

NGUYỄN THỊ THANH VÂN (Chủ biên)
HUỲNH NGUYỄN CHÍNH

GIÁO TRÌNH
AN NINH MẠNG
(Dùng cho sinh viên ngành Công nghệ thông tin, An toàn thông tin)

NHÀ XUẤT BẢN ĐẠI HỌC QUỐC GIA
THÀNH PHỐ HỒ CHÍ MINH - 2023

TaiLieu.vn

LỜI NÓI ĐẦU

Giáo trình An ninh mạng là tài liệu phục vụ cho sinh viên ngành Công nghệ thông tin và An toàn thông tin thuộc chương trình đào tạo 150 tín chỉ của Trường Đại học Sư phạm Kỹ thuật Thành phố Hồ Chí Minh. Tài liệu được biên soạn nhằm cung cấp cho sinh viên các kiến thức cơ bản về an toàn thông tin, các nguy cơ tấn công và giải pháp an toàn trên cơ sở hạ tầng mạng, mạng wifi, cũng như các ứng dụng mạng. Ngoài ra, tài liệu cũng đề cập đến các giao thức bảo mật mạng như TLS, IPSec, PGP, SSH nhằm hỗ trợ các dịch vụ mạng hoạt động an toàn, đồng thời đưa ra các giải pháp tổng thể cho toàn hệ thống mạng như Firewall, IDS/IPS. Tài liệu không chỉ đề cập đến những cơ sở lý thuyết mà còn trình bày một số kỹ năng cần thiết để khai thác các lỗ hổng, thực hiện tấn công; đồng thời thiết lập, cài đặt và quản trị hệ thống mạng một cách an toàn. Hy vọng tài liệu sẽ có ích cho các sinh viên và những người muốn xây dựng các hệ thống mạng, quản trị an toàn các mạng doanh nghiệp. Mặc dù đã rất cố gắng trong quá trình biên soạn, nhưng tài liệu có thể vẫn còn thiếu sót trong trình bày, biên soạn, nhóm tác giả mong nhận được những đóng góp của độc giả để tài liệu được hoàn thiện hơn trong những lần tái bản sau.

Nhóm tác giả

TaiLieu.vn

MỤC LỤC

MỤC LỤC.....	5
DANH MỤC TỪ VIẾT TẮT.....	12
DANH MỤC CÁC HÌNH ẢNH.....	13
DANH MỤC BẢNG BIỂU.....	19
CHƯƠNG 1 GIỚI THIỆU VỀ AN NINH MẠNG.....	21
1.1. Khái quát về mạng máy tính.....	21
1.1.1. Mô hình kết nối hệ thống mở OSI và TCP/IP.....	21
1.1.2. Giao thức TCP và UDP.....	23
1.1.3. Thiết lập kết nối trong TCP.....	24
1.1.4. Giao thức IP, địa chỉ IP và cổng.....	25
1.1.5. Địa chỉ MAC và giao thức phân giải địa chỉ ARP.....	26
1.1.6. Dịch vụ phân giải tên miền DNS.....	28
1.1.7. Dịch vụ cấp phát IP động DHCP.....	28
1.1.8. Cơ chế chuyển dịch địa chỉ NAT.....	28
1.1.9. Các thiết bị mạng.....	29
1.1.10. Mạng riêng ảo VPN.....	30
1.2. An toàn thông tin trên mạng.....	31
1.2.1. CIA Triad.....	31
1.2.2. AAA - Authentication, Authorization, Accounting.....	32
1.2.3. Thuật ngữ về an toàn thông tin.....	33
1.3. Các nguy cơ về an toàn thông tin.....	34
1.4. Đối phó với các nguy cơ về an toàn thông tin.....	34
1.5. Các dạng tin tặc (hackers).....	35
1.6. Quản lý sự cố.....	36
1.7. Tổng kết chương.....	37
1.8. Câu hỏi và bài tập.....	37
 CHƯƠNG 2 ĐÁNH GIÁ AN TOÀN HỆ THỐNG MẠNG	
VÀ CÁC DỊCH VỤ MẠNG.....	41
2.1. Sự cần thiết của đánh giá an toàn mạng.....	41
2.1.1. Security Audit.....	41
2.1.2. Vulnerability Assessments.....	42
2.1.3. Penetration Testing.....	42
2.2. Các phương pháp đánh giá an toàn mạng.....	42
2.3. Footprinting và Reconnaissance.....	43

2.3.1. Giới thiệu	43
2.3.2. Các dạng Footprinting.....	43
2.3.3. Enumeration – liệt kê thông tin mạng.....	46
2.3.4. Các công cụ quét, liệt kê thông tin mạng.....	47
2.4. Scanning	49
2.4.1. Quét host	50
2.4.2. Quét cổng	52
2.4.3. Quét lỗ hổng.....	56
2.5. Penetration Testing	58
2.5.1. Hộp đen (Black box).....	58
2.5.2. Hộp trắng (White box).....	59
2.5.3. Hộp xám (Gray box).....	59
2.6. Đánh giá các dịch vụ mạng	59
2.6.1. Đánh giá các dịch vụ mạng thông thường	59
2.6.2. Đánh giá các dịch vụ mạng của Microsoft.....	74
2.6.3. Đánh giá các dịch vụ Email	82
2.6.4. Đánh giá các dịch vụ Web Server	89
2.7. Tổng kết chương	94
2.8. Câu hỏi ôn tập	95
 CHƯƠNG 3 TẤN CÔNG MẠNG	 99
3.1. Giới thiệu về tấn công mạng	99
3.2. Tấn công mật khẩu	100
3.2.1. Non-Electronic	100
3.2.2. Active Online	100
3.2.3. Passive Online.....	101
3.2.4. Default Password	101
3.2.5. Offline	102
3.2.6. Cách phòng chống tấn công mật khẩu	102
3.3. Tấn công leo thang đặc quyền (Escalating Privileges)	102
3.3.1. Khái niệm tấn công leo thang đặc quyền.....	102
3.3.2. Các dạng leo thang đặc quyền	103
3.3.3. Phòng chống tấn công leo thang đặc quyền.....	103
3.4. Tấn công DoS (Denial of Service).....	104
3.4.1. Flooding: SYN TCP, UDP, ICMP, HTTP	105
3.4.2. Spoofing: SYN, source address.....	107
3.4.3. Distributed DoS (DDoS).....	108
3.4.4. Reflection DoS	109

3.4.5. Amplification DoS: DNS	109
3.4.6. Smurf.....	110
3.4.7. Ping of death	111
3.4.8. Cách phòng chống tấn công DoS.....	111
3.5. Tấn công Sniffing.....	112
3.5.1. Khái niệm Sniffing	112
3.5.2. Sniffing chủ động và thụ động	112
3.5.3. Cách phòng chống tấn công Sniffing	113
3.6. Tấn công Session Hijacking	114
3.6.1. Khái niệm Session Hijacking.....	114
3.6.2. Quá trình Session Hijacking	114
3.6.3. Các dạng Session Hijacking.....	115
3.6.4. Cách phòng chống tấn công Session Hijacking.....	116
3.7. Tấn công Web Server.....	117
3.7.1. Các sự cố bảo mật Web Server	117
3.7.2. Các tấn công Web Server	117
3.7.3. Các phương pháp tấn công Web Server	118
3.7.4. Cách phòng chống tấn công Web Server	119
3.8. Tấn công ứng dụng Web.....	120
3.8.1. Các mối đe dọa ứng dụng Web	120
3.8.2. Các phương pháp tấn công ứng dụng Web	121
3.8.3. Cách phòng chống tấn công ứng dụng Web.....	122
3.9. Tấn công SQL Injection.....	122
3.9.1. Khái niệm SQL Injection	122
3.9.2. Các dạng SQL Injection	123
3.9.3. Các phương pháp tấn công SQL Injection	124
3.9.4. Cách phòng chống tấn công SQL Injection	125
3.10. Tấn công Social Engineering.....	125
3.10.1. Khái niệm Social Engineering	125
3.10.2. Các giai đoạn tấn công Social Engineering	125
3.10.3. Các hình thức tấn công Social Engineering	126
3.10.4. Phòng chống tấn công Social engineering	127
3.11. Mã độc tấn công mạng.....	127
3.11.1. Khái niệm về mã độc tấn công mạng	127
3.11.2. Các dạng mã độc và phòng chống	128
3.12. Tổng kết chương	134
3.13. Câu hỏi và bài tập	135

CHƯƠNG 4 AN TOÀN CƠ SỞ HẠ TẦNG MẠNG.....	141
4.1. Giới thiệu về an toàn hạ tầng mạng	141
4.1.1. Hạ tầng mạng và các nguy cơ	141
4.1.2. Chức năng của an toàn hạ tầng mạng	143
4.1.3. Các thách thức với an toàn hạ tầng mạng	144
4.2. An toàn hạ tầng mạng – phần Switching.....	145
4.2.1. Hoạt động của Switch và các nguy cơ	145
4.2.2. Tấn công MAC Flooding	146
4.2.3. Tấn công ARP Poisoning	149
4.2.4. Tấn công STP	152
4.2.5. Tấn công VLAN.....	156
4.2.6. Thực nghiệm các tấn công phần Switching	161
4.3. An toàn hạ tầng mạng – phần Routing	173
4.3.1. Hoạt động định tuyến và các nguy cơ.....	173
4.3.2. Tấn công External và Internal.....	174
4.3.3. Tấn công giao thức RIP và phương pháp phòng chống	177
4.3.4. Tấn công giao thức OSPF và phương pháp phòng chống	182
4.3.5. Tấn công giao thức BGP và phương pháp phòng chống	183
4.4. An toàn hạ tầng mạng – Dịch vụ địa chỉ, tên miền	191
4.4.1. Các dạng tấn công DHCP	191
4.4.2. Các dạng tấn công DNS	196
4.5. Bảo vệ cơ sở hạ tầng mạng - Phương pháp tiếp cận mới	200
4.5.1. Nguồn gốc vấn đề bảo mật của cơ sở hạ tầng mạng.....	200
4.5.2. Tách và phân tầng cơ sở hạ tầng mạng.....	200
4.5.3. Tách lớp 2 cơ sở hạ tầng mạng - Lọc địa chỉ MAC.....	202
4.5.4. Phân cấp cơ sở hạ tầng mạng trong mạng STP.....	203
4.5.5. Phân tách cơ sở hạ tầng mạng lớp 3.....	205
4.5.6. Một cơ sở hạ tầng mạng hoàn toàn ẩn – một định hướng mới	257
4.6. Tổng kết chương	208
4.7. Câu hỏi và bài tập	208
 CHƯƠNG 5 CÁC GIAO THỨC AN TOÀN MẠNG	 212
5.1. Bảo mật tầng trong TCP/IP.....	212
5.2. Giao thức bảo mật tầng Network – IPSec	213
5.2.1. Giới thiệu IPSec	213
5.2.2. Các thành phần của IPSec.....	216
5.2.3. Giao thức AH và ESP.....	217

5.2.4. Chế độ truyền.....	218
5.2.5. Quản lý khóa IKE - Internet Key Exchange	221
5.2.6. Thuật toán mã hóa trong IPSec	225
5.2.7. Chính sách IPsec	227
5.3. Giao thức bảo mật tầng Transport.....	228
5.3.1. Giới thiệu SSL.....	228
5.3.2. Các khái niệm trong SSL	229
5.3.3. Kiến trúc SSL.....	232
5.3.4. Giao thức TLS – Transport Layer Security.....	235
5.4. Giao thức bảo mật tầng Application	237
5.4.1. Giao thức HTTPS	237
5.4.2. Giao thức SSH	239
5.4.3. Giao thức PGP.....	246
5.4.4. Chuẩn S/MIME.....	253
5.5. Tổng kết chương	257
5.6. Câu hỏi và bài tập	257
 CHƯƠNG 6 AN TOÀN MẠNG KHÔNG DÂY.....	 261
6.1. Các nguy cơ của mạng Wireless	261
6.2. Bảo mật mạng Wireless	261
6.2.1. Wired Equivalent Privacy (WEP)	262
6.2.2. Chuẩn bảo mật IEEE 802.11i.....	263
6.2.3. WiFi Protected Access (WPA), WPA2, WPA3	271
6.3. Bảo mật tầng vận chuyển mạng không dây.....	272
6.3.1. Giới thiệu WTLS (Wireless Transport Layer Security)	272
6.3.2. Kiến trúc WTLS.....	273
6.3.3. So sánh TLS và WTLS	274
6.4. Các tấn công mạng WiFi và giải pháp phòng chống	275
6.4.1. Tấn công dựa vào các tiêu chuẩn của an toàn thông tin	275
6.4.2. Tấn công dựa vào đặc điểm mạng không dây.....	275
6.5. Giải pháp phòng chống tấn công WiFi.....	278
6.6. Thực nghiệm một số tấn công WiFi	279
6.6.1. Tấn công DoS trên AP.....	279
6.6.2. Tấn công crack mật khẩu WPA-PSK	280
6.7. Tổng kết chương	283
6.8. Câu hỏi và bài tập	283

CHƯƠNG 7 GIẢI PHÁP AN TOÀN MẠNG.....	287
7.1. Firewall	287
7.1.1. Giới thiệu Firewall.....	287
7.1.2. Các dạng Firewall	288
7.1.3. Kiến trúc của Firewall.....	297
7.1.4. Thiết kế Firewall	299
7.2. IDS - Intrusion detection system	303
7.2.1. Khái niệm.....	303
7.2.2. Kiến trúc và hoạt động IDS	304
7.2.3. Phân loại IDS	304
7.3. IPS - Intrusion Prevention Systems.....	307
7.3.1. Khái niệm.....	307
7.3.2. Phân loại.....	308
7.3.3. Triển khai IDS/IPS	308
7.4. Tổng kết chương	309
7.5. Câu hỏi và bài tập	309
 CHƯƠNG 8 AN TOÀN ĐIỆN TOÁN Đám Mây.....	 313
8.1. Các thành phần của điện toán đám mây	313
8.1.1. Giới thiệu	313
8.1.2. Dịch vụ của điện toán đám mây.....	313
8.1.3. Các đặc tính của điện toán đám mây	314
8.1.4. Các mô hình triển khai của điện toán đám mây.....	315
8.2. Các rủi ro với điện toán đám mây	315
8.2.1. Lạm dụng và sử dụng bất chính điện toán đám mây	316
8.2.2. Giao diện và API không an toàn	316
8.2.3. Nội gián độc hại	316
8.2.4. Các vấn đề chia sẻ.....	316
8.2.5. Mất hoặc rò rỉ dữ liệu.....	317
8.2.6. Chiếm đoạt tài khoản hoặc dịch vụ.....	317
8.2.7. Các rủi ro không xác định.....	317
8.3. Bảo vệ dữ liệu trong đám mây	317
8.3.1. Đặc điểm dữ liệu trong đám mây.....	317
8.3.2. Một giải pháp bảo mật dữ liệu trong đám mây	318
8.4. Dịch vụ bảo mật điện toán đám mây.....	319
8.4.1. Quản lý danh tính và truy cập (IAM).....	320
8.4.2. Ngăn ngừa mất mát dữ liệu (DLP).....	321
8.4.3. Bảo mật web và email.....	321

8.4.4. Đánh giá bảo mật	321
8.4.5. Quản lý xâm nhập, sự kiện và thông tin an toàn (SIEM)	321
8.4.6. Mã hóa	321
8.4.7. Tính liên tục trong kinh doanh và phục hồi sau thảm họa	322
8.4.8. An ninh mạng	322
8.5. Tổng kết chương	322
8.6. Câu hỏi và bài tập	322
TÀI LIỆU THAM KHẢO	327

TaiLieu.vn

DANH MỤC TỪ VIẾT TẮT

Viết tắt	Nội dung	Viết tắt	Nội dung
OSI	Open Systems Interconnection Reference	CIA	Confidentiality Integrity Availability
ARP	Address Resolution Protocol	RIP	Routing Information Protocol
RARP	Reverse ARP	OSPF	Open Shortest Path First
MAC	Media Access Control	VLAN	Virtual Local Area Network
TCP	Transmission Control Protocol	EIGRP	Enhanced Interior Gateway Routing Protocol
UDP	User Datagram Protocol	STP	Spanning Tree Protocol
IP	Internet Protocol	NAT	Network Address Translation
HTTP	Hypertext Transfer Protocol	VTP	VLAN Trunking Protocol
FTP	File Transfer Protocol		
DHCP	Dynamic Host Configuration Protocol	AAA	Authentication Authority Accounting
DNS	Domain Name System	EFS	Encrypted File Service
SMTP	Simple Mail Transfer Protocol	SNMP	Simple Network Management Protocol
POP	Post Office Protocol	ACL	Access Control List
BSS	Basic service sets	IDS	Intrusion Detection System
AP	Access Point	DoS	Denial of Service
SSID	Service Set Identifier	DDoS	Distributed Dos
AES	Advanced Encryption Standard	SIEM	Security Information and Event Management
DES	Data Encryption Standard	IPS	Intrusion Prevention Systems
S/MIME	Secure / Multipurpose Internet Mail Extension	CIDR	Classless Inter-Domain Routing
SSL	Security Socket Layer	AH	Authentication Header
TLS	Transport Layer Security	ESP	Encapsulating Security Payload
PGP	Pretty Good Privacy	IKE	Internet Key Exchange
SSH	Secure Shell		
IPSec	Internet Protocol Security		

DANH MỤC CÁC HÌNH ẢNH

Hình 1.1: Mô hình OSI và chức năng các tầng.....	21
Hình 1.2: So sánh mô hình OSI và TCP/IP.....	22
Hình 1.3: Quá trình bắt tay ba bước của TCP.....	24
Hình 1.4: Các gói tin bắt được từ quá trình bắt tay ba bước.....	24
Hình 1.5: Lệnh xem địa chỉ MAC của các card mạng.....	26
Hình 1.6: Hoạt động của giao thức ARP.....	27
Hình 1.7: Kỹ thuật NAT.....	29
Hình 1.8: Mô hình kết nối các thiết bị mạng.....	30
Hình 1.9: Kỹ thuật VPN.....	30
Hình 1.10: Mô hình CIA.....	31
Hình 1.11: Ví dụ ứng dụng AAA.....	33
Hình 1.12: Bảo mật nhiều lớp.....	35
Hình 2.1: Các dạng đánh giá bảo mật mạng.....	41
Hình 2.2: Nmap.....	47
Hình 2.3: Zenmap.....	48
Hình 2.4: NetScanTools Pro.....	48
Hình 2.5: Superscan.....	49
Hình 2.6: MegaPing.....	51
Hình 2.7: Advanced IP Scanner.....	52
Hình 2.8: Full Scan.....	53
Hình 2.9: SYN Scan.....	53
Hình 2.10: FIN Scan.....	54
Hình 2.11: XMAS Scan.....	54
Hình 2.12: NULL Scan.....	54
Hình 2.13: UDP Scan.....	55
Hình 2.14: Idle Scan.....	55
Hình 2.15: Dùng Nmap quét lỗ hổng MS17-010.....	57
Hình 2.16: Nessus.....	57
Hình 3.1: Tấn công DoS.....	104
Hình 3.2: Tấn công SYN Flood.....	105
Hình 3.3: Tấn công UDP Flood.....	106
Hình 3.4: Tấn công HTTP Flood.....	106
Hình 3.5: Tấn công ICMP Flood.....	107
Hình 3.6: Tấn công giả mạo IP.....	107

Hình 3.7: Tấn công giả mạo cờ SYN.....	108
Hình 3.8: Tấn công Distributed DoS (DDoS).....	108
Hình 3.9: Tấn công Reflection DoS.....	109
Hình 3.10: Tấn công Amplification DoS	109
Hình 3.11: Tấn công DNS Amplification.....	110
Hình 3.12: Tấn công Smurf.....	110
Hình 3.13: Tấn công Ping of Death	111
Hình 3.14: Tấn công Sniffing.....	112
Hình 3.15: Sniffing chủ động và bị động	112
Hình 3.16: Tấn công Session Hijacking.....	114
Hình 3.17: Tấn công Session Hijacking chủ động.....	115
Hình 3.18: Tấn công Session Hijacking bị động	115
Hình 3.19: Firewall, IDS/IPS trong bảo mật Web Server.....	119
Hình 3.20: Hoạt động của SQL Injection	123
Hình 3.21: Social Engineering.....	125
Hình 3.22: Các giai đoạn tấn công Social Engineering	125
Hình 3.23: Chu trình hoạt động của virus.....	128
Hình 4.1: Các thành phần trong cơ sở hạ tầng mạng.....	141
Hình 4.2: Hoạt động cập nhật bảng CAM [4].....	147
Hình 4.3: Minh họa tấn công MAC Flooding [4]	148
Hình 4.4: Hoạt động của giao thức ARP.....	149
Hình 4.5: Tấn công ARP Poisoning [4]	150
Hình 4.6: Mọi traffic đều đổ về Host-X [4]	150
Hình 4.7: Sơ đồ kết nối các Switch dự phòng	152
Hình 4.8: Hoạt động của STP [4].....	153
Hình 4.9: Thay đổi luồng lưu lượng mạng [4].....	154
Hình 4.10: Minh họa chức năng BPDU Guard [4]	155
Hình 4.11: Minh họa chức năng Root Guard [4]	156
Hình 4.12: Mạng VLAN dùng đường trunk	157
Hình 4.13: Định dạng VLAN frame	157
Hình 4.14: Hoạt động của VLAN Frame tagging.....	158
Hình 4.15: Autotrunking trên Switch [4]	159
Hình 4.16: Minh họa tấn công VLAN double tagging [4].....	160
Hình 4.17: Sơ đồ mạng thực hiện tấn công MAC Flooding [4]	161
Hình 4.18: Hiện thị bảng CAM trên Switch	161
Hình 4.19: Thực hiện tấn công bằng macof.....	162

Hình 4.20: Bảng CAM với nhiều MAC giả mạo	162
Hình 4.21: Bật chế độ bảo vệ trên Et0/2	163
Hình 4.22: Sơ đồ mạng thực hiện tấn công ARP Poisoning [4].....	163
Hình 4.23: Kiểm tra bảng cache ARP dùng arp	163
Hình 4.24: Cấu hình forward gói tin.....	163
Hình 4.25: Dùng Wireshark bắt gói tin.....	164
Hình 4.26: Traffic giữa Host A và Host đầu tới máy Attacker	164
Hình 4.27: Sơ đồ thực hiện tấn công STP.....	165
Hình 4.28: Xem thông tin STP.....	166
Hình 4.29: Tấn công chiếm quyền Root Bridge trên Yersinia	166
Hình 4.30: Cảnh báo STP tại Switch 1	167
Hình 4.31: Cấu hình PortFast và BPDU Guard	167
Hình 4.32: Cổng f1/0 đóng khi có dấu hiệu tấn công	168
Hình 4.33: Kiểm tra CPU của Switch trước tấn công: <5%.....	168
Hình 4.34: Số lượng BPDU nhận được trước tấn công: 0	168
Hình 4.35: Tấn công STP DoS trên Yersinia	169
Hình 4.36: CPU của Switch sau tấn công: 65%-75%.....	169
Hình 4.37: Số lượng BPDU nhận được sau tấn công: 1869888	170
Hình 4.38: Sơ đồ mạng tấn công VLAN	170
Hình 4.39: Kiểm tra VLAN trên Switch và trạng thái VLAN.....	171
Hình 4.40: Cấu hình Dynamic Desirable.....	171
Hình 4.41: Bật trunking trên Yersinia	172
Hình 4.42: Trạng thái trunk của Gi0/0	172
Hình 4.43: Các VLAN được phép hoạt động trên port Gi0/0.....	172
Hình 4.44: Nguồn tấn công Internal và External [4]	174
Hình 4.45: Ví dụ về chữ ký số cho việc cập nhật định tuyến	176
Hình 4.46: Trường hợp cập nhật định tuyến đúng [4]	178
Hình 4.47: Trường hợp cập nhật định tuyến sai [4]	179
Hình 4.48: Ví dụ thuật toán PAIR [4]	181
Hình 4.49: Cập nhật không hợp lệ [4]	181
Hình 4.50: Minh họa tấn công Prefix Hijacking [4]	184
Hình 4.51: Minh họa tấn công Prefix De-aggregation [4]	185
Hình 4.52: Giải pháp lọc đường đi [4].....	187
Hình 4.53: Hoạt động của S-BGP [4]	188
Hình 4.54: Hoạt động của so-BGP [4].....	189
Hình 4.55: Hoạt động của IRV [4]	190

Hình 4.56: Tấn công DoS DHCP Server dùng Address Starvation [4]	192
Hình 4.57: Tấn công DoS DHCP Server với Yersinia	192
Hình 4.58: Tấn công MITM dùng DHCP Server giả mạo [4]	193
Hình 4.59: Giả mạo DHCP dùng Yersinia	194
Hình 4.60: Chuyển hướng DNS dùng DHCP Server giả mạo [4]	195
Hình 4.61: Sơ đồ mạng giải pháp DHCP snooping	196
Hình 4.62: Các thành phần và hoạt động của DNSSEC	199
Hình 4.63: Một mạng có sự tách biệt về cơ sở hạ tầng mạng [4]	201
Hình 4.64: Network Infrastructure Switch (NI-Switch) [4].....	202
Hình 4.65: Một mạng chuyển mạch với t tầng của các Switch [4].....	204
Hình 4.66: Cổng Higher Tier và cổng Lower Tier trên Switch [4].....	204
Hình 4.67: ERS hoạt động trong một mạng thông thường [4]	206
Hình 4.68: Sơ đồ minh họa một cơ sở hạ tầng mạng ẩn [4]	207
Hình 5.1: Các giao thức bảo mật trong TCP/IP	213
Hình 5.2: IPSec trong TCP/IP.....	214
Hình 5.3: Một ví dụ sử dụng IPSec.....	215
Hình 5.4: Các thành phần của IPSec.....	216
Hình 5.5: Định dạng gói tin AH.....	217
Hình 5.6: Định dạng gói tin ESP.....	217
Hình 5.7: Chế độ Transport với giao thức AH, ESP và kết hợp	219
Hình 5.8: Chế độ Tunnel với giao thức AH, ESP và kết hợp.....	219
Hình 5.9: Mạng bảo mật theo chế độ Transport.....	220
Hình 5.10: Mạng VPN site to site theo chế độ Tunnel	221
Hình 5.11: Trao đổi IKE	223
Hình 5.12: Định dạng gói tin giao thức IKE.....	223
Hình 5.13: Quá trình hoạt động của IKE	224
Hình 5.14: Mối quan hệ giữa SAD và SPD	227
Hình 5.15: Hoạt động cấp chứng chỉ	231
Hình 5.16: Kiến trúc SSL.....	232
Hình 5.17: Hoạt động của giao thức SSL Record [1]	232
Hình 5.18: Hoạt động của giao thức Handshake	235
Hình 5.19: Khởi tạo kết nối trong HTTPS.....	238
Hình 5.20: Kiến trúc SSH	240
Hình 5.21: Định dạng gói tin giao thức lớp truyền tải SSH [1].....	241
Hình 5.22: Trao đổi thông điệp trong giao thức lớp truyền tải SSH.....	242
Hình 5.23: Trao đổi thông điệp trong giao thức kết nối [1].....	245

Hình 5.24: Chuyển tiếp cổng [1].....	246
Hình 5.25: Hoạt động dịch vụ xác thực	248
Hình 5.26: Hoạt động dịch vụ bảo mật.....	248
Hình 5.27: Hoạt động dịch vụ xác thực và bảo mật.....	248
Hình 5.28: Truyền và nhận thông điệp PGP	250
Hình 5.29: Vòng khóa riêng và vòng khóa công khai	251
Hình 5.30: Định dạng gói tin PGP	252
Hình 6.1: Mã hóa trong WEP.....	262
Hình 6.2: Giải mã trong WEP	262
Hình 6.3: Các thành phần của IEEE 802.11i [1].....	263
Hình 6.4: 5 giai đoạn hoạt động của 802.11i [1].....	265
Hình 6.5: Giai đoạn khám phá khả năng, xác thực và liên kết [1].....	266
Hình 6.6: Điều khiển truy xuất theo chuẩn 802.1X	267
Hình 6.7: Phân cấp khóa cặp [1].....	268
Hình 6.8: Phân cấp khóa nhóm [1]	268
Hình 6.9: Phân phối khóa cặp [1]	269
Hình 6.10: Phân phối khóa nhóm [1].....	270
Hình 6.11: Kiến trúc của WTLS	273
Hình 6.12: Tấn công Rogue Access Point.....	276
Hình 6.13: Tấn công Client Mis-association	276
Hình 6.14: Tấn công Misconfigured Access Point.....	277
Hình 6.15: Tấn công Unauthorized Association	277
Hình 6.16: Tấn công Ad Hoc Connection.....	278
Hình 6.17: Tấn công Jamming Signal.....	278
Hình 6.18: Hiện thị thông tin của các AP	280
Hình 6.19: Quá trình hủy xác thực.....	281
Hình 6.20: Lấy mật khẩu dựa vào quá trình bắt tay.....	282
Hình 6.21: Lấy mật khẩu thành công.....	283
Hình 7.1: Một hệ thống Firewall.....	287
Hình 7.2: Firewall tại các layer của mô hình OSI.....	288
Hình 7.3: Packet filter firewall	289
Hình 7.4: Application gateway firewalls.....	292
Hình 7.5: Ví dụ về Connection Gateway Firewall.....	293
Hình 7.6: Ví dụ về Cut-Through Proxy Firewalls	293
Hình 7.7: Circuit-level gateways	294
Hình 7.8: Ví dụ về Address-translation firewalls.....	295

Hình 7.9: Host-based firewalls.....	296
Hình 7.10: Kiến trúc Dual-homed Host	297
Hình 7.11: Kiến trúc Screened Host	298
Hình 7.12: Kiến trúc Screened Subnet Host	299
Hình 7.13: Thiết kế Firewall với Single DMZ - Single segment.....	301
Hình 7.14: Thiết kế Firewall Single DMZ – Service leg segment.....	302
Hình 7.15: Thiết kế Firewall với Multiple DMZs	302
Hình 7.16: Thiết kế Firewall với Internal DMZ	303
Hình 7.17: Kiến trúc hệ thống IDS	304
Hình 7.18: Hoạt động Signature-based IDS	305
Hình 7.19: Hoạt động của Anomaly-Based	305
Hình 7.20: Network-based IDS	306
Hình 7.21: Host-based IDS	307
Hình 7.22: Chế độ Inline.....	309
Hình 7.23: Chế độ Passive	309
Hình 8.1: Mô hình dịch vụ cơ bản của điện toán đám mây	314
Hình 8.2: Mô hình triển khai của điện toán đám mây	315
Hình 8.3: Mô hình mã hóa cơ sở dữ liệu trong đám mây	319
Hình 8.4: Mô hình dịch vụ bảo mật điện toán đám mây.....	320

DANH MỤC BẢNG BIỂU

Bảng 1.1: Các giao thức ở từng tầng của mô hình OSI.....	22
Bảng 1.2: Bảng so sánh TCP và UDP	23
Bảng 1.3: Các cổng dịch vụ thông dụng	26
Bảng 1.4: Một số tấn công vào bộ ba CIA	32
Bảng 2.1: Cổng, dịch vụ và thông tin thông thường	47
Bảng 2.2: Port và giao thức các dịch vụ thông thường	59
Bảng 2.3: Cơ chế xác thực SSH phổ biến	65
Bảng 2.4: Port và giao thức các dịch vụ độc quyền của Microsoft.....	74
Bảng 2.5: Các dịch vụ của Microsoft sử dụng các giao thức.....	75
Bảng 2.6: Port và giao thức các dịch vụ email.....	82
Bảng 4.1: Các mối đe dọa của cơ sở hạ tầng mạng.....	142
Bảng 4.2: Các hậu quả của tấn công cơ sở hạ tầng mạng	142
Bảng 4.3: Các mối đe dọa của tấn công External.....	175
Bảng 4.4: Lọc khung tại cổng NNI	203
Bảng 4.5: Bảng so sánh các giải pháp.....	208
Bảng 5.1: Các bộ mã hóa cho mạng VPN.....	226
Bảng 5.2: Các thuật toán và thông số cho hai bộ của NSA.....	226
Bảng 5.3: Các kiểu thông báo của giao thức Handshake	235
Bảng 5.4: Một số khác biệt cơ bản của TLS so với SSL.....	257
Bảng 5.5: Các đặc điểm kỹ thuật của PGP và openPGP	247
Bảng 5.6: Các kiểu nội dung của S/MIME	256
Bảng 6.1: Các dịch vụ, giao thức và thuật toán trong IEEE 802.11i....	264
Bảng 6.2: Bảng so sánh TLS và WTLS	274
Bảng 6.3: Các tiêu chuẩn bị phá vỡ bởi các tấn công	275
Bảng 7.1: Ví dụ về rule được thiết lập trong tường lửa lọc gói	289
Bảng 7.2: Ví dụ về bảng trạng thái.....	291

TaiLieu.vn