nghiệp lên thiết bị di động, bao gồm chức năng bảo mật và phân tách dữ liệu.
<b>Monitoring as a Service (MaaS)</b>	Việc sử dụng bên-thứ-ba để cung cấp dịch vụ giám sát bảo mật.

<b>MS-CHAP</b>	Xem Microsoft Challenge Handshake Authentication Protocol.
<b>MTBF</b>	Xem mean time between failures.
<b>MTTF</b>	Xem mean time to failure.
<b>MTTR</b>	Xem mean time to repair/recover.
<b>multifactor authentication (MFA)</b>	Sử dụng nhiều hơn một yếu tố khác nhau để xác thực một người dùng với một hệ thống.
<b>multifunction device (MFD)</b>	Một thiết bị, chẳng hạn như máy in, có nhiều chức năng, chẳng hạn như in và quét.
<b>Multimedia Message Service (MMS)</b>	Một cách thức tiêu chuẩn để gửi tin nhắn đa phương tiện đến và từ điện thoại di động thông qua một mạng di động.
<b>Multiprotocol Label Switching (MPLS)</b>	Một phương pháp định tuyến có tính xác định được thực hiện để xử lý hiệu quả hơn các loại lưu lượng khác nhau trên mạng WAN.
<b>N</b>	
<b>NAC</b>	Xem network access control.
<b>NAP</b>	Xem Network Access Protection

<b>NAT</b>	Xem Network Address Translation.
<b>National Institute of Standards and Technology (NIST)</b>	Một cơ quan thuộc chính phủ Hoa Kỳ chịu trách nhiệm về các tiêu chuẩn và công nghệ.
<b>NDA</b>	Xem nondisclosure agreement.
<b>near field communication (NFC)</b>	Một tập hợp các tiêu chuẩn và giao thức để thiết lập một liên kết giao tiếp trong khoảng cách rất ngắn. Được sử dụng trong các thiết bị di động.
<b>network access control (NAC)</b>	Một phương pháp tiếp cận bảo mật điểm đầu cuối liên quan đến việc giám sát và khắc phục các vấn đề bảo mật điểm đầu cuối trước khi cho phép một đối tượng kết nối với mạng.
<b>Network Access Protection (NAP)</b>	Một phương pháp tiếp cận của Microsoft để kiểm soát truy cập mạng.
<b>Network Address Translation (NAT)</b>	Một phương pháp đánh địa chỉ lại các gói tin trong mạng tại một điểm cửa ngõ để cho phép sử dụng các địa chỉ IP cục bộ và không thể định tuyến qua một mạng công cộng như Internet.

<b>network-based intrusion detection system (NIDS)</b>	Một hệ thống kiểm tra lưu lượng mạng để xác định những hành vi đáng ngờ, độc hại hoặc không mong muốn.
<b>network-based intrusion prevention system (NIPS)</b>	Một hệ thống kiểm tra lưu lượng mạng và tự động ứng phó với các xâm nhập vào máy tính.
<b>Network Basic Input/Output System (NetBIOS)</b>	Một hệ thống cung cấp các dịch vụ truyền thông qua một mạng cục bộ.
<b>network function virtualization (NFV)</b>	Sử dụng các công nghệ ảo hóa để ảo hóa cơ sở hạ tầng mạng.
<b>network operating system (NOS)</b>	Hệ điều hành bao gồm các chức năng và năng lực bổ sung để hỗ trợ cho việc kết nối máy tính và thiết bị, chẳng hạn như máy in, với mạng cục bộ.
<b>Network Time Protocol (NTP)</b>	Một giao thức để truyền các gói đồng bộ hóa thời gian qua một mạng.
<b>New Technology File System (NTFS)</b>	Hệ thống tập tin độc quyền do Microsoft phát triển, được giới thiệu vào năm 1993, hỗ trợ nhiều hoạt động tập tin trên máy chủ, máy tính cá nhân và phương tiện.

<b>New Technology LANMAN (NTLM)</b>	Một bộ bảo mật không còn được sử dụng nữa của Microsoft cung cấp tính năng xác thực, tính toàn vẹn và tính bảo mật cho người dùng. Bởi vì nó không hỗ trợ các phương pháp mã hóa hiện tại nên nó không còn được khuyến khích sử dụng.
<b>next-generation access control (NGAC)</b>	Một trong những phương pháp chính để triển khai kiểm soát truy cập dựa trên thuộc tính (ABAC). Phương pháp khác là XACML.
<b>next-generation firewall (NGFW)</b>	Một tường lửa được lập trình để sử dụng các cấp cao hơn của thông điệp thay vì chỉ có các địa chỉ và cổng để đưa ra quyết định.
<b>next-generation secure web gateway (NG-SWG)</b>	Một giải pháp được thiết kế để lọc lưu lượng truy cập web không mong muốn khỏi phiên được người-dùng-khởi-tạo để thực thi tuân thủ chính sách.
<b>NFC</b>	Xem near field communication.
<b>NFV</b>	Xem network function virtualization.
<b>NIST</b>	Xem National Institute of Standards and Technology.
<b>nondisclosure agreement (NDA)</b>	Một hợp đồng pháp lý giữa các bên nêu rõ chi tiết các hạn chế và yêu cầu mà mỗi bên phải chịu đối với các vấn đề bảo mật liên quan đến thông tin được chia sẻ.

<b>nonrepudiation</b>	Khả năng xác minh rằng một hoạt động đã được thực hiện bởi một người hoặc tài khoản cụ thể. Đây là thuộc tính hệ thống để ngăn chặn các bên tham gia giao dịch sau đó từ chối việc tham gia vào giao dịch.
<b>O</b>	
<b>Oakley protocol</b>	Một giao thức trao đổi khóa xác định cách lấy được tài liệu khóa đã được xác thực dựa trên thuật toán trao đổi khóa Diffie-Hellman.
<b>object identifier (OID)</b>	Một cơ chế định danh được chuẩn hóa để đặt tên cho bất kỳ đối tượng nào.
<b>object reuse</b>	Gán một phương tiện đã sử dụng trước đó cho một chủ thẻ. Hàm ý bảo mật là rằng trước khi nó được cung cấp cho chủ thẻ, bất kỳ dữ liệu nào có từ người dùng trước đó đều phải bị xóa bỏ.
<b>On-the-Go (OTG)</b>	Xem Universal Serial Bus (USB) On-The-Go (OTG).
<b>one-time-pad (OTP)</b>	Một lược đồ mã hóa không thể phá vỡ trong đó một loạt các bit ngẫu nhiên, không lặp lại được sử dụng một lần làm khóa để mã hóa một thông điệp. Vì mỗi pad chỉ được sử dụng một lần nên không có hình mẫu nào có thể được thiết lập và các kỹ thuật phân tích mật mã truyền thống sẽ không có hiệu quả.
<b>Online Certificate Status Protocol (OCSP)</b>	Một giao thức được sử dụng để yêu cầu trạng thái thu hồi của một chứng chỉ số. Đây là một giải pháp thay thế cho danh sách thu hồi chứng chỉ.

<b>Open Authorization (OAuth)</b>	Một tiêu chuẩn mở để xác thực và ủy quyền dựa-trên-mã-thông-báo (token-based) trên Internet.
<b>open source intelligence (OSINT)</b>	Thông tin bảo mật có nguồn gốc từ các nguồn sẵn có cho công chúng.
<b>Open Vulnerability and Assessment Language (OVAL)</b>	Một tiêu chuẩn dựa-trên-XML để truyền thông tin bảo mật giữa các công cụ và dịch vụ.
<b>Open Web Application Security Project (OWASP)</b>	Một tổ chức phi lợi nhuận chuyên biệt để cải thiện tính bảo mật trong các ứng dụng web.
<b>operating system (OS)</b>	Phần mềm cơ bản xử lý đầu vào, đầu ra, hiển thị, quản lý bộ nhớ và tất cả các tác vụ rất chi tiết khác được yêu cầu để hỗ trợ cho môi trường người dùng và các ứng dụng liên quan.
<b>operational technology (OT)</b>	Tên gọi của một hệ thống CNTT được sử dụng trong môi trường công nghiệp để kiểm soát các tiến trình vật lý.
<b>OVAL</b>	Xem Open Vulnerability and Assessment Language.
<b>over the air (OTA)</b>	Đề cập đến việc thực hiện một hành động không dây.

## P

<b>P12</b>	Xem PKCS # 12.
<b>PAC</b>	Xem Proxy Auto-Configuration.
<b>Packet Capture (PCAP)</b>	Các phương pháp và tập tin liên quan đến việc ghi nhận lưu lượng mạng ở dạng tập tin văn bản.
<b>Padding Oracle on Downgraded Legacy Encryption (POODLE)</b>	Một lỗ hổng trong SSL 3.0 có thể bị khai thác.
<b>PAM</b>	Xem Pluggable Authentication Modules.
<b>pan-tilt-zoom (PTZ)</b>	Một thuật ngữ được sử dụng để mô tả một máy quay video hỗ trợ điều khiển thu phóng và điều hướng từ xa.
<b>pass-the-hash attack</b>	Một cuộc tấn công trong đó thông tin xác thực được chuyển ở dạng băm để thuyết phục một đối tượng rằng quyền hạn đã được cấp.
<b>password</b>	Một chuỗi ký tự được sử dụng để chứng minh danh tính của một cá nhân đối với một hệ thống hoặc đối tượng. Được sử dụng cùng với ID người dùng, đây là phương

	pháp xác thực phổ biến nhất. Mật khẩu nên được giữ bí mật bởi cá nhân sở hữu nó.
<b>Password Authentication Protocol (PAP)</b>	Một giao thức đơn giản được sử dụng để xác thực người dùng với máy chủ truy cập mạng.
<b>Password-Based Key Derivation Function 2 (PBKDF2)</b>	Một chức năng trích xuất khóa là một phần của Tiêu chuẩn Mã hóa Khóa Công khai (RSA Laboratories Public Key Cryptography Standards) của Phòng thí nghiệm RSA, được xuất bản dưới tên IETF RFC 2898.
<b>patch</b>	Một bộ mã [phần mềm] thay thế được thiết kế để khắc phục các sự cố hoặc lỗ hổng trong phần mềm hiện có.
<b>Payment Card Industry Data Security Standard (PCI DSS)</b>	Một tiêu chuẩn bảo mật dữ liệu theo hợp đồng được khởi xướng bởi ngành thẻ tín dụng để bảo vệ dữ liệu của chủ thẻ.
<b>PBX</b>	Xem private branch exchange.
<b>peer-to-peer (P2P)</b>	Một phương pháp kết nối mạng liên quan đến kết nối trực tiếp từ mạng ngang hàng.
<b>penetration testing</b>	Một kiểm tra bảo mật trong đó một nỗ lực được thực hiện để phá vỡ các biện pháp kiểm soát bảo mật nhằm phát hiện ra các lỗ hổng và điểm yếu. Còn gọi là pen test.

<b>perfect forward security (PFS)</b>	Một thuộc tính của hệ thống mã hóa, theo đó việc mất một khóa không ảnh hưởng đến tài liệu được mã hóa trước hoặc sau khi sử dụng.
<b>permissions</b>	Các hành động được phép mà một chủ thể có thể thực hiện trên một đối tượng. <i>Xem thêm access control.</i>
<b>personal electronic device (PED)</b>	Một thuật ngữ được sử dụng để mô tả một thiết bị điện tử thuộc sở hữu của người dùng và được đưa vào doanh nghiệp, sử dụng dữ liệu doanh nghiệp. Điều này bao gồm máy tính xách tay, máy tính bảng và điện thoại di động.
<b>personal health information (PHI)</b>	Thông tin liên quan đến hồ sơ y tế của một người, bao gồm dữ liệu tài chính, nhận dạng và y tế.
<b>personal identification number (PIN)</b>	Một số bí mật, chỉ người dùng mới biết để xác lập danh tính.
<b>Personal Identity Verification (PIV)</b>	Các chính sách, quy trình, phần cứng và phần mềm được sử dụng để xác định danh tính nhân viên liên bang một cách an toàn.
<b>personal identifiable information (PII)</b>	Thông tin có thể được sử dụng để nhận dạng một người.
<b>personal information exchange format (PFX)</b>	Một định dạng tập tin được sử dụng khi xuất chứng chỉ. Còn được gọi là PKCS #12.

<b>phreaking</b>	Được sử dụng trong các phương tiện truyền thông để chỉ việc tấn công hệ thống máy tính và mạng có liên quan đến công ty điện thoại. <i>Xem thêm</i> bẻ khóa (cracking).
<b>PKCS # 12</b>	Một thành viên thường được sử dụng của họ các tiêu chuẩn được gọi là Tiêu chuẩn Mã hóa Khóa Công khai (PKCS), được công bố bởi Phòng thí nghiệm RSA.
<b>plain old telephone service</b>	Thuật ngữ được sử dụng để mô tả dịch vụ điện thoại analog cũ và sau này là dịch vụ điện thoại kỹ thuật số "đường-dây-cố-định (land-line)".
<b>plaintext</b>	Trong mã hóa, đây là một phần dữ liệu không được mã hóa. Nó cũng có thể có nghĩa là dữ liệu đầu vào đi vào một thuật toán mã hóa sẽ xuất ra kết quả là văn bản mã hóa.
<b>Platform as a Service (PaaS)</b>	Một dịch vụ của bên-thứ-ba cho phép khách hàng xây dựng, vận hành và quản lý các ứng dụng mà không cần phải quản lý cơ sở hạ tầng bên dưới.
<b>Pluggable Authentication Modules (PAM)</b>	Một cơ chế được sử dụng trong các hệ thống Linux để tích hợp các phương pháp xác thực cấp thấp vào một API.
<b>Point-to-Point Protocol (PPP)</b>	Tiêu chuẩn Internet để truyền các gói tin IP qua đường dây tuần tự, như trong kết nối quay số tới ISP.

<b>Poин-to-Point Protocol Extensible Authentication Protocol (PPP EAP)</b>	Một phần mở rộng của PPP cung cấp hỗ trợ cho các phương pháp xác thực bổ sung trong PPP.
<b>Poин-to-Point Protocol Password Authentication Protocol (PPP PAP)</b>	Một phần mở rộng của PPP cung cấp hỗ trợ cho các phương pháp xác thực mật khẩu qua PPP.
<b>Poин-to-Point Tunneling Protocol (PPTP)</b>	Sử dụng đóng gói định tuyến chung qua PPP để tạo ra một phương pháp luận được sử dụng cho mạng riêng ảo.
<b>Port Address Translation (PAT)</b>	Thao tác thông tin cổng trong một lược đồ dữ liệu IP tại một điểm trong mạng để ánh xạ các cổng theo cách tương tự như việc thay đổi địa chỉ mạng của Biên dịch Địa chỉ Mạng (Network Address Translation).
<b>Post Office Protocol (POP)</b>	Một định dạng được tiêu chuẩn hóa để trao đổi email.
<b>potentially unwanted program (PUP)</b>	Một chương trình phần mềm mà bạn có thể không muốn cài đặt trên máy tính của mình. PUP thường gặp trong các hệ thống được đóng gói.

<b>power distribution unit (PDU)</b>	Một hệ thống để quản lý phân phối điện cho nhiều thành phần, giống như trong một hệ thống giá đỡ (rack mount).
<b>pre-shared key (PSK)</b>	Một bí mật được chia sẻ trước đây đã từng được chia sẻ giữa các bên và được sử dụng để thiết lập một kênh an toàn.
<b>Pretty Good Privacy (PGP)</b>	Một chương trình mã hóa phổ biến có khả năng mã hóa và ký điện tử và các tập tin.
<b>preventative intrusion detection</b>	Một hệ thống phát hiện các hành động thù địch hoặc các hoạt động mạng và ngăn chặn chúng gây tác động đến hệ thống thông tin.
<b>privacy</b>	Bảo vệ những thông tin cá nhân của một cá nhân khỏi những người không được phép xem thông tin đó.
<b>Privacy-enhanced Electronic Mail (PEM)</b>	Tiêu chuẩn Internet đem đến cho việc trao đổi thư điện tử một cách an toàn bằng cách sử dụng các chức năng mật mã.
<b>private branch exchange</b>	Một tổng đài điện thoại phục vụ một doanh nghiệp hoặc tổ chức cụ thể.
<b>privilege auditing</b>	Quá trình kiểm tra các quyền và đặc quyền đã được gán cho một tài khoản hoặc nhóm tài khoản cụ thể.

<b>privilege escalation</b>	Bước này thuộc về một cuộc tấn công mà kẻ tấn công tăng đặc quyền của họ, tốt hơn là lên đến cấp quản trị viên hoặc cấp root.
<b>privilege management</b>	Quá trình hạn chế khả năng tương tác của người dùng với hệ thống máy tính.
<b>Protected Extensible Authentication Protocol (PEAP)</b>	Một phiên bản được bảo vệ của EAP được phát triển bởi Cisco, Microsoft và RSA Security hoạt động bằng cách đóng gói các khung EAP trong một đường hầm TLS.
<b>Proxy Auto-Configuration (PAC)</b>	Một phương pháp về việc tự động kết nối trình duyệt web với các dịch vụ proxy thích hợp để truy xuất một URL cụ thể.
<b>PSK</b>	Xem pre-shared key.
<b>PTZ</b>	Xem pan-tilt-zoom.
<b>public key cryptography</b>	Xem asymmetric encryption.
<b>Public Key Cryptography Standards (PKCS)</b>	Một loạt các tiêu chuẩn bao gồm các khía cạnh của việc triển khai mã hóa khóa công khai.
<b>Public Key Infrastructure (PKI)</b>	Cơ sở hạ tầng để ràng buộc khóa công khai với một người dùng đã biết thông qua một trung gian đáng tin cậy, thường là cơ quan cấp chứng chỉ.

<b>PUP</b>	<i>Xem potentially unwanted program.</i>
<b>Q</b>	
<b>qualitative assessment</b>	<b>risk</b> Quá trình xác định một cách chủ quan tác động của một sự kiện gây ảnh hưởng đến một dự án, chương trình hoặc doanh nghiệp. Nó liên quan đến việc sử dụng đánh giá của chuyên gia, kinh nghiệm hoặc sự đồng thuận của nhóm để hoàn thành đánh giá.
<b>Quality of Service (QoS)</b>	Chất lượng dịch vụ (QoS) Việc sử dụng công nghệ để quản lý lưu lượng dữ liệu, giảm mất gói và kiểm soát độ trễ và chập chờn trên mạng.
<b>quantitative assessment</b>	<b>risk</b> Quá trình xác định một cách khách quan tác động của một sự kiện có ảnh hưởng đến dự án, chương trình hoặc doanh nghiệp. Nó thường liên quan đến việc sử dụng các thước đo và mô hình để hoàn thành đánh giá.
<b>R</b>	
<b>RADIUS</b>	Dịch vụ Người dùng Quay-số Xác thực Từ xa (Remote Authentication Dial-In User Service) Một giao thức tiêu chuẩn để cung cấp các dịch vụ xác thực thường được sử dụng trong các môi trường quay số, không dây và PPP.
<b>RAID</b>	<i>Xem Redundant Array of Inexpensive Disks.</i>

<b>rainbow table</b>	Một bộ các bảng băm được tính toán trước để đổi sánh mật khẩu bằng cách tìm kiếm thay vì tính toán nhanh từng bảng.
<b>rapid application development (RAD)</b>	Một phương pháp luận phát triển phần mềm ủng hộ việc sử dụng các nguyên mẫu và thay đổi nhanh chóng thay vì lập kế hoạch toàn diện.
<b>RAS</b>	<i>Xem</i> Remote-Access Service/Server.
<b>RAT</b>	<i>Xem</i> Remote-Access Trojan.
<b>RBAC</b>	<i>Xem</i> rule-based access control <i>hoặc</i> role-based access control.
<b>RC4</b>	Một luồng mật mã được sử dụng trong TLS và WEP.
<b>real-time operating system (RTOS)</b>	Hệ điều hành được thiết kế để hoạt động trong môi trường thời-gian-thực.
<b>Real-time Transport Protocol (RTP)</b>	Một giao thức dành cho một định dạng gói tin được tiêu chuẩn hóa được sử dụng để truyền lưu lượng âm thanh và hình ảnh qua mạng IP.
<b>Recovery Agent (RA)</b>	Trong môi trường Microsoft Windows, đây là thực thể được hệ thống ủy quyền sử dụng chứng chỉ khôi phục khóa công khai để giải mã tập tin của người dùng khác bằng chức năng khóa riêng tư đặc biệt được liên kết với Hệ thống Tập tin được Mã hóa (EFS).

<b>recovery point objective (RPO)</b>	Lượng dữ liệu mà một doanh nghiệp sẵn sàng chịu rủi ro. Nó được xác định bằng khoảng thời gian doanh nghiệp có để khôi phục lại quy trình trước khi lượng dữ liệu không thể chấp nhận được bị mất do gián đoạn.
<b>recovery time objective (RTO)</b>	Khoảng thời gian doanh nghiệp phải khôi phục lại quy trình trước khi có kết quả không thể chấp nhận được do gián đoạn.
<b>Redundant Array of Inexpensive Disks (RAID)</b>	Sử dụng một mảng đĩa được sắp xếp trong một đơn vị lưu trữ duy nhất để gia tăng dung lượng lưu trữ, khả năng dự phòng và các đặc tính hiệu suất.
<b>refactoring</b>	Quá trình tái cấu trúc mã máy tính hiện có mà không thay đổi hành vi bên ngoài của nó để cải thiện các thuộc tính phi chức năng của phần mềm, chẳng hạn như cải thiện khả năng đọc mã và/hoặc giảm độ phức tạp.
<b>registration authority (RA)</b>	Một phần của hệ thống PKI chịu trách nhiệm cho việc thiết lập các thông số đăng ký trong quá trình tạo ra một chứng chỉ.
<b>Remote-Access Service/Server (RAS)</b>	Đây là sự kết hợp giữa phần cứng và phần mềm được sử dụng để cho phép truy cập từ xa vào mạng.
<b>Remote-Access Trojan (RAT)</b>	Một tập hợp các phần mềm độc hại được thiết kế để khai thác một hệ thống cung cấp quyền truy cập từ xa.

<b>remotely triggered black hole (RTBH)</b>	Một kỹ thuật lọc phổ biến và hiệu quả để giảm thiểu các cuộc tấn công từ chối dịch vụ.
<b>replay attack</b>	Việc sử dụng lại dữ liệu trong một cuộc tấn công để khiến hệ thống phản hồi dựa trên các hành vi trước đó.
<b>repudiation</b>	Hành động từ chối rằng một thông điệp đã được gửi hoặc nhận.
<b>residual risk</b>	Rủi ro còn lại sau một lần lặp lại tiến trình quản lý rủi ro.
<b>return on investment (ROI)</b>	Thước đo hiệu quả của việc sử dụng vốn [đầu t].
<b>RFID</b>	Nhận dạng tần số vô tuyến (radio frequency identification). Một công nghệ được sử dụng để nhận dạng từ xa qua sóng vô tuyến.
<b>RIPEMD</b>	Một hàm băm được phát triển ở Bỉ. Từ viết tắt mở rộng thành Thông báo Đánh giá tính Toàn vẹn Nguyên thủy RACE (RACE Integrity Primitives Evaluation Message Digest), nhưng tên này hiếm khi được sử dụng. Phiên bản hiện tại là RIPEMD-160.
<b>risk</b>	Khả năng phải chịu tổn thất.

<b>risk assessment or risk analysis</b>	Quá trình phân tích môi trường để xác định các mối đe dọa, lỗ hổng và các hành động giảm thiểu nhằm xác định (cả về mặt định lượng hoặc định tính) tác động của một sự kiện ảnh hưởng đến dự án, chương trình hoặc doanh nghiệp.
<b>risk management</b>	Quá trình đưa-ra-quyết-định tổng thể nhằm xác định các mối đe dọa và lỗ hổng và các tác động tiềm tàng của chúng, xác định chi phí để giảm thiểu những sự kiện đó và quyết định những hành động hiệu quả về chi phí có thể được thực hiện để kiểm soát những rủi ro này.
<b>Rivest, Shamir, Adleman (RSA)</b>	Tên của ba người đã phát triển hệ thống mật mã khóa công khai và tên gọi của công ty mà họ thành lập để thương mại hóa hệ thống.
<b>role-based acces control (RBAC)</b>	Một cơ chế kiểm soát truy cập thay vì người dùng được chỉ định các quyền truy cập cụ thể cho các đối tượng được liên kết với hệ thống máy tính hoặc mạng, một tập hợp các vai trò mà người dùng có thể thực hiện được chỉ định cho từng người dùng.
<b>RTP</b>	Xem Real-time Transport Protocol.
<b>rule-based access control (RBAC)</b>	Một cơ chế kiểm soát truy cập dựa trên các quy tắc.
<b>S</b>	
<b>S/MIME</b>	Xem Secure/Multipurpose Internet Mail Extensions.

<b>SaaS</b>	<i>Xem Software as a Service.</i>
<b>safeguard</b>	<i>Xem security controls.</i>
<b>SAML</b>	<i>Xem Security Assertion Markup Language.</i>
<b>SAN</b>	<i>Xem storage area network.</i>
<b>SCADA</b>	<i>Xem supervisory control and data acquisition.</i>
<b>SCEP</b>	<i>Xem Simple Certificate Enrollment Protocol.</i>
<b>SDK</b>	<i>Xem software development kit.</i>
<b>SDLC</b>	<i>Xem software development lifecycle.</i>
<b>SDLM</b>	<i>Xem software development lifecycle methodology.</i>
<b>SDN</b>	<i>Xem software-defined networking.</i>
<b>SDP</b>	<i>Xem Service Delivery Platform.</i>
<b>SDV</b>	<i>Xem Software-Defined Visibility.</i>

<b>Secure Copy Protocol (SCP)</b>	Một giao thức mạng hỗ trợ truyền tải tập tin an toàn.
<b>Secure FTP</b>	Một phương pháp truyền tải tập tin an toàn liên quan đến đường hầm của FTP thông qua kết nối SSH. Điều này khác với SFTP, là Giao thức Truyền tải Tập tin Shell An toàn (Secure Shell File Transfer Protocol).
<b>Secure Hash Algorithm (SHA)</b>	Một thuật toán băm được sử dụng để băm dữ liệu khối. Phiên bản đầu tiên là SHA-1, với các phiên bản tiếp theo nêu chi tiết độ dài thông báo băm: SHA-256, SHA-384 và SHA-512.
<b>Secure Hypertext Transfer Protocol (SHTTP)</b>	Một giải pháp thay thế cho HTTPS trong đó chỉ các trang được truyền và trường POST mới được mã hóa. Nhìn chung, cuộc tranh luận được đưa ra bởi việc áp dụng rộng rãi HTTPS.
<b>Secure/Multipurpose Internet Mail Extensions (S/MIME)</b>	Một triển khai được mã hóa của đặc tả giao thức MIME.
<b>Secure Real-time Transport Protocol (SRTP)</b>	Một phiên bản an toàn của giao thức tiêu chuẩn dành cho một định dạng gói tin được tiêu chuẩn hóa được sử dụng để truyền lưu lượng âm thanh và hình ảnh qua mạng IP.

<b>Secure Shell (SSH)</b>	Một tập hợp các giao thức để thiết lập kết nối từ xa an toàn với máy tính. Giao thức này yêu cầu một ứng dụng khách trên mỗi đầu của kết nối và có thể sử dụng nhiều giao thức mã hóa khác nhau.
<b>Secure Shell File Transfer Protocol (SFTP)</b>	Một hệ thống con truyền tải tập tin an toàn được liên kết với Secure Shell (SSH).
<b>Secure Sockets Layer (SSL)</b>	Lớp mã hóa giữa lớp phiên và lớp truyền tải của mô hình OSI được thiết kế để mã hóa phía trên lớp truyền tải, cho phép các phiên bảo mật giữa các máy chủ. SSL đã được thay thế bằng TLS.
<b>secure web gateway (SWG)</b>	Xem next-generation secure web gateway.
<b>Secure Assertion Markup Language (SAML)</b>	Một tiêu chuẩn dựa trên XML để trao đổi dữ liệu xác thực và ủy quyền.
<b>security association (SA)</b>	Một ví dụ về chính sách bảo mật và tài liệu khóa được áp dụng cho một luồng dữ liệu cụ thể. Cả IKE và IPSec đều sử dụng SA, mặc dù các SA này độc lập với nhau. IPSec SA là một chiều và là duy nhất trong mỗi giao thức bảo mật, trong khi IKE SA là hai chiều. Một tập hợp các SA là cần thiết cho một đường ống dữ liệu được

	bảo vệ, một SA cho mỗi giao thức. SA được xác định duy nhất bởi địa chỉ đích (điểm đầu cuối IPSec), giao thức bảo mật (AH hoặc ESP) và chỉ số tham số bảo mật (SPI).
<b>security baseline</b>	Kết quả cuối cùng của quá trình thiết lập trạng thái bảo mật của hệ thống thông tin. Nó là một cấu hình tốt-đã-được-biết (known-good configuration) có khả năng chống lại các cuộc tấn công và đánh cắp thông tin.
<b>Security Automation Protocol (SCAP)</b>	Một phương pháp sử dụng các giao thức cụ thể và trao đổi dữ liệu để tự động hóa việc xác định quản lý lỗ hổng bảo mật, đo lường và tuân thủ chính sách trên một hệ thống hoặc tập hợp các hệ thống.
<b>security controls</b>	Một nhóm các chính sách và thủ tục kỹ thuật, quản lý hoặc vận hành được thiết kế để triển khai chức năng bảo mật cụ thể. Kiểm soát truy cập là một ví dụ về kiểm soát an ninh.
<b>security information and event management (SIEM)</b>	Tên gọi được sử dụng cho một loạt các giải pháp công nghệ để thu thập và phân tích thông tin liên-quan-đến-bảo-mật trong toàn doanh nghiệp.
<b>security operations center (SOC)</b>	Nhóm các hoạt động an ninh trong một doanh nghiệp.

<b>security orchestration, automation, response (SOAR)</b>	Một hệ thống được thiết kế để tạo điều kiện thuận lợi cho các biện pháp ứng phó trong các tình huống ứng phó sự cố.
<b>segregation or seperation of duties</b>	Một biện pháp kiểm soát cơ bản nhằm ngăn ngừa hoặc phát hiện các sai sót và bất thường bằng cách phân công trách nhiệm công việc đối với các nhiệm vụ rủi ro gia tăng cho các cá nhân khác nhau sao cho không một cá nhân nào có thể thực hiện các hành động gian lận hoặc độc hại.
<b>self-encrypting drive (SED)</b>	Là ổ dữ liệu có khả năng mã hóa tích hợp trên chính bộ điều khiển đĩa.
<b>Sender Policy Framework (SPF)</b>	Hệ thống xác thực email được thiết kế để phát hiện giả mạo email bằng cách xác minh rằng thư đến được gửi từ máy chủ được quản trị viên của miền đó ủy quyền.
<b>Server Message Block (SMB)</b>	Giao thức tiêu chuẩn Internet được Microsoft Windows sử dụng để chia sẻ tập tin, máy in và cổng nối tiếp.
<b>Service Delivery Platform (SDP)</b>	Một tập hợp các thành phần cung cấp một kiến trúc cung cấp dịch vụ (tạo dịch vụ, điều khiển phiên và các giao thức) cho một dịch vụ được chuyển giao cho khách hàng hoặc hệ thống khác.

<b>service level agreement (SLA)</b>	Một thỏa thuận giữa các bên liên quan đến thời gian hoạt động dự kiến hoặc theo hợp đồng liên quan đến một hệ thống.
<b>Service Set Identifier (SSID)</b>	Xác định một mạng không dây 802.11 cụ thể. Nó truyền thông tin về điểm truy cập cho những máy khách không dây đang kết nối.
<b>session hijacking</b>	Một cuộc tấn công chống lại một phiên giao tiếp bằng cách chèn các gói vào giữa phiên giao tiếp.
<b>shielded twisted pair (STP)</b>	Một kết nối mạng vật lý bao gồm hai dây xoắn và được bọc bằng một lớp bảo vệ chắn để ngăn nhiễu.
<b>shimming</b>	Quá trình đặt một lớp mã phần mềm giữa trình điều khiển và hệ điều hành để cho phép tính linh hoạt và tính di động.
<b>Short Message Service (SMS)</b>	Một hình thức nhắn tin văn bản qua các mạch điện thoại và điện thoại di động cho phép gửi các tin nhắn dài tới 160-ký-tự qua các kênh tín hiệu.
<b>shoulder surfing</b>	Đánh cắp thông tin đăng nhập bằng cách nhìn qua vai ai đó trong khi họ đang nhập chúng vào hệ thống.
<b>signature database</b>	Một tập hợp các hình mẫu hoạt động đã được xác định và phân loại và thường chỉ ra hoạt động đáng ngờ hoặc độc hại.

<b>SIM</b>	Xem Subscriber Identity Module.
<b>Simple Certificate Enrollment Protocol (SCEP)</b>	Một giao thức được sử dụng trong PKI để đăng ký và các dịch vụ khác.
<b>Simple Mail Transfer Protocol (SMTP)</b>	Giao thức Internet tiêu chuẩn được sử dụng để truyền email giữa các máy chủ.
<b>Simple Mail Transfer Protocol Secure (SMTPS)</b>	Phiên bản bảo mật của giao thức Internet tiêu chuẩn được sử dụng để truyền email giữa các máy chủ.
<b>Simple Network Management Protocol (SNMP)</b>	Một giao thức tiêu chuẩn được sử dụng để quản lý từ xa các thiết bị mạng trên một hệ thống mạng.
<b>Simple Object Access Protocol (SOAP)</b>	Một đặc tả thông số kỹ thuật dựa-trên-XML để trao đổi thông tin được liên kết với các dịch vụ web.
<b>single loss expectancy (SLE)</b>	Tổn thất hoặc tác động bằng tiền của mỗi lần xảy ra một mối đe dọa. SLE = giá trị tài sản × hệ số tiếp xúc.

<b>single point of failure (SPoF)</b>	Một thành phần hệ thống đơn lẻ bị lỗi có thể dẫn đến lỗi hệ thống.
<b>single sign-on (SSO)</b>	Một quy trình xác thực, theo đó người dùng có thể nhập một ID người dùng và mật khẩu, sau đó chuyển từ ứng dụng này sang ứng dụng khác hoặc tài nguyên này sang tài nguyên khác mà không cần phải cung cấp thêm thông tin xác thực.
<b>slack space</b>	Không gian chưa được sử dụng trên ổ đĩa được tạo ra khi tập tin nhỏ hơn đơn vị lưu trữ được cấp phát (chẳng hạn như sector).
<b>Small Computer System Interface (SCSI)</b>	Một giao thức để truyền dữ liệu đến và đi từ một máy.
<b>SMB</b>	Xem Server Message Block.
<b>SMS</b>	Xem Short Message Service.
<b>sniffer</b>	Một phần mềm hoặc thiết bị phần cứng được sử dụng để quan sát lưu lượng mạng khi nó đi qua mạng trên một phương tiện quảng bá được chia sẻ.
<b>SOAR</b>	Xem security orchestration, automation, and response.
<b>SOC</b>	Xem security operations center.

<b>SoC</b>	Xem system on a chip.
<b>social engineering</b>	Nghệ thuật đánh lừa người khác để người đó tiết lộ thông tin bí mật. Điều này thường được thực hiện bằng cách đóng giả là một cá nhân có quyền được tiếp cận thông tin.
<b>Software as a Service (SaaS)</b>	Việc cung cấp phần mềm như một dịch vụ, thường được gọi là phần mềm theo yêu cầu.
<b>software-defined network (SDN)</b>	Sử dụng phần mềm để hoạt động như một lớp điều khiển tách biệt với lớp dữ liệu trong mạng để quản lý lưu lượng.
<b>Software-Defined Visibility (SDV)</b>	Một khuôn khổ cho phép khả năng hiển thị vào các hoạt động và chức năng mạng.
<b>software development kit (SKD)</b>	Một tập hợp các công cụ và quy trình được sử dụng để tương tác với phần tử hệ thống lớn hơn khi việc lập trình làm thay đổi môi trường.
<b>software development lifecycle (SDLC)</b>	Các quy trình và thủ tục được sử dụng để phát triển phần mềm.
<b>software development methodology (SDLM)</b>	Các quy trình và thủ tục được sử dụng để phát triển phần mềm. Đôi khi còn được gọi là <i>mô hình vòng đời phát triển [phần mềm] an toàn</i> khi bảo mật là một phần của quá trình phát triển.

<b>solid-state drive (SSD)</b>	Một thiết bị lưu trữ chung, chẳng hạn như ổ cứng, cấu thành từ bộ nhớ điện tử chứ không phải thiết bị vật lý bao gồm các đĩa quay.
<b>SONET</b>	<i>Xem Synchronous Optical Network Technology.</i>
<b>spam</b>	Thư điện tử không được yêu cầu bởi người nhận và thường có tính chất thương mại. Còn được gọi là email thương mại không mong muốn (unsolicited commercial email - UCE).
<b>spam filter</b>	Một công cụ bảo mật được thiết kế để loại bỏ thư rác ở lớp mạng trước khi nó đi vào máy chủ email.
<b>spear phishing</b>	Một cuộc tấn công lừa đảo nhắm vào một cá nhân cụ thể.
<b>spim</b>	Thư rác được gửi qua một kênh nhắn tin tức thời.
<b>spoofing</b>	Làm cho dữ liệu trông có vẻ như có nguồn gốc từ một nguồn khác để che giấu nguồn gốc thực sự với người nhận.
<b>SSD</b>	<i>Xem solid-state drive.</i>
<b>SSID</b>	<i>Xem Service Set Identifier.</i>
<b>SSL</b>	<i>Xem Secure Sockets Layer.</i>

<b>SSO</b>	Xem single sign-on.
<b>storage area network</b>	Một mạng chuyên dụng cung cấp quyền truy cập vào khu vực lưu trữ dữ liệu.
<b>STP</b>	Xem shielded twisted pair.
<b>Structured Exception Handler (SHE)</b>	Quy trình được sử dụng để xử lý các ngoại lệ trong các chức năng cốt lõi của Hệ điều hành Windows.
<b>Structured Query Language (SQL)</b>	Một ngôn ngữ được sử dụng trong các truy vấn cơ sở dữ liệu quan hệ.
<b>Structured Query Language Injection (SQLi)</b>	Một cuộc tấn công chống lại một giao diện sử dụng SQL.
<b>Structured Information Exchange Threat Exchange (STIX)</b>	Một khuôn khổ để truyền tải thông tin về mối đe dọa qua các giao diện tự động.
<b>Subject Alternative Name (SAN)</b>	Một trường trên một chứng chỉ xác định các tên thay thế cho thực thể mà chứng chỉ đang áp dụng.

<b>Subscriber Identity Module (SIM)</b>	Một mạch tích hợp hoặc thành phần phần cứng để lưu trữ an toàn Nhận dạng Thuê bao Di động Quốc tế (International Mobile Subscriber Identity - IMSI) và khóa liên quan được sử dụng để nhận dạng và xác thực thuê bao trên điện thoại di động.
<b>supervisory control and data acquisition (SCADA)</b>	Một thuật ngữ chung được sử dụng để mô tả mạng lưới hệ thống điều khiển công nghiệp để kết nối các phần tử cơ sở hạ tầng (chẳng hạn như nhà máy sản xuất, đường ống dẫn dầu và khí đốt, hệ thống phát điện và phân phối, v.v...) và hệ thống máy tính lại với nhau.
<b>symmetric encryption</b>	Quá trình mã hóa yêu cầu tất cả các bên đều có một bản sao của khóa, đôi khi được gọi là bí mật được chia sẻ. Khóa đơn duy nhất được sử dụng cho cả mã hóa và giải mã.
<b>Synchronous Optical Network Technology (SONET)</b>	Một tập hợp các tiêu chuẩn được sử dụng để truyền dữ liệu qua mạng quang học.
<b>system on a chip (SoC)</b>	Tích hợp các chức năng hệ thống hoàn chỉnh trên một chip duy nhất để đơn giản hóa việc xây dựng các thiết bị.
T	

<b>tailgating</b>	Hành động theo sau người được cấp phép đi qua ngưỡng cửa mà không sử dụng thông tin đăng nhập của chính người đó.
<b>TACACS+</b>	Xem Terminal Access Controller Access Control System Plus.
<b>tactics, techniques, and procedures (TTPs)</b>	Các phương pháp được sử dụng bởi một đối thủ, được tổ chức theo cách thức để hỗ trợ việc nhận diện và phòng thủ.
<b>tangible asset</b>	Một tài sản có thể xác định được một khoản tiền tương đương. Ví dụ như hàng tồn kho, tòa nhà, tiền mặt, phẩn cứng, phần mềm, v.v...
<b>TAXII</b>	Xem Trusted Automated eXchange of Intelligence Information.
<b>Telnet</b>	Một giao thức mạng không an toàn được sử dụng để cung cấp giao tiếp văn bản rõ ràng hai chiều qua TCP. Được thay thế thường xuyên nhất bằng Secure Shell (SSH).
<b>Temporal Key Integrity Protocol (TKIP)</b>	Một giao thức bảo mật được sử dụng trong mạng không dây 802.11.
<b>Terminal Access Controller Access Control System Plus (TACACS+)</b>	Một hệ thống xác thực từ xa sử dụng giao thức TACACS+ qua cổng TCP 49 và được định nghĩa trong RFC 1492.

<b>threat</b>	Bất kỳ tình huống hoặc sự kiện nào có khả năng gây thiệt hại cho tài sản.
<b>ticket-granting ticket (TGT)</b>	Một phần của hệ thống xác thực Kerberos được sử dụng để chứng minh danh tính khi yêu cầu phiếu dịch vụ.
<b>time-based one-time password (TOTP)</b>	Mật khẩu được sử dụng một lần và chỉ có giá trị trong một khoảng thời gian cụ thể.
<b>time bomb</b>	Một dạng bom logic trong đó sự kiện kích hoạt là một ngày tháng hoặc thời gian cụ thể. <i>Xem thêm</i> logic bomb.
<b>TKIP</b>	<i>Xem</i> Temporal Key Integrity Protocol.
<b>token</b>	Một thiết bị phần cứng có thể được sử dụng trong quy trình xác thực phản hồi thử thách.
<b>Transaction Signature (TSIG)</b>	Một giao thức được sử dụng như một phương tiện xác thực các bản ghi DNS động trong quá trình cập nhật DNS.
<b>Transmission Control Protocol/Internet Protocol (TCP/IP)</b>	Một giao thức hướng kết nối để giao tiếp qua các mạng IP.

<b>Transport Layer Security (TLS)</b>	Một sự thay thế cho SSL hiện đang được sử dụng để bảo mật quá trình giao tiếp liên lạc giữa máy chủ và trình duyệt.
<b>trapdoor</b>	Xem backdoor.
<b>Trivial File Transfer Protocol (TFTP)</b>	Một phiên bản đơn giản của FTP được sử dụng để truyền tập tin với chi phí thấp bằng cách sử dụng cổng UDP 69.
<b>Trojan horse</b>	Một dạng mã độc hại dường như cung cấp một dịch vụ (và có thể thực sự cung cấp dịch vụ đó) nhưng cũng ẩn chứa một mục đích khác. Mục đích ẩn này thường có ý định xấu. Mã này cũng có thể đơn giản được gọi là <i>Trojan</i> .
<b>Trusted Automated eXchange of Intelligence Information (TAXII)</b>	Một khuôn khổ vận chuyển để truyền tải dữ liệu STIX.
<b>Trusted Platform Module (TPM)</b>	Một con chip phần cứng để hỗ trợ các hoạt động của nền tảng máy tính đáng tin cậy.
<b>TTPs</b>	Xem tactics, techniques, and procedures.

<b>typo squatting</b>	Một hình thức tấn công liên quan đến việc tận dụng các lỗi đánh máy chung ở cấp URL, với hy vọng người dùng trình duyệt sẽ không nhận thấy họ được đưa đến một trang web khác.
<b>U</b>	
<b>unified endpoint management (UEM)</b>	Việc tập hợp nhiều sản phẩm thành một hệ thống duy nhất trên một điểm đầu cuối vì mục đích hiệu quả.
<b>Unified Extensible Firmware Interface (UEFI)</b>	Một đặc tả thông số kỹ thuật xác định giao diện giữa hệ điều hành và firmware của phần cứng. Đây là một thay thế cho BIOS.
<b>unified threat management (UTM)</b>	Sự kết hợp của nhiều sản phẩm an ninh mạng vào một thiết bị duy nhất vì mục đích hiệu quả.
<b>Uniform Resource Identifier (URI)</b>	Một tập hợp các ký tự được sử dụng để xác định tên gọi của tài nguyên trong hệ thống máy tính. URL là một hình thức URI.
<b>uninterruptible power supply (UPS)</b>	Một nguồn điện (thường là pin) được thiết kế để cung cấp nguồn điện liên tục cho hệ thống máy tính trong trường hợp mất điện tạm thời.
<b>Universal Resource Locator (URL)</b>	Một chuỗi ký tự cụ thể được sử dụng để trỏ đến một mục cụ thể trên Internet.

<b>Universal Serial Bus (USB)</b>	Một giao thức tiêu chuẩn công nghiệp để giao tiếp qua cáp với thiết bị ngoại vi thông qua một bộ đầu nối tiêu chuẩn.
<b>Universal Serial Bus On-the-Go (USB OTG)</b>	Một thông số kỹ thuật được tiêu chuẩn hóa cho phép thiết bị đọc dữ liệu từ thiết bị USB mà không cần PC.
<b>unmanned aerial vehicle (UAV)</b>	Một phương tiện bay được điều khiển từ xa.
<b>unshielded twisted pair (UTP)</b>	Một kết nối vật lý bao gồm một cặp dây xoắn tạo thành một mạch.
<b>usage auditing</b>	Quá trình ghi nhận lại việc ai đã làm gì và khi nào trên một hệ thống thông tin.
<b>user acceptance testing (UAT)</b>	Việc áp dụng các tiêu chí kiểm tra chấp thuận để xác định tính phù hợp để sử dụng theo yêu cầu của người dùng đầu cuối.
<b>User and Entity Behavioral Analytics (UEBA)</b>	Một quy trình bảo mật sử dụng các mẫu hành vi của người dùng để xác định các điểm bất thường.
<b>User Datagram Protocol (UDP)</b>	Một giao thức trong bộ giao thức TCP/IP dành cho lớp truyền tải không cần trình tự của các gói tin - bản chất nó là “cháy và quên (fire and forget)”.

<b>user ID</b>	Một mã định danh chữ và số duy nhất chỉ định các cá nhân đang đăng nhập hoặc truy cập vào hệ thống.
<b>V</b>	
<b>vampire tap</b>	Một kết nối rẽ nhánh với đường dây mạng mà không cần cắt kết nối.
<b>Variable Length Subnet Masking (VLSM)</b>	Quá trình sử dụng mạng con có độ-dài-thay-đổi để tạo thành mạng con bên trong mạng con.
<b>video teleconferencing (VTC)</b>	Một quy trình nghiệp vụ sử dụng tín hiệu video để truyền tín hiệu âm thanh và hình ảnh giữa các địa điểm riêng biệt, do đó cho phép những người tham gia gặp nhau thông qua một cuộc họp ảo thay vì di chuyển đến một địa điểm thực tế. Thiết bị hội nghị truyền hình hiện đại có thể cung cấp kết nối rất thực tế khi ánh sáng và nền được kiểm soát.
<b>virtual desktop environment (VDE)</b>	Sử dụng công nghệ ảo hóa để thiết lập các hệ thống máy tính để bàn trên một máy chủ tập trung.
<b>virtual desktop infrastructure (VDI)</b>	Sử dụng máy chủ để thiết lập nền các máy tính để bàn ảo bằng cách chuyển quá trình xử lý đến máy chủ và sử dụng máy tính để bàn đơn thuần như một thiết bị hiển thị đầu cuối. VDI mang lại hiệu quả hoạt động cũng như các lợi ích về chi phí và bảo mật.

<b>virtual local area network (VLAN)</b>	Một miền quảng bá bên trong hệ thống chuyển mạch.
<b>virtual machine (VM)</b>	Một dạng hệ điều hành được đóng gói cho phép một hệ thống được chạy trên hệ điều hành khác.
<b>virtual private cloud (VC)</b>	Một phiên bản đám mây hầu như bị cô lập bởi nhà cung cấp.
<b>virtual private network (VPN)</b>	Một kết nối mạng được mã hóa qua một mạng khác, cung cấp một kênh giao tiếp riêng tư trên một phương tiện công cộng.
<b>virus</b>	Một dạng mã độc hoặc phần mềm tự gắn chính mình vào các đoạn mã khác để nhân bản. Vi-rút có thể chứa một tải trọng, vốn là một phần của mã [phần mềm] được thiết kế để thực thi khi một điều kiện nhất định được đáp ứng (chẳng hạn như vào một ngày nhất định). Trọng tải này thường có bản chất độc hại.
<b>ishing</b>	Một dạng tấn công kỹ thuật xã hội qua đường dây thoại (VoIP).
<b>Visual Basic for Applications (VBA)</b>	Một đặc tả thông số kỹ thuật của Microsoft để sử dụng Visual Basic trong các ứng dụng như Office Suite. Microsoft đã tuyên bố đây là một phương pháp luận kế thừa vào năm 2006.
<b>Voice over IP (VoIP)</b>	Truyền tín hiệu thoại (điện thoại) được đóng gói qua Giao thức Internet.

<b>vulnerability</b>	Một điểm yếu của tài sản có thể bị lợi dụng bởi một mối đe dọa để gây ra thiệt hại.
<b>W</b>	
<b>war dialing</b>	Nỗ lực của một kẻ tấn công để truy cập trái phép vào hệ thống máy tính hoặc mạng bằng cách phát hiện ra các kết nối không được bảo vệ với hệ thống thông qua hệ thống điện thoại và modem.
<b>war driving</b>	Cố gắng của kẻ tấn công để khám phá các mạng không dây không được bảo vệ bằng cách lang thang (hoặc lái xe) xung quanh với một thiết bị không dây, tìm kiếm các điểm truy cập không dây đang có sẵn.
<b>watering hole attack</b>	Việc lây nhiễm phần mềm độc hại vào một trang web mục tiêu cụ thể - một trang web mà người dùng tin tưởng và truy cập thường xuyên.
<b>whaling</b>	Một cuộc tấn công lừa đảo nhắm vào mục tiêu có giá trị cao như nhân viên công ty hoặc quản trị viên hệ thống.
<b>web application firewall (WAF)</b>	Tường lửa hoạt động ở cấp ứng dụng, được thiết kế đặc biệt để bảo vệ các ứng dụng web bằng cách kiểm tra các yêu cầu tại mức ngăn xếp ứng dụng.
<b>WEP</b>	Xem Wired Equivalent Privacy.

<b>wide area network (WAN)</b>	Là mạng trải dài trên một vùng địa lý rộng lớn.
<b>Wi-Fi Protected Access/Wi-Fi Protected Access 2 (WPA / WPA2)</b>	Một giao thức để bảo mật giao tiếp không dây bằng cách sử dụng một tập hợp con của tiêu chuẩn 802.11i.
<b>Wi-Fi Protected Access 3 (WPA3)</b>	Tiêu chuẩn bảo mật Wi-Fi mới nhất khắc phục những thiếu sót của WPA2.
<b>Wi-Fi Protected Setup (WPS)</b>	Một tiêu chuẩn bảo mật mạng cho phép dễ dàng thiết lập mạng gia đình không dây.
<b>Wired Equivalent Privacy (WEP)</b>	Lược đồ mã hóa được sử dụng để cố gắng cung cấp tính bảo mật và tính toàn vẹn của dữ liệu trên mạng 802.11.
<b>wireless access point (WAP)</b>	Một thiết bị truy cập mạng hỗ trợ kết nối các thiết bị không dây vào một mạng.
<b>Wireless Application Protocol (WAP)</b>	Một giao thức để truyền tải dữ liệu đến các thiết bị cầm tay nhỏ như điện thoại di động.

<b>wireless detection system (WIDS)</b>	Một hệ thống phát hiện xâm nhập được thiết lập để bao phủ một mạng không dây.
<b>wireless intrusion prevention system (WIPS)</b>	Một hệ thống ngăn chặn xâm nhập được thiết lập để bao phủ một mạng không dây.
<b>Wireless Transport Layer Security (WTLS)</b>	Giao thức mã hóa được sử dụng trên mạng WAP.
<b>worm</b>	Một đoạn mã độc hoặc phần mềm độc lập tự-nhân-bản. Không giống như vi-rút, nó không cần phải được gắn vào một đoạn mã khác. Một con sâu nhân bản bằng cách đột nhập vào một hệ thống khác và tạo một bản sao của chính nó trên hệ thống mới này. Một con sâu có thể chứa một tải trọng phá hủy nhưng không nhất thiết phải như vậy.
<b>write one read many (WORM)</b>	Một công nghệ lưu trữ dữ liệu trong đó mọi thứ được ghi một lần (vĩnh viễn) và sau đó có thể được đọc nhiều lần, như trong các đĩa quang học.
<b>X</b>	
<b>X.509</b>	Định dạng tiêu chuẩn dành cho chứng chỉ kỹ thuật số.

<b>XaaS</b>	Từ viết tắt của Anything as a Service.
<b>XML</b>	<i>Xem</i> Extensible Markup Language.
<b>XOR</b>	Phép loại trừ OR, một hoạt động thường được sử dụng trong mật mã.
<b>XSRF</b>	<i>Xem</i> cross-site request forgery.
<b>XSS</b>	<i>Xem</i> cross-site scripting.
<b>Z</b>	
<b>zero day</b>	Một lỗ hổng mà chưa từng có kiến thức nào về nó trước đó.