Chương 1:

Câu 3: Một trang web bận rộn đã không được đáp ứng tốt vì khối lượng lớn kết nối HTTP đến máy chủ web. Giải pháp nào sẽ tăng hiệu suất máy chủ web?

A. Thêm RAM vào máy chủ web.

B. Cài đặt hai máy chủ web lưu trữ cùng một nội dung. Định cấu hình bộ cân bằng tải để phân phối các kết nối HTTP đến giữa hai máy chủ web.

C. Đặt bộ định tuyến giữa máy chủ web và Internet để điều tiết các kết nối HTTP đến.

D. Kích hoạt SSL trên máy chủ web.

Câu 4: Tính năng bảo mật bộ định tuyến nào làm giảm lưu lượng truy cập trong nước với địa chỉ nguồn giả mạo của mạng nội bộ?

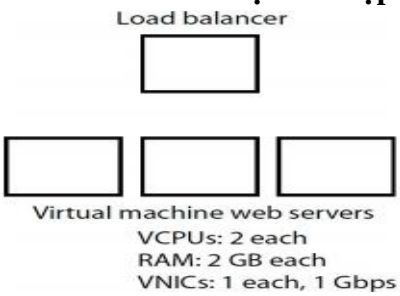
A. Stateful packet inspection

B. Stateless packet inspection

C. Anti-malware

D. Anti-spoofing

Câu 5: Tham khảo sơ đồ trong hình 1-1. Bạn muốn ngăn chặn các yêu cầu của khách hàng được phục vụ bởi các máy chủ back-end bận rộn hơn. Bạn nên cấu hình thuật toán lập lịch cân bằng tải nào?



A. Vòng tròn (Round Robin)

B. Trọng số vòng tròn (Weighted round robin)

C. Ngẫu nhiên (Random)

D. ít kết nối nhất (least connections)

Câu 7: Trong một cuộc họp CNTT, đồng nghiệp Raylee của bạn gợi ý rằng có một điểm thất bại duy nhất trong bộ cân bằng tải duy nhất thay cho hệ thống đặt hàng trang web của công ty. Cô đề nghị có hai bộ cân bằng tải được cấu hình, chỉ có một bộ phận phục vụ tại một thời điểm nhất định. Raylee đã mô tả loại cấu hình cân bằng tải nào?

A. Vòng tròn (Round Robin)

B. Hoạt động tích cực (Active-active)

C. Thụ động tích cực (Active-passive)

D. ít kết nối nhất (least connections)

Câu 8: Một giải pháp cân bằng tải thụ động chủ động được cấu hình trên mạng của bạn. Khi bộ cân bằng tải dự phòng xác định rằng bộ cân bằng tải chính bị hỏng, nó sẽ kiểm soát thuộc tính nào?

A. Tải cân bằng địa chỉ MAC

B. Tải cân bằng địa chỉ IP

C. Địa chỉ MAC máy chủ phụ trợ đầu tiên

D. Địa chỉ IP máy chủ phụ trợ đầu tiên

Câu 9: Phát biểu nào sau đây liên quan đến ACL của bộ định tuyến là đúng?

A. Các quy tắc được xử lý theo cách từ trên xuống.

B. Các quy tắc được xử lý theo cách từ dưới lên.

C. Quy tắc đầu tiên phải là quy tắc từ chối tất cả.

D. Quy tắc cuối cùng phải là quy tắc cho phép tất cả.

Câu 10: Khi viết quy tắc ACL của bộ định tuyến, cần tuân thủ hướng dẫn chung nào?

A. Không cho phép lưu lượng truy cập dựa trên địa chỉ IP.

B. Không chặn lưu lượng dựa trên địa chỉ IP.

C. Quy tắc đầu tiên phải là quy tắc từ chối tất cả.

D. Quy tắc cuối cùng phải là quy tắc từ chối tất cả.

Câu 11: Mạng của bạn yêu cầu các bộ định tuyến có thể chặn lưu lượng dựa trên địa chỉ MAC. Những loại hỗ trợ quy tắc ACL phải hỗ trợ bộ định tuyến?

A. Layer 1

B. Layer 2

C. Layer 3

D. Layer 4

Câu 12: Hình 1-2 cho thấy các quy tắc ACL của bộ định tuyến cho bộ định tuyến 1. Các truy vấn DNS của người dùng phải có thể đi qua bộ định tuyến 1. Phát biểu nào liên quan đến cấu hình này là chính xác? (Chọn hai.)

```
access-list 112 permit tcp any any eq 53
access-list 112 permit udp any any eq 80
access-list 112 permit tcp any any eq 22
access-list 112 permit tcp any any eq 443
```

A. Truy vấn DNS của người dùng sẽ đi qua bộ định tuyến 1.

B. Lưu lượng sao chép máy chủ DNS sẽ đi qua bộ định tuyến 1.

C. Lưu lượng người dùng SSH sẽ đi qua bộ định tuyến 1.

D. Tin nhắn máy chủ SMTP sẽ đi qua bộ định tuyến 1.

Câu 13: Là một phần của nhóm bảo mật mạng, bạn cần nắm bắt các truyền phát mạng đến và từ tất cả các máy chủ trên bộ chuyển đổi mạng Ethernet. Tuy nhiên, sau khi cắm vào cổng chuyển đổi 24 và bắt đầu phiên xử lý gói, bạn chỉ thấy truyền phát và phát đa hướng từ các máy chủ khác. Bạn phải làm gì?

A. Cắm vào cổng chuyển đổi 1.

B. Cắm một hub vào cổng chuyển đổi 24 và cắm trạm của bạn vào hub.

C. Cấu hình giám sát cổng chuyển đổi trên cổng 24.

D. Cấu hình giám sát cổng chuyển đổi trên cổng 1.

Câu 14: Những loại thiết bị mạng kết quả trong các lĩnh vực phát sóng bổ sung?

A. Hub

B. Layer 2 switch

C. Router

D. Bridge

Câu 15: Các nhân viên CNTT khởi tạo một khối lượng lớn lưu lượng mạng đến và từ máy chủ 1 và máy chủ 2. Tất cả các trạm nhân viên được cắm vào bốn thiết bị chuyển mạch được liên kết với nhau. Nên làm gì để sử dụng hiệu quả hơn băng thông mạng?

A. Đặt các nhân viên CNTT và các máy chủ trên Vlan của riêng họ.

B. Đặt máy chủ 1 và máy chủ 2 trên các Vlan riêng biệt.

C. Đặt bộ định tuyến giữa các nhân viên CNTT và máy chủ.

D. Đặt một chuyển đổi giữa các nhân viên CNTT và các máy chủ.

Câu 16: Telnet được sử dụng cho mục đích nào sau đây?

A. Xác minh bộ định tuyến trong đường truyền

B. Thực hiện quản lý dòng lệnh được mã hóa từ xa

C. Thực hiện quản lý dòng lệnh từ xa rõ ràng

D. Buộc truy xuất các bản cập nhật hệ điều hành

Câu 17: Zoey, trợ lý của bạn, đã chiếm được lưu lượng mạng trên mạng LAN của bạn trong khoảng thời gian 24 giờ, như trong Hình 1-3. Bạn muốn xem lưu lượng truy cập mạng liên quan đến người dùng kết nối với các trang web. Giao thức nào trong cột giao thức bạn nên lọc theo?

No.	Time	Source	Destination	Protocol
435	20.7784120	192.168.1.100	216.239.32.20	HTTP
436	20.7800690	24.222.0.94	192.168.1.100	DNS
437	20.7812440	192.168.1.100	24.222.0.94	DNS
438	20.7842200	24.222.0.94	192.168.1.100	DNS
439	20.7859060	192.168.1.100	24.222.0.94	DNS
440	20.7937460	24.222.0.94	192.168.1.100	DNS
441	20.7953450	192.168.1.100	24.222.0.94	DNS
442	20.8071990	24.222.0.94	192.168.1.100	DNS
443	20.8085020	192.168.1.100	24.222.0.94	DNS
444	20.8197630	192.168.1.100	8.28.16.203	TCP
445	20.8222520	192.168.1.1	239.255.255.250	SSDP
446	20.8224780	24.222.0.94	192.168.1.100	DNS

A. HTTP

B. DNS

C. TCP

D. SSDP

Câu 18: Giao thức mạng nào không thể định tuyến?

A. HTTP

B. DNS

C. NetBIOS

D. Telnet

Câu 20: Tủ nối dây của bạn bao gồm ba bộ chuyển mạch Ethernet 24 cổng được liên kết với nhau. Các máy tính từ phòng Kế toán được cắm vào từng bộ chuyển mạch Ethernet, cũng như các máy tính từ phòng Nghiên cứu. Người quản lý của bạn yêu cầu bạn đảm bảo rằng các máy tính trong phòng Kế toán nằm trên một mạng khác với các máy tính trong phòng Nghiên cứu. Bạn có thể làm gì? (Chọn hai.)

A. Thay thế các thiết bị chuyển mạch Ethernet bằng các trung tâm Ethernet.

B. Định cấu hình tất cả các máy tính Kế toán trên cùng một mạng con TCP / IP (ví dụ: 192.268.2.0 / 24) và định cấu hình tất cả các máy tính nghiên cứu trên mạng con TCP / IP của riêng chúng (ví dụ: 192.168.3.0 / 16).

C. Định cấu hình Vlan kế toán bao gồm các máy tính Kế toán và Vlan nghiên cứu bao gồm các máy tính nghiên cứu.

D. Định cấu hình tất cả các máy tính Kế toán trên cùng một mạng con TCP / IP (ví dụ: 192.168.2.0 / 24) và định cấu hình tất cả các máy tính nghiên cứu trên mạng con TCP / IP của riêng chúng (ví dụ: 192.168.3.0 / 24).

Câu 22: Phát biểu nào sau đây liên quan đến DNS là đúng? (Chọn hai.)

A. Nó phân giải tên máy tính NetBIOS thành địa chỉ IP.

B. Truy vấn máy khách đến máy chủ sử dụng cổng TCP 53.

C. Nó phân giải FQDN thành địa chỉ IP.

D. Cho một địa chỉ IP, DNS có thể trả về FQDN.

Câu 23: Giao thức nào sử dụng TCP cổng 443?

A. FTPS

B. HTTP

C. HTTPS

D. SSH

Câu 24: Bạn đang khắc phục sự cố cài đặt TCP / IP trên máy trạm. Địa chỉ IP của máy trạm là 10.17.6.8/24, cài đặt máy chủ DNS được đặt thành 199.126.129.86 và cài đặt cổng mặc định là 10.17.5.6./24. Bộ định tuyến có địa chỉ IP công cộng là 199.126.129.76/24 và địa chỉ IP nội bộ riêng là 10.17.5.6/24. Máy trạm này là trạm duy nhất trên mạng không thể kết nối với Internet. Những gì bạn nên làm?

A. Thay đổi cài đặt máy chủ DNS thành 10.17.5.6.

B. Thay đổi địa chỉ IP riêng của bộ định tuyến thành 10.17.6.6.

C. Thay đổi địa chỉ IP của máy trạm thành 10.17.5.8.

D. Thay đổi cài đặt cổng mặc định thành 199.126.129.76

Câu 26: Giao thức TCP / IP nào được thiết kế để đồng bộ hóa thời gian giữa các máy tính?

A. SNMP

B. Windows Time Service

C. NTP

D. SMTP

Câu 28: Trong khi chụp lưu lượng mạng, bạn nhận thấy một số gói được dành cho cổng UDP 69. Đây là loại lưu lượng mạng nào?

A. FTP

B. TFPT

C. SNMP

D. IMAP

Câu 29: Những giao thức TCP / IP nào sử dụng mã hóa để bảo mật truyền dữ liệu?

A. SCP, DNS, SSH

B. SSH, SCP, Telnet

C. HTTPS, FTP, SSH

D. SSH, SCP, FTPS

Câu 31: Điều nào sau đây được coi là giao thức truyền tải TCP / IP? (Chọn hai.)

A. HTTP

B. TCP

C. Telnet

D. UDP

Câu 32: Người dùng Vancouver của bạn không thể kết nối với máy chủ web của công ty được đặt tại Seattle, nhưng họ có thể kết nối với các trang web Internet. Các kỹ thuật viên mạng ở Seattle khẳng định máy chủ web đang chạy vì người dùng Seattle không gặp vấn đề gì khi kết nối với máy chủ web Seattle. Từ mạng Vancouver, bạn ping máy chủ web Seattle nhưng không nhận được phản hồi. Bạn sẽ sử dụng công cụ nào tiếp theo?

A. Tracert

B. Ipconfig

C. telnet

D. HTTP

Câu 33: Một máy trạm có địa chỉ IP là 169.254.46.86. Các quản trị viên máy chủ nhận ra dịch vụ DHCP đang ngoại tuyến, vì vậy họ bắt đầu dịch vụ DHCP. Lệnh nào sẽ được sử dụng tiếp theo trên máy trạm để ngay lập tức có được cấu hình TCP / IP hợp lệ?

A. Ping –t

B. Tracert

C. Netstat –a

D. Ipconfig/renew

Câu 34: Điều nào sau đây là cách thực hành bảo mật tốt nhất để định cấu hình bộ chuyển mạch Ethernet?

A. Vô hiệu hóa các cổng không sử dụng và gán địa chỉ MAC cho các cổng được kích hoạt.

B. Vô hiệu hóa các cổng không sử dụng và định cấu hình các cổng được kích hoạt cho bán song công.

C. Vô hiệu hóa các cổng không sử dụng và cấu hình các Vlan bổ sung.

D. Vô hiệu hóa các cổng không sử dụng và định cấu hình các cổng được kích hoạt cho song công hoàn toàn.

Câu 35: Bạn đang cố gắng kết nối với một trong những máy tính người dùng của bạn bằng RDP nhưng không thể kết nối. Một tường lửa mới đã được cài đặt trên mạng của bạn. Cổng nào phải được mở trên tường lửa để cho phép lưu lượng RDP?

A. 143

B. 389

C. 3389

D. 443

Chương 2:

Câu 2: Bạn là quản trị viên mạng cho công ty của bạn. Người quản lý của bạn đã yêu cầu bạn đánh giá các giải pháp sao lưu đám mây cho các văn phòng chi nhánh từ xa. Để áp dụng khái niệm bảo mật cơ bản này?

A. Bảo mật

B. Tính toàn vẹn

C. Có ích

D. Trách nhiệm

Câu 5: Bạn muốn gửi một tin nhắn bí mật cho một thành viên gia đình thông qua e-mail, nhưng bạn không có cách nào để mã hóa tin nhắn. Phương pháp thay thế nào sẽ cho phép bạn đạt được mục tiêu của mình?

A. PKI
B. Băm tệp tin
C. Steganography
D. Cho phép tệp tin

Câu 6: Chính sách bảo mật của công ty nhấn mạnh tính bảo mật dữ liệu và bạn phải định cấu hình các thiết bị máy tính phù hợp. Những gì bạn nên làm? (Chọn hai.)

A. Trình đọc cài đặt thẻ thông minh để người dùng có thể nhận dạng chính họ trước khi gửi tin nhắn e-mail quan trọng.
B. Thực thi mã hóa thẻ SD trên điện thoại thông minh cấp cho nhân viên.
C. Cấu hình một cụm chuyển đổi dự phòng máy chủ để đảm bảo rằng các tài liệu nhạy cảm luôn có sẵn.
D. Đặt quyền truy cập tệp và thư mục để kiểm soát quyền truy cập tệp của người dùng.

Câu 9: Ana phải gửi một tin nhắn e-mail quan trọng tới Glen, giám đốc nhân sự (HR). Chính sách của công ty nói rằng tin nhắn cho HR phải được ký điện tử. Khẳng định nào sau đây là đúng?

A. Khóa công khai của Ana được sử dụng để tạo ra chữ ký số
B. Khóa công khai của Ana được sử dụng để xác thực chữ ký số
C. Khóa công khai của Glen được sử dụng để tạo ra chữ ký số
D. Khóa công khai của Glen được sử dụng để xác thực chữ ký số

Câu 10: John đang cấp chứng chỉ kỹ thuật số cho máy tính Carolyn. Giấy chứng nhận có thể được sử dụng để làm gì? (Chọn hai.)

A. Đặt quyền trên các tệp nhạy cảm
B. Mã hóa các tệp nhạy cảm
C. Xác minh danh tính máy tính trên máy chủ để bảo mật máy chủ
D. Gửi tin nhắn e-mail được mã hóa

Câu 11: Hàng tháng, Gene tải xuống và kiểm tra các bản vá phần mềm mới nhất trước khi áp dụng chúng vào sản xuất điện thoại thông minh. Ví dụ này áp dụng cho mục tiêu bảo mật nào?

A. Bảo mật
B. Tính toàn vẹn
C. Có ích
D. An toàn

Câu 12: Bạn đang đánh giá các giải pháp lưu trữ email dựa trên đám mây công cộng. Tất cả các nhà cung cấp đều tuyên bố rằng nhiều máy chủ luôn chạy để đảm bảo hộp thư có sẵn. Đây là một ví dụ về?

A. Phân cụm
B. Steganography
C. Chữ ký hộp thư kỹ thuật số
D. trùng lặp hộp thư

Câu 13: Mạng của bạn chỉ cho phép các tập lệnh đáng tin cậy chạy trên các thiết bị được quản lý. Bạn viết một tập lệnh phải chạy trên tất cả các thiết bị được quản lý. Bạn phải làm gì Đặt các bước chính xác sau đây theo đúng thứ tự. (Chọn ba.)

A. Nhận chứng chỉ kỹ thuật số đáng tin cậy và cài đặt nó trên máy tính của bạn.
B. Xuất khóa riêng từ chứng chỉ kỹ thuật số của bạn sang tất cả các thiết bị được quản lý.

C. Tạo kịch bản.

D. Chữ ký số.

E. Trên máy tính của bạn, nhập chứng chỉ kỹ thuật số từ tất cả các thiết bị được quản lý

Câu 15: Bạn là quản trị viên máy chủ cho công ty của bạn. Bạn đang cấu hình lưu trữ đĩa như trong Hình 2-2. Cấu hình đĩa của bạn áp dụng điều khiển bảo mật nào sau đây?

A. Không tính toán (Nonrepudiation)

B. Phân cụm (Clustering)

C. Chịu lỗi (Fault tolerance)

D. Băm (Hashing)

Câu 19: Điều nào sau đây cấu thành các phương pháp xác định thích hợp từ kém an toàn nhất đến an toàn nhất?

A. Thẻ thông minh, quét võng mạc, mật khẩu

B. Quét võng mạc, mật khẩu, thẻ thông minh

C. Tên người dùng và mật khẩu, thẻ thông minh, quét võng mạc

D. ACL, tên người dùng và mật khẩu, quét võng mạc

Câu 20: Bạn đang giải thích chính sách kiểm toán tệp công ty sẽ hoạt động như thế nào đối với nhân viên CNTT mới. Đặt các mục sau theo đúng thứ tự: ___, ___, ___ và ___. **C-B-A-D**

A. Người dùng mở tệp, sửa đổi nội dung và sau đó lưu tệp.

B. Một máy chủ xác nhận kết hợp tên người dùng và mật khẩu chính xác.

C. Một người dùng cung cấp tên người dùng và mật khẩu tại màn hình đăng nhập.

D. Hoạt động tập tin được tạo bởi người dùng được ghi lại.

Câu 21: Người quản lý của bạn đã yêu cầu bạn thực hiện một giải pháp sẽ ngăn người dùng xem các trang web không phù hợp. Bạn nên sử dụng giải pháp nào?

A. Bộ định tuyến ACL

B. Quyền truy cập trang web

C. Máy chủ proxy

D. Chứng thư số

Câu 23: Sean đang nắm bắt lưu lượng mạng Wi-Fi bằng cách sử dụng bộ phân tích gói và có thể đọc nội dung truyền qua mạng. Những gì có thể được thực hiện để giữ truyền dẫn mạng riêng tư?

A. Cài đặt chứng chỉ số trên mỗi thiết bị truyền.

B. Đặt mật khẩu quản trị viên mạnh cho bộ định tuyến Wi-Fi.

C. Sử dụng xác thực thẻ thông minh.

D. Mã hóa lưu lượng Wi-Fi.

Câu 24: Những cơ chế bảo mật nào có thể được sử dụng cho mục đích không tính toán? (Chọn hai.)

A. Mã hóa
B. Phân cụm
C. Kiểm toán
D. Chữ ký số

Câu 25: Bạn là quản trị viên mạng cho một dược phẩm. Tháng trước, công ty đã thuê một bên thứ ba để thực hiện kiểm toán bảo mật. Từ kết quả kiểm toán, bạn biết rằng khách hàng của dữ liệu y tế bí mật không được bảo mật đúng cách. Những khái niệm bảo mật đã bị bỏ qua trong trường hợp này?

A. Due diligence
B. Due care
C. Due process
D. Separation of duties

Câu 26: Điều nào sau đây là ví dụ tốt nhất về vai trò bảo mật của người giám sát? (Chọn ba.)

A. Nhân viên phòng nhân sự
B. Điều hành sao lưu máy chủ
C. CEO
D. Nhân viên thi hành qui tắc đáng tin cậy xuất trình rõ ràng
E. Điều hành bán hàng

Câu 29: Chọn ví dụ tốt nhất về xác thực từ các mục sau:

A. Mỗi sáng, quản trị viên mạng truy cập các trang web khác nhau để tìm lỗ hổng Windows Server mới nhất.
B. Trước khi hai hệ thống liên lạc với nhau qua mạng, chúng trao đổi chứng chỉ PKI để đảm bảo chúng có chung một gốc.
C. Một máy chủ tập tin có hai nguồn cung cấp trong trường hợp một không thành công.
D. Một ứng dụng có một số hành vi ngoài ý muốn có thể cho phép người dùng độc hại ghi vào sổ đăng ký Windows.

Câu 30: Raylee là quản trị viên mạng mới cho một công ty luật. Cô nghiên cứu các cấu trúc và quyền của thư mục máy chủ tệp hiện có và nhanh chóng nhận ra rằng quản trị viên trước đó không bảo mật đúng cách các tài liệu pháp lý trong các thư mục này. Cô đặt quyền truy cập tệp và thư mục phù hợp để đảm bảo rằng chỉ những người dùng phù hợp mới có thể truy cập dữ liệu, dựa trên chính sách của công ty. Raylee đã đảm nhận vai trò bảo mật nào?

A. Người giám sát
B. Chủ sở hữu dữ liệu
C. Người dùng
D. Người chi phối

Câu 31: Từ danh sách sau đây, mô tả tốt nhất xác thực?

A. Đăng nhập vào máy chủ TFTP bằng tên người dùng và mật khẩu
B. Sử dụng tên người dùng, mật khẩu và thẻ mã thông báo để kết nối với VPN công ty
C. Kiểm tra thư trên web của công ty trên một trang web được bảo mật tại http://owa.acme.com sau khi cung cấp thông tin đăng nhập
D. Sao chép tệp từ máy chủ sang ổ flash USB

Câu 32: Trong khi thử nghiệm với các cấu hình mạng máy chủ khác nhau, bạn phát hiện ra một điểm yếu không xác định trong hệ điều hành máy chủ có thể cho phép kẻ tấn công từ xa kết nối với máy chủ với các đặc quyền quản trị. Bạn đã phát hiện ra điều gì?

A. Khai thác
B. Lỗi
C. Nhược điểm
D. Từ chối dịch vụ

Câu 33: Sean là một nhà tư vấn bảo mật và đã được thuê để thực hiện một bài kiểm tra thâm nhập mạng đối với mạng khách hàng của anh ấy. Vai trò của Sean Quay được mô tả tốt nhất như sau:

A. Hacker mũ trắng
B. Hacker mũ đen
C. Hacker mũ xám
D. Hacker mũ tím

Câu 34: Điều nào sau đây được phân loại là giải pháp sẵn có? (Chọn hai.)

A. Kiểm toán
B. . RAID
C. . Sao lưu máy chủ tệp
D. Xác thực thẻ thông minh

Câu 35: Bạn đang xem xét bảo mật tài liệu trên máy chủ tài liệu đám mây riêng của mình. Bạn nhận thấy nhân viên trong bộ phận Bán hàng đã được cấp toàn quyền cho tất cả các tài liệu dự án. Nhân viên bán hàng chỉ nên đọc quyền đối với tất cả các tài liệu dự án. Nguyên tắc bảo mật nào đã bị vi phạm?

A. Tách nhiệm vụ
B. Đặc quyền tối thiểu
C. Luân chuyển công việc
D. Toàn vẹn

Câu 36: Một người dùng, Sylvain, tải xuống một khai thác lợi dụng lỗ hổng trang web. Không có kiến thức chi tiết về khai thác, Sylvain chạy mã độc đối với nhiều trang web mà anh ta muốn truy cập. Nhãn nào xác định tốt nhất Sylvain?

A. Hacker mũ trắng
B. Kiddie kịch bản
C. Hacker mũ đỏ
D. Thử nghiệm thâm nhập

Câu 37: Which term refers to individuals who use computer hacking to promote a political or ideological agenda?

A. Scriptivist
B. Script kiddie
C. Black-hat hacker
D. Hacktivist

Câu 38: Khi lập kế hoạch cơ sở hạ tầng mạng của bạn, bạn quyết định sử dụng phương pháp tường lửa phân lớp giữa Internet và mạng nội bộ của bạn. Những loại tường lửa bạn cũng nên sử dụng?

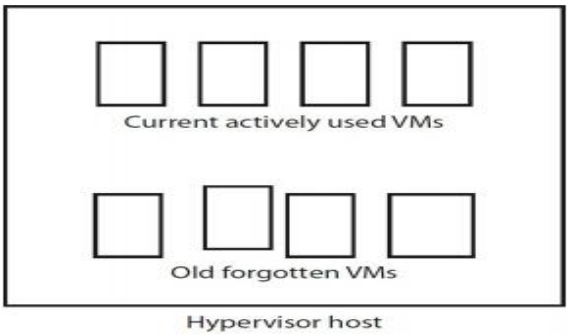
A. Quy tắc ACL cuối cùng sẽ cho phép tất cả.

B. Sử dụng các thiết bị tường lửa từ các nhà cung cấp khác nhau.

C. Quy tắc ACL đầu tiên nên từ chối tất cả.

D. Sử dụng các thiết bị tường lửa từ cùng một nhà cung cấp.

Câu 39: Tham khảo hình 2-3. Thuật ngữ nào mô tả chính xác vấn đề trong hình?



A. VM sprawl

B. VM overload

C. VM shielding

D. VM shadowing

Câu 40: Những kỹ thuật ứng dụng kiểm tra phát hiện ra xử lý đầu vào không đúng cách?

A. Fuzzing

B. Overloading (Quá tải)

C. Penetration test

D. Vulnerability scan (Quét lỗ hổng)

Câu 41: Loại công cụ nào được sử dụng để trinh sát để thu thập và phân tích thông tin công khai về một tổ chức?

A. Bộ dữ liệu lớn (big data suite)

B. Gói sniffer (Packet sniffer)

C. mã nguồn mở thông minh (Open source intellige)

D. Kỹ thuật xã hội (social engineering)

Câu 42: Vấn đề lập trình nào bắt nguồn từ nhiều luồng không thực hiện theo mô hình tuần tự dự đoán được?

A. Fuzzing

B. Màn hình xanh chết

C. Điều khiển đa lõi

D. Race conditition (???)

Câu 43: Công ty của bạn có kế hoạch sử dụng nhiều thiết bị Internet of Things (IoT) trong cơ sở để kiểm soát ánh sáng và nhiệt độ. Bạn đề nghị với ban quản lý rằng việc sử dụng các thiết bị IoT có nhiều rủi ro bảo mật. Điều nào sau đây là vấn đề bảo mật được biết đến với nhiều thiết bị IoT?

A. Sử dụng Telnet

B. Không thể cập nhật firmware nhúng

C. Sử dụng SSH

D. Không có khả năng ghi lại các sự kiện

Câu 44: Jim là một kỹ thuật viên CNTT cho một phòng khám y tế cỡ trung bình. Phòng khám gần đây đã mua bốn điểm truy cập không dây để đảm bảo các thiết bị y tế trong một tầng của tòa nhà. Jim đã cài đặt các điểm truy cập ở những vị trí tốt nhất để phủ sóng tín hiệu và sau đó thay đổi mật khẩu WPA2. Jim đã phạm sai lầm gì?

A. Jim nên đã kích hoạt WEP.
B. Không nên sử dụng quá hai điểm truy cập do nhiễu.
C. Jim nên đã kích hoạt WPA.
D. Cấu hình quản trị viên mặc định được giữ nguyên.

Câu 46: Một phần mềm độc hại thay thế một thư viện mã được sử dụng khi cần thiết bởi một chương trình kiểm soát. Tên gì mô tả loại vấn đề an toàn này?

A. DLL injection
B. Con trỏ
C. tràn số nguyên
D. Tràn bộ đệm

CHƯƠNG 3:

Câu 1: mục đích chính của các chính sách bảo mật là?
A. Thiết lập các căn cứ pháp lý để truy tố
B. Cải thiện hiệu suất dịch vụ CNTT
C. Giảm nguy cơ vi vi phạm an toàn
D. Đảm bảo rằng người dùng chịu trách nhiệm cho nhiệm vụ của họ

Câu 2: Bạn đã được giao nhiệm vụ tạo chính sách bảo mật cho công ty liên quan tới cách sử dụng điện thoại thông minh cho mục đích kinh doanh?
A. Phát hành điện thoại thông minh cho tất cả các nhân viên
B. Đạt được sự ủng hộ từ quản lý
C. Lấy ý kiến pháp lý
D. Tạo bản thảo đầu tiên của chính sách

Câu 4: Christine là quản trị viên máy chủ của tập đoàn Concoto. Quản lý của cô cung cấp từng bước phác thảo chính sách bảo mật cách máy chủ được cấu hình để tối đa hóa an ninh. Christine sẽ thực hiện những loại chính sách bảo mật nào?
A. Sử dụng chính sách Mailserver
B. Sử dụng chính sách VPN
C. Chính sách thủ tục
D. Sử dụng chính sách máy chủ tệp

Câu 5: Điều nào sau đây là ví dụ về PII? (chọn hai)
A. Địa chỉ IP riêng trên mạng nội bộ
B. Số điện thoại di động
C. Chứng chỉ số
D. Gender (???)

Câu 6: Sau quá trình kiểm tra lý lịch và phỏng vấn kéo dài, công ty của bạn đã thuê một nhân viên biên chế mới có tên là Stacey. Stacey sẽ sử dụng trình duyệt web trên máy tính của công ty tại văn phòng để truy cập ứng dụng bảng lương trên trang web của nhà cung cấp đám mây công cộng qua Internet. Stacey nên đọc và ký loại tài liệu nào?

A. Chính sách sử dụng Internet được chấp nhận

B. Chính sách mật khẩu

C. Thỏa thuận cấp độ dịch vụ

D. Chính sách sử dụng truy cập từ xa được chấp nhận

Câu 7: Bạn đang cấu hình chính sách mật khẩu cho người dùng trong văn phòng Berlin. Mật khẩu phải được thay đổi sau mỗi 60 ngày. Bạn phải đảm bảo rằng mật khẩu người dùng không thể thay đổi nhiều lần trong khoảng thời gian 60 ngày. Bạn nên cấu hình cái gì?

A. Tuổi mật khẩu tối thiểu

B. Tuổi mật khẩu tối đa

C. Độ phức tạp của mật khẩu

D. Lịch sử mật khẩu

Câu 8: Bạn đã được thuê làm tư vấn bởi một công ty dược phẩm. Công ty lo ngại rằng các tài liệu nghiên cứu thuốc bí mật có thể được phục hồi từ các đĩa cứng bị loại bỏ. Bạn nên giới thiệu gì?

A. Định dạng đĩa cứng.

B. Phân vùng lại các đĩa cứng.

C. Đóng băng các ổ cứng.

D. Vật lý xé nhỏ đĩa cứng.

Câu 9: Acme Corporation đang nâng cấp bộ định tuyến mạng của mình. Các bộ định tuyến cũ sẽ được gửi đến trụ sở chính trước khi chúng được xử lý. Những gì phải được thực hiện cho các bộ định tuyến trước khi xử lý để giảm thiểu vi phạm an ninh?

A. Thay đổi mật khẩu chế độ đặc quyền của bộ định tuyến.

B. Loại bỏ các mục máy chủ DNS khỏi cấu hình bộ định tuyến.

C. Đặt bộ định tuyến về cài đặt mặc định của nhà sản xuất.

D. Định dạng ổ cứng bộ định tuyến.

Câu 10: Công ty của bạn đã quyết định áp dụng giải pháp quản lý thiết bị đám mây công cộng, nơi tất cả các thiết bị được quản lý tập trung từ một trang web được lưu trữ trên các máy chủ trong một trung tâm dữ liệu. Quản lý đã hướng dẫn bạn đảm bảo rằng giải pháp đáng tin cậy và luôn có sẵn. Những loại tài liệu bạn nên tập trung vào?

A. Chính sách mật khẩu

B. Thỏa thuận cấp độ dịch vụ

C. Chính sách sử dụng truy cập từ xa được chấp nhận

D. Chính sách sử dụng thiết bị di động được chấp nhận

Câu 11: Điều nào sau đây tốt nhất thể hiện khái niệm đặc quyền tối thiểu?

A. Phát hiện sử dụng Internet không phù hợp

B. Phát hiện phần mềm độc hại đang chạy mà không có đặc quyền nâng cao

C. Gán cho người dùng toàn quyền kiểm soát tài nguyên mạng

D. Gán các quyền cần thiết để cho phép người dùng hoàn thành nhiệm vụ

Câu 12: Việc tạo ra các chính sách bảo mật dữ liệu bị ảnh hưởng nhiều nhất bởi hai yếu tố nào? (Chọn hai.)

A. Quy định của ngành
B. Sơ đồ địa chỉ IP đang được sử dụng
C. Phiên bản hệ điều hành đang được sử dụng
D. PII

Câu 14: Bạn đang xem lại cảnh quay camera giám sát sau khi các mục bị mất tích từ văn phòng công ty của bạn vào buổi tối. Trên video, bạn nhận thấy một người không xác định bước vào lối vào chính của tòa nhà phía sau một nhân viên đã mở khóa cửa bằng thẻ quẹt. Loại vi phạm an toàn này là gì?

A. Tailgating
B. Mantrapping
C. Horseback riding
D. Door jamming

Câu 16: Bạn đang kiểm tra cấu hình bộ định tuyến của mình và phát hiện ra lỗ hổng bảo mật. Sau khi tìm kiếm trên Internet, bạn nhận ra rằng lỗ hổng này chưa được biết. Loại tấn công nào là bộ định tuyến của bạn dễ bị công kích?

A. Từ chối dịch vụ
B. Tấn công lừa đảo
C. Khai thác zero-day
D. Ping of death

Câu 17: Lựa chọn nào sau đây mô tả đúng nhất cách sử dụng PII đúng cách? (Chọn hai.)

A. Thực thi pháp luật theo dõi một người phạm tội Internet sử dụng địa chỉ IP công cộng
B. Phân phối danh sách liên hệ email đến các công ty tiếp thị
C. Đăng nhập vào máy tính xách tay bảo mật bằng máy quét dấu vân tay
D. Due diligence (???)

Câu 18: Công ty của bạn hạn chế quản trị viên tường lửa sửa đổi nhật ký tường lửa. Chỉ nhân viên an ninh CNTT mới được phép làm điều này. Đây là một ví dụ về?

A. Bảo dưỡng đúng hạn (Due care)
B. Phân chia nhiệm vụ
C. Nguyên tắc đặc quyền tối thiểu
D. Sử dụng được chấp nhận (Acceptable use)

Câu 19: Bạn là quản trị viên mạng cho một sự cố. Người dùng ở Vancouver phải có thể xem các bí mật thương mại để nộp bằng sáng chế. Bạn chia sẻ thư mục mạng có tên Trade Secrets và cho phép các quyền NTFS sau:
Vancouver_Staff: Đọc, liệt kê nội dung thư mục
Giám đốc điều hành: Viết
IT_Adins: FullControl
Về nhân viên Vancouver, nguyên tắc nào đang được tôn trọng?

A. Luân chuyển công việc
B. Đặc quyền tối thiểu
C. Kỳ nghỉ bắt buộc
D. Phân chia nhiệm vụ

Câu 20: ISP địa phương của bạn cung cấp tệp PDF cho biết khả năng cung cấp dịch vụ 99,97 % cho kết nối T1 với Internet. Làm thế nào bạn sẽ phân loại loại tài liệu này?

A. Bí mật hàng đầu
B. Chính sách sử dụng được chấp nhận
C. Thỏa thuận cấp độ dịch vụ
D. Có ích

Câu 21: Bộ phận Tài khoản phải trả thông báo các giao dịch mua ngoài nước lớn được thực hiện bằng thẻ tín dụng doanh nghiệp. Sau khi thảo luận vấn đề với Juan, nhân viên có tên trong thẻ tín dụng, họ nhận ra ai đó đã lấy bất hợp pháp các chi tiết thẻ tín dụng. Bạn cũng biết rằng gần đây anh ta đã nhận được một e-mail từ công ty thẻ tín dụng yêu cầu anh ta đăng nhập vào trang web của họ để xác thực tài khoản của mình, điều mà anh ta đã làm. Làm thế nào điều này có thể tránh được?

A. Cung cấp cho chủ thẻ tín dụng thẻ thông minh.
B. Nói với người dùng để tăng sức mạnh của mật khẩu trực tuyến.
C. Cài đặt tường lửa dựa trên máy trạm.
D. Cung cấp đào tạo nâng cao nhận thức an ninh cho nhân viên.

Câu 22: Khẳng định nào sau đây là đúng? (Chọn hai.)

A. **Nhãn bảo mật được sử dụng để phân loại dữ liệu như hạn chế và tối mật**.
B. PII chỉ áp dụng cho các thiết bị xác thực sinh trắc học.
C. Buộc thay đổi mật khẩu người dùng được coi là quản lý thay đổi.
D. Một chữ ký người trên séc được coi là PII.

Câu 23: Điều nào sau đây minh họa tốt nhất các vấn đề bảo mật tiềm ẩn liên quan đến các trang mạng xã hội?

A. Người dùng khác có thể dễ dàng nhìn thấy địa chỉ IP của bạn.
B. Nhân viên biết nói có thể tiết lộ một công ty sở hữu trí tuệ.
C. Người dùng độc hại có thể sử dụng hình ảnh của bạn để chụp ảnh bản đồ (steganography).
D. Số thẻ tín dụng của bạn dễ dàng bị đánh cắp.

Câu 24: Là nhân viên bảo mật CNTT, bạn thiết lập chính sách bảo mật yêu cầu người dùng bảo vệ tất cả các tài liệu giấy để dữ liệu khách hàng, nhà cung cấp hoặc công ty nhạy cảm không bị đánh cắp. Đây là loại chính sách gì?

A. Quyền riêng tư
B. Sử dụng được chấp nhận
C. Clean desk
D. Mật khẩu

Câu 25: Mục đích chính của việc thực thi một chính sách nghỉ phép bắt buộc là gì?

A. Tuân thủ quy định của chính phủ
B. Để đảm bảo rằng nhân viên được làm mới
C. Để cho phép các nhân viên khác trải nghiệm các vai trò công việc khác
D. Để ngăn chặn hoạt động không đúng

Câu 26: Chính sách bảo mật bảo vệ cái gì?

A. Dữ liệu khách hàng
B. Giao dịch bí mật
C. Thư mục nhà của nhân viên

D. Cấu hình tường lửa

Câu 27: Phát biểu nào sau đây về chính sách bảo mật là đúng? (Chọn hai.)

A. Người dùng phải đọc và ký chính sách bảo mật.

B. Nó đảm bảo mức độ thời gian hoạt động cho các dịch vụ CNTT.

C. Nó bao gồm các tài liệu phụ.

D. Phải có sự phê duyệt của ban quản lý.

Câu 28: Bạn đang phát triển một đề cương đào tạo bảo mật cho bộ phận Kế toán sẽ diễn ra trong văn phòng. Hai mục không nên được đưa vào đào tạo? (Chọn hai.)

A. Cấu hình tường lửa

B. Bộ phận kế toán hỗ trợ các sáng kiến bảo mật

C. An toàn vật lý

D. Kỹ thuật xã hội

Câu 29: Chọn phát biểu đúng:

A. Người dùng được chỉ định nhãn phân loại để truy cập dữ liệu nhạy cảm.

B. Dữ liệu được chỉ định mức giải phóng mặt bằng để truy cập dữ liệu nhạy cảm.

C. Dữ liệu được chỉ định mức giải phóng mặt bằng để bảo vệ dữ liệu nhạy cảm.

D. Người dùng được chỉ định mức giải phóng mặt bằng để truy cập dữ liệu nhạy cảm.

Câu 30: Bạn là quản trị viên máy chủ tệp cho một tổ chức y tế. Quản lý đã yêu cầu bạn định cấu hình máy chủ của mình để phân loại các tệp chứa dữ liệu lịch sử y tế của bệnh nhân một cách thích hợp. Phân loại dữ liệu phù hợp cho các loại tệp này là gì? (Chọn tất cả các áp dụng.)

A. Cao

B. Trung bình

C. Thấp

D. Riêng tư

E. Công khai

F. Bảo mật

Câu 31: Bạn đang định cấu hình mạng Wi-Fi cho cửa hàng bán lẻ quần áo. Theo quy định của Ngành Thẻ thanh toán (PCI) đối với các công ty xử lý thẻ thanh toán, bạn phải đảm bảo thay đổi mật khẩu mặc định trên bộ định tuyến không dây. Điều này được mô tả tốt nhất là:

A. Chính sách PCI

B. Tuân thủ các tiêu chuẩn bảo mật

C. Giáo dục và nhận thức người dùng

D. Chính sách Wi-Fi

Câu 32: Công ty của bạn cung cấp một máy hủy tài liệu giấy trên mỗi tầng của tòa nhà. Vấn đề bảo mật nào giải quyết vấn đề này?

A. Xử lý dữ liệu

B. Chính sách Clean desk

C. Xếp hàng

D. Mantrap

Câu 33: Chính sách của công ty bạn BYOD trả tiền hàng tháng cho nhân viên sử dụng điện thoại cho mục đích công việc. Công ty nên đảm bảo loại ứng dụng nào được cài đặt và chạy trên tất cả các điện thoại thông minh BYOD?

A. Ứng dụng thời tiết

B. Ứng dụng eBay

C. Ứng dụng đọc PDF

D. Ứng dụng chống vi-rút

Câu 34: Bảo vệ tốt nhất chống lại virus mới là gì?

A. Luôn cập nhật các định nghĩa chống vi-rút

B. Tắt máy tính khi không sử dụng

C. Không kết nối với mạng Wi-Fi

D. Sử dụng chứng chỉ số để xác thực

Câu 35: Bạn và nhóm CNTT của bạn đã hoàn thành việc soạn thảo các chính sách bảo mật để sử dụng e-mail và truy cập từ xa thông qua VPN của công ty. Người dùng hiện đang sử dụng cả e-mail và VPN. Phải làm gì tiếp theo? (Chọn hai.)

A. Cập nhật chương trình cơ sở thiết bị VPN.

B. Cung cấp đào tạo nâng cao nhận thức người dùng bảo mật.

C. Mã hóa tất cả thư người dùng.

D. Bắt buộc kiểm tra nhận thức bảo mật cho người dùng

Câu 36: Margaret, người đứng đầu bộ phận nhân sự, thực hiện một cuộc phỏng vấn với một kỹ thuật viên máy chủ CNTT đang rời đi có tên là Irving. Cuộc phỏng vấn bao gồm quan điểm của Irving, về tổ chức, lợi ích của vai trò công việc mà anh ta nắm giữ và những cải tiến tiềm năng có thể được thực hiện. Vấn đề nào sau đây cũng cần được giải quyết trong cuộc phỏng vấn thoát?

A. Kiểm tra lý lịch

B. Luân chuyển công việc

C. Thỏa thuận không tiết lộ (Nondisclosure agreement)

D. Hình thức hoàn trả tài sản

Câu 37: Một nhân viên an ninh CNTT đang cấu hình các tùy chọn nhãn dữ liệu cho máy chủ tệp nghiên cứu của công ty. Người dùng hiện có thể gắn nhãn tài liệu là công khai, nhà thầu hoặc nguồn nhân lực. Đối với giao dịch bí mật của công ty, nên sử dụng nhãn nào?

A. Độc quyền

B. Cao

C. Thấp

D. Bí mật hàng đầu

Câu 39: Một kiểm toán viên bảo mật đang cố gắng xác định một tổ chức sao lưu dữ liệu và chiến lược lưu trữ dài hạn của tổ chức. Những loại tài liệu tổ chức mà kiểm toán viên nên tham khảo?

A. Chính sách bảo mật

B. Chính sách lưu giữ dữ liệu

C. Chính sách rò rỉ dữ liệu

D. Chính sách sử dụng máy chủ tệp chấp nhận được

Chương 4:

Câu 1. Bạn đang kiểm tra một hệ thống người dùng sau khi cô ấy phàn nàn về việc sử dụng Internet chậm. Sau khi phân tích hệ thống, bạn nhận thấy rằng địa chỉ MAC của cổng mặc định trong bộ đệm ARP đang tham chiếu sai địa chỉ MAC. Những kiểu tấn công đã xảy ra?

A. Brute force
B. DNS poisoning
C. Buffer overflow
D. ARP poisoning

Câu 2. Bạn muốn thực hiện kiểm soát bảo mật giới hạn điều chỉnh trong môi trường bảo mật cao. Bạn sẽ sử dụng biện pháp kiểm soát bảo vệ nào sau đây?

A. Thẻ quẹt
B. Mantrap
C. Khóa cửa (Looked door)
D. Cài đặt CMOS

Câu 3. Mô tả nào sau đây mô tả đúng nhất về một cuộc tấn công tràn bộ đệm?

A. Tiêm mã cơ sở dữ liệu vào một trang web
B. Sử dụng tệp từ điển để bẻ khóa mật khẩu
C. Gửi quá nhiều dữ liệu cho một ứng dụng cho phép tin tặc chạy mã tùy ý
D. Thay đổi địa chỉ nguồn của gói

Câu 7. Tin tặc nào sau đây có thể sửa đổi sau khi có quyền truy cập vào hệ thống của bạn để đạt được chuyển hướng DNS?

A. / etc / passwd
B. Hosts
C. SAM
D. Services

Câu 8. Kiểu tấn công nào liên quan đến việc hacker gửi quá nhiều dữ liệu đến một dịch vụ hoặc ứng dụng thường dẫn đến việc hacker có quyền truy cập quản trị vào hệ thống?

A. Birthday attack
B. Typo squatting/URLhijacking
C. Eavesdrop (nghe lén)
D. Buffer overflow

Câu 9. Phương pháp nào sau đây có thể được sử dụng để ngăn ngừa ngộ độc ARP trên mạng? (Chọn hai.)

A. Các mục ARP tĩnh
B. Patching
C. Phần mềm chống vi-rút
D. An toàn vật lý
E. Tường lửa

Câu 10. Là quản trị viên mạng, bạn nên làm gì để ngăn chặn các cuộc tấn công tràn bộ đệm xảy ra trên hệ thống của mình?

A. Các mục ARP tĩnh
B. Phần mềm chống vi-rút

C. An toàn vật lý

D. Patching

Câu 11. Điều nào sau đây là thuật ngữ cho một tên miền được đăng ký và bị xóa liên tục để người đăng ký có thể tránh phải trả tiền cho tên miền?

A. Chuyển hướng DNS

B. Domain poisoning

C. Domain kiting

D. Transitive access

Câu 14. Người quản lý của bạn đã đảm bảo rằng một chính sách được thực thi đòi hỏi tất cả nhân viên phải băm nhỏ các tài liệu nhạy cảm. Loại tấn công nào mà người quản lý của bạn hy vọng ngăn chặn?

A. Xếp hàng (Tailgating)

B. Từ chối dịch vụ

C. Kỹ thuật xã hội (Social engineering)

D. Dumpster diving

Câu 18. Điều nào sau đây mô tả đúng nhất về cuộc tấn công zero-day?

A. Một cuộc tấn công sửa đổi địa chỉ nguồn của gói

B. Một cuộc tấn công làm thay đổi ngày hệ thống máy tính thành 00/00/00

C. Một cuộc tấn công không bao giờ xảy ra

D. Một cuộc tấn công sử dụng khai thác mà nhà cung cấp sản phẩm chưa biết

Câu 19. Loại tệp nào trên ổ cứng của bạn lưu trữ các tùy chọn từ các trang web?

A. Cookie

B. Hosts

C. LMHOSTS

D. Attachments

Câu 20. Kiểu tấn công nào liên quan đến việc hacker ngắt kết nối một trong các bên khỏi liên lạc và tiếp tục liên lạc trong khi mạo danh hệ thống đó?

A. Cookie

B. Hosts

C. LMHOSTS

D. Attachments

Câu 21. Kiểu tấn công mật khẩu nào liên quan đến việc sử dụng tệp từ điển và sửa đổi các từ trong tệp từ điển?

A. Dictionary attack

B. Brute-force attack

C. Hybrid attack

D. Modification attack

Câu 23. Ba nhân viên trong công ty đã nhận được các cuộc gọi từ một cá nhân hỏi về thông tin tài chính cá nhân. Những kiểu tấn công đang xảy ra?

A. Phishing

B. Whaling

C. Tailgating

D. Vishing

Câu 25. Jeff gần đây báo cáo rằng anh ta đang nhận được một số lượng lớn tin nhắn văn bản không mong muốn đến điện thoại của mình. Những kiểu tấn công đang xảy ra?

A. Bluesnarfing

B. Whaling

C. Bluejacking

D. Packet sniffing

Câu 26. Một nhân viên bị nghi ngờ tiết lộ bí mật của công ty với đối thủ cạnh tranh. Sau khi thu giữ máy tính xách tay của nhân viên, các nhà phân tích pháp y thông báo rằng có một số hình ảnh cá nhân trên máy tính xách tay đã được gửi qua email cho bên thứ ba trên Internet. Khi nhà phân tích so sánh giá trị băm của các hình ảnh cá nhân trên ổ cứng với những gì được tìm thấy trong hộp thư của nhân viên, các giá trị băm không khớp. Đã như thế nào Nhân viên chia sẻ bí mật công ty?

A. Chữ kí số

B. Steganography

C. MP3Stego

D. Whaling

Câu 27. Bạn đến nơi làm việc hôm nay để tìm ai đó bên ngoài tòa nhà đang đào qua ví của họ. Khi bạn đến gần cửa, người này nói, tôi đã quên đường chuyền ở nhà. Tôi có thể đi với bạn không? Loại hình tấn công nào có thể xảy ra?

A. Tailgating

B. Dumpster diving

C. Brute force

D. Whaling

Câu 28. Người quản lý của bạn đã yêu cầu các khóa kết hợp được sử dụng để bảo đảm các khu vực khác nhau của cơ sở công ty phải được thay thế bằng thẻ quẹt điện tử. Loại tấn công kỹ thuật xã hội nào mà người quản lý của bạn hy vọng tránh được với sự thay đổi này?

A. Hoaxes

B. Tailgating

C. Dumpster diving

D. Shoulder surfing

Câu 29. Người quản lý của bạn đã được nghe rất nhiều về các cuộc tấn công kỹ thuật xã hội và tự hỏi tại sao các cuộc tấn công như vậy lại hiệu quả đến vậy. Điều nào sau đây xác định lý do tại sao các cuộc tấn công rất thành công? (Chọn ba.)

A. Authority

B. DNS poisoning

C. Urgency

D. Brute force

E. Trust

Câu 31. Một người dùng gọi và yêu cầu bạn gửi các tài liệu nhạy cảm ngay lập tức vì nhân viên bán hàng cần họ để đóng một thỏa thuận trị giá hàng triệu đô la và các tệp của họ bị hỏng. Đây là hình thức kỹ thuật xã hội nào?

A. Familiarity

B. Intimidation
C. Consensus
D. Scarcity
Câu 32. Kẻ tấn công lừa người dùng nhấp vào liên kết độc hại gây ra hành động không mong muốn trên trang web mà người dùng hiện đang được xác thực. Đây là loại khai thác gì?
A. Cross-site request forgery
B. Cross-site scripting
C. Replay
D. Pass the hash
Câu 33. Máy chủ của bạn đang tràn ngập các yêu cầu tra cứu DNS và điều này khiến máy chủ không khả dụng cho các máy khách hợp pháp. Đây là loại tấn công chung nào?
A. Tràn bộ đệm
B. Đánh cắp tên miền
C. Man-in-the-browser
D. Khuếch đại (Amplification)
Câu 34. Một người dùng gọi cho bạn nói rằng trình duyệt của anh ta đã thực hiện một hành động ngoài ý muốn sau khi anh ta nhấp vào nút trên trang web. Những kiểu tấn công đã diễn ra?
A. Replay
B. Shimming
C. Click-jacking
D. Integer overflow
Câu 35. Trình điều khiển phần cứng được tải xuống không khớp với tổng kiểm tra từ nhà sản xuất, nhưng nó cài đặt và dường như hoạt động như bình thường. Nhiều tháng sau, bạn biết rằng thông tin nhạy cảm từ thiết bị của bạn đã bị rò rỉ trực tuyến. Thuật ngữ nào mô tả đúng nhất về loại tấn công này?
A. Refactoring
B. Collision
C. ARP poisoning
D. Typo squatting
Câu 36. Một người dùng đang cố đăng nhập vào một ứng dụng web nhưng thông báo rằng phiên bản TLS đang được sử dụng thấp hơn dự kiến. Đây là loại tấn công nào?
A. Weak implementations
B. Known plain text/cipher text
C. Downgrade
D. Replay

CHƯƠNG 5

2. các báo cáo sau đây là đúng? (Chọn hai.)
A. Worms đăng nhập tất cả các ký tự gõ vào một tập tin văn bản.
B. Worms tuyên truyền mình vào hệ thống khác.
C. Worms có thể mang virus.
D. sâu lây nhiễm đĩa cứng MBR.

3. một trong những người dùng của bạn, Christine, báo cáo rằng khi cô thăm các trang web, quảng cáo bật lên xuất hiện không ngừng. Sau khi điều tra thêm, bạn tìm hiểu một trong những trang web cô đã truy cập đã bị nhiễm Flash Mã. Christine hỏi những gì đã được vấn đề. Những gì bạn nói với cô ấy gây ra vấn đề?
A. Cross-Site tấn công kịch bản
B. Worm
C. adware
D. Spyware
4. Mô tả tốt nhất định nghĩa một vi rút máy tính?
A. một chương trình máy tính mà sao chép chính nó
B. một tập tin với một phần mở rộng tập tin. VBS
C. một chương trình máy tính thu thập thông tin người dùng
D. một chương trình máy tính chạy hành động độc hại
7. một người sử dụng báo cáo vấn đề bàn phím USB. Bạn kiểm tra sau của máy tính để đảm bảo bàn phím là kết nối đúng và nhận thấy một đầu nối nhỏ giữa bàn phím và cổng USB máy tính.
Sau khi điều tra, bạn biết rằng phần cứng này bắt tất cả mọi thứ một loại người dùng in Loại gì
của phần cứng là điều này?
A. SmartCard
B. Trojan
C. Keylogger
D. PS/2 chuyển đổi
9. nào sau đây là sự thật về backdoors? (Chọn hai.)
A. họ là mã độc hại.
B. họ cho phép người sử dụng từ xa truy cập vào cổng TCP 26.
C. họ được thực hiện có thể truy cập thông qua Rootkits.
D. họ cung cấp quyền truy cập vào tài khoản root Windows.
10. bạn đang lưu trữ một cuộc họp bảo mật CNTT liên quan đến an ninh phòng physicalserver. Một đồng nghiệp, Syl, đề nghị
Thêm CMOS cứng cho các chính sách bảo mật máy chủ hiện tại. Những loại đe dọa an ninh là những gì Sylám
Để?
A. thay đổi lượng RAM cài đặt
B. thay đổi cài đặt của CPU throttling
C. thay đổi thứ tự khởi động
D. thay đổi thiết đặt quản lý nguồn điện
11. bạn là cán bộ an ninh CNTT cho một bộ phận của chính phủ. Bạn đang sửa đổi chính sách bảo mật USB. Những khoản mục áp dụng cho bảo mật USB? (Chọn hai.)
A. không cho phép ổ USB bên ngoài lớn hơn 1TB.
B. vô hiệu hoá cổng USB.
C. ngăn chặn dữ liệu của công ty bị sao chép sang thiết bị USB trừ khi mã hóa thiết bị USB Kích hoạt.
D. ngăn chặn dữ liệu của công ty bị sao chép sang thiết bị USB trừ khi mã hóa cổng USB được bật.
12. những điều sau đây không được coi là mối đe dọa điện thoại di động nghiêm trọng? (Chọn hai.)

A. hacker với các thiết bị phải đặt ra như là tháp tế bào
B. có Bluetooth cho phép
C. thay đổi thứ tự khởi động
D. Ransomware
13. những gì được định nghĩa là việc truyền tải các tin nhắn số lượng lớn không chào đón?
A. Worm
B. ping của cái chết
C. thư rác
D. DOS
14. những công nghệ tách lưu trữ từ máy chủ?
A. router
B. Switch
C. NAS
D. bộ định tuyến không dây
15. bạn có trách nhiệm xác định những công nghệ sẽ cần thiết trong một không gian văn phòng mới. Nhân viên sẽ cần một mạng duy nhất để chia sẻ dữ liệu, các cuộc gọi thoại truyền thống, cuộc gọi VoIP, hộp thư thoại, và các dòch vuï nhö cuoäc goïi chôø vaø chuyeån cuoäc goïi. Loại ofservice cung cấp chức năng này?
A. chuyển đổi Ethernet
B. PBX
C. NAS
D. router
17. là một quản trị viên Windows, bạn cấu hình một dịch vụ mạng Windows để chạy với một đặc biệt được tạo ra tài khoản có quyền hạn chế. Tại sao bạn sẽ làm điều này?
A. để ngăn chặn sâu máy tính vào mạng.
B. để ngăn chặn một hacker nhận được quyền được nâng cao vì một dịch vụ mạng bị xâm phạm.
C. Dịch vụ mạng của Windows sẽ không chạy với quyền quản trị.
D. Dịch vụ mạng Windows phải chạy với truy nhập bị giới hạn.
19. cuộc tấn công Stuxnet được phát hiện vào tháng 6 2010. Chức năng chính của nó là để ẩn sự hiện diện của nó trong khi reprogramming hệ thống máy tính công nghiệp (gọi là PLCs), đặc biệt ly tâm hạt nhân trong một Iran nhà máy điện hạt nhân. Các phần mềm độc hại đã được lan truyền qua ổ đĩa USB Flash, mà nó truyền bản sao của chính nó đến các máy chủ khác. Những điều sau đây áp dụng cho Stuxnet? (Chọn hai.)
A. Rootkit
B. thư rác
C. Worm
D. adware
22. những mục sau đây bị ảnh hưởng bởi Spyware? (Chọn hai.)
A. bộ nhớ
B. địa chỉ IP
C. tên máy tính
D. mạng lưới băng thông

23. Juanita sử dụng trình duyệt web Firefox trên máy trạm Linux của cô. Cô báo cáo rằng trang chủ trình duyệt của mình Giữ thay đổi để các trang web cung cấp tiền tiết kiệm trên các sản phẩm điện tử tiêu dùng. Máy quét virus của cô là chạy và là đến nay. Điều gì gây ra vấn đề này?
A. Firefox trên Linux tự động thay đổi trang chủ mỗi hai ngày.
B. Juanita đang trải qua một cuộc tấn công từ chối dịch vụ.
C. Juanita của tài khoản người dùng đã bị xâm phạm.
D. Juanita trình duyệt của cấu hình đang được thay đổi bởi phần mềm quảng cáo.
24. nào sau đây là sự thật về phần mềm Trojan?
A. nó bí mật thu thập thông tin người dùng.
B. nó tự sao chép.
C. nó có thể được tuyên truyền thông qua các mạng peer-to-peer chia sẻ tập tin.
D. nó sẽ tự động lây lan qua Windows file-và in-chia sẻ mạng.
27. loại phần mềm độc hại động làm thay đổi chính nó để tránh phát hiện?
A. Chameleon Malware
B. polymorphic phần mềm độc hại
C. changeling phần mềm độc hại
D. thiết giáp vi rút
28. những hành động sau sẽ không làm giảm khả năng lây nhiễm phần mềm độc hại? (Chọn tất cả những gì áp dụng.)
A. giữ các định nghĩa vi rút đến nay
B. quét rời phương tiện truyền thông
C. mã hóa nội dung đĩa cứng
D. sử dụng các router có khả năng NAT
29. một người dùng phàn nàn rằng hệ thống của ông đã đột nhiên trở thành không phản hồi và quảng cáo cho các sản phẩm khác nhau và Dịch vụ được popping lên trên màn hình và không thể đóng cửa. Những hành động người dùng có thể dẫn đến điều này không ai ưa hành vi? (Chọn tất cả những áp dụng.)
A. nhấp vào một kết quả tìm kiếm web
B. xem một trang web
C. xem một bộ phim trong định dạng file AVI
D. chèn một ổ USB Flash
30. một máy chủ tại địa điểm của bạn làm việc đã có tất cả các tập tin được mã hóa sau khi một kẻ tấn công xâm một thiết bị trên mạng. Cuộc tấn công nào đã diễn ra?
A. virus
B. Worm
C. crypto-Malware
Mất Keylogger
31. sau khi cài đặt một đoạn mới ofsoftware từ một trang web trực tuyến và sau đó xem xét các bản ghi hệ thống, bạn chú ý rằng các chương trình đã chạy mà không có sự đồng ý của bạn. Bạn cũng nhận ra rằng các tập tin cũng đã được Thêm vào và gỡ bỏ vào các thời điểm khi bạn không sử dụng máy tính. Những mục sau đây được nhiều khả năng được sử dụng để kết quả trong những tin nhắn đã đăng nhập? (Chọn hai.)

A. công cụ quản trị từ xa
B. adware
Quả bom C. logic
D. backdoor

CHƯƠNG 6

1. các nhà phát triển web tại công ty của bạn đang thử nghiệm mã trang web mới nhất của họ trước khi đi sống để đảm bảo rằng nó là mạnh mẽ và an toàn. Trong thời gian thử nghiệm của họ, họ cung cấp các URL bị dị tật với bất thường tham số cũng như một sự phong phú của dữ liệu ngẫu nhiên. Thuật ngữ nào mô tả hành động của họ?
A. Cross-Site Scripting
B. Fuzzing
C. Patching
D. gỡ lỗi
2. quá trình vô hiệu hoá các dịch vụ mạng không cần thiết trên một máy tính được gọi là những gì?
A. Patching
B. Fuzzing
C. cứng
D. gỡ lỗi
3. bạn đang trên một cuộc gọi hội nghị với các nhà phát triển của bạn, Serena và Thomas, thảo luận về sự an toàn của travelsite mới. Bạn bày tỏ mối quan tâm hơn một bài viết gần đây mô tả cách người dùng gửi đến các trang web có thể chứa mã độc hại chạy tại địa phương khi những người khác chỉ đơn giản là đọc bài. Serena gợi ý phê chuẩn người dùng đầu vào trước khi cho phép người dùng gửi. Những vấn đề có thể xác nhận giải quyết?
A. Cross-Site Scripting
B. Fuzzing
C. cứng
D. Patching
4. nào sau đây làm giảm sự thành công của các cuộc tấn công mật khẩu từ điển?
A. yêu cầu phức tạp mật khẩu
B. tài khoản khóa ngưỡng
C. gợi ý mật khẩu
D. thực thi lịch sử mật khẩu
5. một máy chủ bán kính được sử dụng để xác thực người dùng mạng không dây của bạn. Trong khi tạo một người dùng mới tài khoản, bạn nhận thấy có nhiều tài khoản người dùng hơn so với người dùng thực tế. Điều gì nên được thực hiện?
A. xóa tất cả các tài khoản không được liên kết với người dùng.
B. vô hiệu hoá tất cả tài khoản không được liên kết với người dùng.
C. xác minh cách các tài khoản được sử dụng và sau đó xóa các tài khoản không cần thiết.
D. xác minh cách các tài khoản được sử dụng và sau đó tắt các tài khoản không cần thiết.
6. mạng không dây 802.11 n trong bộ phận của bạn phải được lớp 2 bảo đảm. Bạn muốn kiểm soát
thiết bị không dây cụ thể nào được phép kết nối. Làm thế nào bạn có thể làm điều này?
A. thẻ SIM

B. tên máy tính NetBIOS
C. địa chỉ MAC
D. địa chỉ IP
7. định nghĩa tốt nhất của chuẩn IEEE 802.1 x là gì?
A. nó định nghĩa một nhóm các tiêu chuẩn không dây.
B. nó định nghĩa tiêu chuẩn Ethernet.
C. nó định nghĩa điều khiển truy nhập mạng chỉ cho mạng không dây.
D. nó xác định truy cập mạng controlfor Wired và mạng không dây.
8. bạn đang cứng một máy tính Linux và đã vô hiệu hoá SSH trong lợi của Telnet. Bạn đảm bảo rằng mật khẩu được yêu cầu cho truy cập Telnet. Xác định lỗi của bạn.
A. Telnet Secure nên có xác thực chính công khai kích hoạt.
B. chỉ có mật khẩu mạnh nên được sử dụng với Telnet.
C. SSH nên đã được sử dụng thay vì Telnet.
D. các cổng Telnet cần phải có được thay đổi từ 23 đến 8080.
9. là giám đốc CNTT của một trường trung học sử dụng chính sách nhóm và Active Directory, bạn có kế hoạch thích hợp tiêu chuẩn cài đặt bảo mật cho vừa được triển khai Windows 10 máy trạm. Một số giáo viên yêu cầu các cài đặt này vì phần mềm chuyên dùng mà họ sử dụng. Thuật ngữ nào dùng để chỉ Các tham số bảo mật chuẩn hóa?
A. cấu hình đường cơ sở ban đầu
B. nguyên tắc của đặc quyền ít nhất
C. Sysprepped hình ảnh
D. Localsecurity chính sách
10. Các đánh giá định kỳ ofsecurity chính sách tuân thủ được gọi là những gì?
A. khắc phục
B. cứng
C. Giám sát an ninh liên tục
D. Trend phân tích
11. bạn là một người quản trị Windows Server 2016. Bạn cài đặt và cấu hình máy chủ chính sách mạng (NPS) vai trò và cấu hình chính sách y tế yêu cầu tất cả các khách hàng kết nối để có tường lửa và phần mềm gián điệp phần mềm được kích hoạt. Khách hàng vi phạm các chính sách y tế này willnhaän một địa chỉ IP đặt chúng vào một mạng con bị giới hạn có chứa các máy chủ với tường lửa khách hàng và phần mềm gián điệp để cài đặt. Thuật ngữ gì chính xác đề cập đến vai trò của các máy chủ trên này chơi mạng con bị giới hạn?
A. cô lập
B. khắc phục
C. xác nhận
D. xác thực
12. IT bảo mật personnelphản ứng với việc lạm dụng lặp lại của các cookie phiên của một người dùng xác thực trên một trang web thương mại điện tử. Các báo cáo người dùng bị ảnh hưởng rằng ông thỉnh thoảng sử dụng các trang web nhưng không phải chocác giao dịch trong câu hỏi. Nhân viên bảo mật quyết định giảm lượng thời gian xác thực cookie là hợp lệ. Họ đã đáp lời loại tấn công nào?
A. DoS

B. từ điển
C. leo thang đặc quyền
D.Mất Cross-Site yêu cầu giả mạo
13. một người quản trị mạng nơi một thiết bị mạng trên mạng DMZ và cấu hình nó với nhiều ngưỡng bảo mật, mỗi trong số đó sẽ thông báo cho nhóm IT qua e-mail. Nhóm IT sau đó sẽ tuân thủ các chính sách phản hồi sự cố và có hành động. Điều gì sẽ được kích hoạt khi nào trong số các ngưỡng là Vi phạm?
A. báo động
B. cảnh báo
C. khắc phục
D. xác nhận đầu vào
14. một báo cáo người sử dụng lặp lại trường hợp của Windows 10 làm chậm đến điểm mà cô không còn có thể được Sản xuất. Bạn xem Nhật ký trình xem sự kiện của Windows cho tháng vừa qua và thông báo một cắt cổ lượng giao thông SMTP rời khỏi máy địa phương mỗi buổi sáng từ 10 sáng và 11:00. Loại gì phân tích được thực hiện để tìm hiểu về bất thường này?
A. Forensic
B. xu hướng
C. thống kê mạng
Mất dễ bị tổn thương
16. những gì có thể được thực hiện để cứng lại hệ điều hành Windows? (Chọn ba.)
A. vô hiệu hoá điểm khôi phục Hệ thống.
B. vô hiệu hoá các dịch vụ không cần thiết.
C. vá các hệ điều hành.
D. cấu hình EFS.
E. vô hiệu hóa chính sách nhóm.
17. bạn đang cấu hình một hạm đội của Windows máy tính xách tay cho nhân viên đi du lịch, một số người thích sử dụng USB Chuột. Điều quan trọng là các máy tính càng an toàn càng tốt. Bạn nên đặt cấu hình những gì? (Chọn ba.)
A. vô hiệu hoá cổng USB.
B. yêu cầu mã hóa thiết bị USB.
C. kích hoạt và cấu hình tường lửa của Windows.
D. cài đặt và cấu hình phần mềm chống vi-rút.
E. kích hoạt lược đồ quản lý nguồn điện.
18. một lô hàng của máy tính Windows mới đã đến cho nhân viên bộ phận kế toán. Các Máy vi tính có hệ điều hành cài đặt trước nhưng cố ý additionalfinancialsoftware. Trong đó Đặt hàng nên bạn thực hiện tất cả các sau đây?
A. tham gia miền Active Directory.
B. áp dụng tất cả các bản vá lỗi hệ điều hành.
C. đảm bảo máy quét vi rút là đến nay.
D. đăng nhập vào miền Active Directory để nhận cài đặt bảo mật chính sách nhóm.
E. cài đặt additionalfinancialsoftware.

19. những mục sau đây có thể giúp ngăn ngừa ngộ độc bộ nhớ cache ARP? (Chọn ba.)

A. sử dụng 802.1 x an ninh.

B. vô hiệu hoá ARP.

C. vá các hệ điều hành.

D. cấu hình việc sử dụng digitalchữ ký cho tất cả lưu lượng mạng.

E. vô hiệu hoá các cổng chuyển đổi không sử dụng.

20. Intranet của bạn cung cấp cho nhân viên có khả năng tìm kiếm thông qua một SQLdatabase cho du lịch quá khứ của họ chi phí khi họ đã đăng nhập. Một nhân viên từ bộ phận IT phát hiện ra rằng ifshe bước vào một SQLstring như chọn * từ chi phí mà EMPID = ' x ' = ' x ';, nó trả về tất cả nhân viên du lịch hồ sơ chi phí. Phương châm mã hóa an toàn đã bị bỏ qua?

A. phòng ngừa SQLinjection

B. xác nhận đầu vào

C. vô hiệu hóa các SQLindexes

D. xác thực người dùng

22. một mạng lưới kiểm toán an ninh cho thấy ba router không dây không an toàn sử dụng cấu hình mặc định. Mà nguyên tắc bảo mật đã bị bỏ qua?

A. ứng dụng Patch quản lý

B. thiết bị cứng

C. xác nhận đầu vào

D. nguyên tắc của đặc quyền ít nhất

23. những tiêu chuẩn sau đây phải xác thực các thiết bị tính toán trước khi cho phép truy cập mạng?

A. router

B. Hub

C. IEEE 802.1 x

Mất IEEE 802.11 n

25. mục nào tốt nhất sẽ áp dụng một đường cơ sở an ninh chuẩn cho nhiều máy tính?

A. một hình ảnh đĩa của hệ điều hành

B. Security Templates phân phối thông qua nhóm chính sách

C. cài đặt mật khẩu phân phối thông qua chính sách Nhóm

D. an ninh mẫu phân phối thông qua một chính sách localsecurity

27. trong khi cứng một máy chủ Windows, bạn quyết định vô hiệu hoá một số ofservices. Làm thế nào bạn có thể đảm bảo rằng Các dịch vụ bạn đang vô hiệu hóa sẽ không ảnh hưởng xấu đến các dịch vụ khác?

A. khởi đầu net ' tên dịch vụ '/DEP lệnh.

B. vô hiệu hoá các dịch vụ, để cho hệ thống chạy trong một vài ngày, và sau đó kiểm tra các bản ghi người xem sự kiện.

C. nhấp chuột phải vào dịch vụ và chọn Hiển thị chuỗi phụ thuộc.

D. nhấp đúp vào dịch vụ và xem tab phụ thuộc.

28. công ty của bạn sử dụng Microsoft IIS để lưu trữ nhiều trang web intranet trên một cụm hai nút. Allsites lưu trữ cấu hình và nội dung của họ trên ổ C: và các tập tin đăng nhập được lưu trữ trên ổ D:. Allsites chia sẻ một Hồ bơi ứng

dụng phổ biến. Giám đốc CNTT đã yêu cầu bạn đảm bảo rằng một trang web đơn bị tấn công sẽ không ảnh hưởng xấu đến các trang web khác đang chạy. Bạn nên làm gì?
A. di chuyển mỗi trang web cấu hình cho một đĩa cứng riêng biệt.
B. di chuyển nội dung của mỗi trang web sang một đĩa cứng riêng biệt.
C. cấu hình mỗi trang web để sử dụng hồ bơi ứng dụng riêng của mình.
D. thêm nút thứ ba vào cụm hai nút.
29. bạn đang phát triển Windows của bạn 8,1 doanh nghiệp buổi giới thiệu chiến lược. Chính sách bảo mật IT đã được Cập Nhật để phản ánh các tiêu chuẩn bảo mật nghiêm ngặt của công ty. Mà những điều sau đây sẽ cứng lại Windows 8,1?
(Chọn hai.)
A. sử dụng một địa chỉ IP lớp C.
B. Đặt cấu hình lưu trữ đăng nhập.
C. cấu hình các hạn chế thiết bị USB.
D. vô hiệu hoá các dịch vụ không sử dụng.
30. làm thế nào bạn có thể ngăn chặn Rogue máy kết nối vào mạng của bạn?
A. triển khai cấu hình IEEE 802.1 x.
B. sử dụng mật khẩu mạnh cho tài khoản người dùng.
C. sử dụng IPv6.
D. triển khai cấu hình IEEE 802,11.
31. những gì có thể được thực hiện để bảo đảm lưu lượng truy cập mạng được tạo ra khi quản lý không dây của bạn Router?
A. sử dụng HTTPS với IPv6.
B. sử dụng HTTP với PKI.
C. sử dụng HTTP với IPv6.
D. sử dụng HTTPS với PKI.
32. công ty của bạn đang nâng cấp lên bộ Office mới. Các ứng dụng bảng tính phải tin tưởng macro chỉ ký điện tử của cơ quan chứng chỉ công ty. Bạn có máy chủ được cài đặt trong một cửa sổ riêng Miền Active Directory. Những gì bạn nên cấu hình để đảm bảo an ninh vĩ mô trên allstations là cấu hình đúng?
A. cấu hình ứng dụng bảng tính trên mỗi máy tính để tin tưởng macro công ty.
B. tạo một giấy chứng nhận EFS PKI để ký kết các macro.
C. sử dụng chính sách nhóm để thi hành cơ sở cấu hình ứng dụng được mô tả.
D. sử dụng chính sách nhóm để phân phối các macro để allstations.
33. Aidan là tạo ra một hình ảnh hệ điều hành Linux sẽ được sử dụng để triển khai Linux máy ảo từ một bản mẫu. Sau khi vá hệ điều hành, ông cài đặt phần mềm ứng dụng yêu cầu, cài đặt và Cập nhật phần mềm chống phần mềm độc hại, tạo hình ảnh và lưu trữ nó trên máy chủ ảnh. Điều gì đã làm Aidan quên làm gì?
A. ông đã quên SysPrep cài đặt trước khi chụp ảnh.
B. ông quên vá các phần mềm ứng dụng.
C. ông quên bật chống phần mềm độc hại thời gian thực giám sát.
D. ông quên mật mã hóa ổ đĩa cứng.

34. bạn là người sáng lập của Acme dữ liệu khai thác. Các doanh nghiệp tập trung vào Lấy thói quen có liên quan tiêu dùng từ nhiều nguồn khác nhau, và dữ liệu đó được bán cho các nhà bán lẻ. Vì lượng dữ liệu phải được xử lý, bạn phải thực hiện các giải pháp nhanh nhất có thể. Những loại công nghệ nên bạn
Thực hiện?
A. SQL
B. NoSQL
C. SATA
D. NoSATA
35. bạn đã được yêu cầu phát triển một ứng dụng web an toàn cho một nhà bán lẻ bia gia đình. App willread và viết thư cho một cơ sở dữ liệu Back-end cho các giao dịch khách hàng. Cơ sở dữ liệu có quy tắc tại chỗ để kiểm tra dữ liệu đó là hợp lệ. Trang web sử dụng HTTPS. Điều gì khác nên được thực hiện để bảo đảm các ứng dụng web hơn nữa?
A. sử dụng JavaScript cho Server-Side dữ liệu xác nhận.
B. sử dụng PKI.
C. sử dụng VPN.
D. sử dụng JavaScript cho client-side dữ liệu xác nhận.
36. công ty của bạn đã phát hành điện thoại thông minh dựa trên Android để chọn nhân viên. Người quản lý của bạn yêu cầu bạnđảm bảo rằng dữ liệu trên điện thoại thông minh được bảo vệ. Làm thế nào để bạn giải quyết mối quan tâm của người quản lý?
A. thực hiện SCADA, màn hình khóa, mã hóa thiết bị, và chống phần mềm độc hại, và vô hiệu hóa không cần thiết phần mềm trên điện thoại.
B. thực hiện PKI VPN chứng chỉ xác thực, màn hình khóa, mã hóa thiết bị, và antimalware, và vô hiệu hóa phần mềm không cần thiết trên điện thoại.
C. thực hiện khóa màn hình, mã hóa thiết bị, vá, và chống phần mềm độc hại, và vô hiệu hóa không cần thiết phần mềm trên điện thoại.
D. thực hiện HTTPS, màn hình khóa, mã hóa thiết bị, và chống phần mềm độc hại, và vô hiệu không cần thiết phần mềm trên điện thoại.
37. trong khi cứng Trang chủ của bạn mạng văn phòng, bạn quyết định kiểm tra xem phần vững trong tất cả các mạng thiết bị được Cập Nhật. Mà các thiết bị sau đây sẽ áp dụng điều này?
A. thông minh truyền hình, chơi Game Console, máy in, HVAC, Wireless Router
B. tủ lạnh, máy in, Wireless Router, điện cửa hàng, máy in
C. HVAC, bình chữa cháy, chơi Game Console, máy in, router không dây
D. giao diện điều khiển chơi Game, điện thoại Android, Apple iOS thiết bị, máy in, bình chữa cháy
38. trong đó doanh nghiệp hạng mục trong tổ chức của bạn nên được vá thường xuyên? (Chọn tất cả những gì áp dụng.)
A. Mainframes
B. Thin khách hàng
C. công cộng đám mây ảo hóa hosts
D. địa chỉ IP

40. một dịch vụ trên một localserver không thể giao tiếp với máy chủ cơ sở dữ liệu của nó đang chạy trên máy khác. Các cơ sở dữ liệu máy chủ đang hoạt động chính xác và tất cả các kết nối mạng đang làm việc đúng cách. Những gì là Vấn đề?
A. Insider đe dọa
B. phần mềm trái phép
C. UTM
D. tường lửa bị cấu hình sai
41. kẻ tấn công đã liên lạc với một trong những nhân viên của bạn và đã thuyết phục cô bỏ tên người dùng và mật khẩu, cho kẻ tấn công truy cập vào mạng của bạn. Loại tấn công này là gì?
A. dữ liệu lọc
B. kỹ thuật xã hội
C. HIDS/HIPS
D. các vấn đề cấp phép
42. dữ liệu quan trọng về mạng nội bộ của công ty bạn đã bị rò rỉ trực tuyến. Hiện đã không có
vi phạm mạng của bạn bởi kẻ tấn công. Loại vấn đề là điều này?
A. tập tin Integrity kiểm tra
B. tường lửa dựa trên host
C. truyền thông xã hội
D. DLP thất bại cho một người sử dụng độc hại
43. trong khi giám sát giao thông mạng, bạn nhận thấy rất nhiều liên lạc IMAP giữa mạng của bạn và
một địa chỉ IP không thuộc về công ty e-Mailserver. Nguyên nhân của giao thông này là gì?
A. nâng cao phần mềm độc hại Tools
B. các ứng dụng whitelisted
C. DEP
D. e-mail cá nhân
44. máy tính xách tay mới của công ty đã đến, và trước khi được triển khai trong lĩnh vực này, phần mềm được cài đặt trên chúng để cho phép họ được theo dõi Trung ương và quản lý. Cụm từ nào mô tả tốt nhất kịch bản này?
A. tập tin toàn vẹn Checks
B. ứng dụng web Firewall
C. quản lý tài sản
D. một sự vi phạm cấp phép tuân thủ
45. các "NIST Cybersecurity Framework là một ví dụ về loại hình ngành công nghiệp-tiêu chuẩn khuôn khổ? (Chọn hai.)
A. quy định
B. National
C. không quy định
D. quốc tế
46. tại sao bạn có thể muốn giữ sự đa dạng của các công nghệ người dùng cuối để sử dụng tối thiểu? (Chọn tất cả những gì áp dụng.)
A. phải mất ít nỗ lực để duy trì.

B. nó làm giảm chi phí.
C. phải mất nhiều nỗ lực để duy trì.
D. nó cải thiện kinh nghiệm người dùng.
47. nào sau đây không phải là một ví dụ về một thiết bị thông minh (hoặc IoT)?
A. một xem
B. một lightbulb
C. một UAV/Drone
D. Internet Camera
E. Hệ thống trên một chip
48. bạn đang tiếp cận bởi một công ty mà muốn nhóm của bạn để phát triển một ứng dụng cho họ. Họ sẽ muốn được đánh giá cao tham gia và muốn một phiên bản cơ bản của phần mềm làm việc càng sớm càng tốt. Mô hình phát triển gì là phù hợp nhất cho điều này?
A. Agile
B. Waterfall
C. SCADA
D. SDK
49. những gì có thể được sử dụng để xác nhận Sqlcáo repetitively?
A. tiếp xúc dữ liệu
B. bình thường hoá
C. thủ tục lưu trữ
D. Obfuscation/ngụy trang
50. bảo mật DevOps entail gì? (Chọn tất cả những áp dụng.)
A. tự động hóa bảo mật
B. liên tục hội nhậpCác hệ thống
C. Immutable
D. cơ sở hạ tầng như mã
51. bạn đang tham gia một nhóm các nhà phát triển những người sử dụng git cho sản phẩm của họ. Lợi ích chính là gì git Cung cấp?
A. SDK
B. Phiên bản kiểm soát
C. quản lý bộ nhớ
D. Dead mã
52. nhóm phát triển bạn đang làm việc với muốn phân tích một số mã mà không thực hiện nó. Làm thế nào có thể Điều này đạt được?
A. phân tích mã tĩnh.
B. động phân tích.
C. sandboxing.
D. sử dụng nó như thời gian chạy mã thay vì biên dịch mã.
53. bạn được yêu cầu kiểm tra khả năng của một chương trình hoạt động đúng theo điều kiện tải nặng. Cái gì loại bài kiểm tra bạn nên chạy?

A. mô hình xác minh
B. Baselining
C. mã hóa
D. Stress thử nghiệm

CHƯƠNG 7

2. tài khoản người dùng của Trinity là nhầm lẫn xóa khi cô đi trên ba tháng thai sản để lại. Khi cô ấy trả về, một tài khoản mới với quyền NTFS thích hợp được tạo ra cho cô ấy. Khi cô cố gắng mở tập tin cũ của cô, cô vẫn nhận được "truy cập bị từ chối" tin nhắn. Vấn đề là gì?
A. Trinity không có quyền NTFS thích hợp.
B. Trinity của tài khoản người dùng mới có một SID khác hơn so với một cũ của cô.
C. Trinity của tập tin được mã hóa với tài khoản cũ của cô.
D. Trinity của tài khoản nên được thực hiện một thành viên của nhóm người sử dụng điện.
4. bạn là một hệ phục vụ tư vấn ảo hóa cho không thực sự có, Inc Trong một cuộc họp lập kế hoạch với một khách hàng, vấn đề của máy ảo Point-in-Time chụp nhanh đi lên. Bạn khuyên bạn nên cẩn thận sử dụng ảnh chụp nhanh vì các chi nhánh an ninh. Mối quan tâm của bạn là gì?
A. snapshots có thể tiêu thụ một lượng lớn không gian đĩa.
B. việc sử dụng ofsnapshots có thể kích hoạt một lũ MAC.
C. Invoked ảnh chụp nhanh sẽ có nghĩa là các máy ảo tạm thời không có sẵn.
D. gọi ảnh chụp nhanh sẽ có Cập Nhật bản vá ít hơn các máy ảo hiện đang chạy.
5. những gì có thể được thực hiện để cứng lại một thiết bị di động, cầm tay? (Chọn hai.)
A. vô hiệu hoá Wi-Fi.
B. đảm bảo rằng nó chỉ được sử dụng trong các lĩnh vực bảo đảm thể chất.
C. đặt Bluetooth phát hiện ra vô hiệu hoá.
D. cho phép khóa màn hình.
6. một thực hành y tế tư nhân thuê bạn để xác định tính khả thi của điện toán đám mây, theo đó lưu trữ e-mail và các ứng dụng y tế, cũng như thông tin bệnh nhân, sẽ được tổ chức bởi một nhà cung cấp Internet. Bạn được yêu cầu xác định các vấn đề bảo mật có thể. (Chọn hai.)
A. dữ liệu không được lưu trữ tại địa phương nhưng thay vào đó được lưu trữ trên cơ sở của nhà cung cấp, nơi mà các doanh nghiệp khác cũng có thể truy cập vào các dịch vụ điện toán đám mây.
B. HTTPS sẽ được sử dụng để truy cập các dịch vụ từ xa.
C. nhà cung cấp có nên được phục vụ một trát hầu tòa, khả năng tiết lộ dữ liệu đầy đủ tồn tại.
D. dữ liệu sẽ được mã hóa trong quá cảnh cũng như khi lưu trữ.
7. tùy chọn nào sẽ bảo vệ máy tính xách tay nhân viên khi họ đi du lịch và kết nối với mạng không dây?
A. Personalfirewallsoftware
B. MAC địa chỉ lọc
C. ảo hóa
D. 802.11 n tương thích thẻ không dây
8. những gì có thể được thực hiện để đảm bảo tính bí mật dữ liệu ofsensitive sao chép vào ổ đĩa USB Flash?
A. tập tin băm

B. mã hóa
C. NTFS cấp phép
D. quyền chia sẻ
9. tiêu chuẩn nào là một giải pháp phần vững cho mã hóa ổ đĩa?
A. TPM
B. DLP
C. EFS
D. NTFS
13. loại ofsoftware hoạt động chống lại việc thu thập thông tin cá nhân?
A. chống thư rác
B. Antivirus
C. Antispyware
D. Anti-Adware
14. nào sau đây tốt nhất bảo vệ chống lại các Khuyết tật hệ điều hành?
A. phần mềm chống virus
B. Firewallsoftware
C. mã hóa
D. Patching
16. một người quản trị máy chủ phải tuân thủ pháp luật rằng các tiểu bang mà dữ liệu tài chính phải được giữ an toàn trong sự kiện của một vi phạm physicalsecurity. Thực tiễn nào sẽ đảm bảo rằng người quản trị tuân thủ Luật? (Chọn hai.)
A. áp dụng các quyền NTFS
B. lưu trữ băng sao lưu an toàn
C. mã hóa máy chủ đĩa cứng
D. lưu trữ các băng sao lưu trong tủ bị khóa
17. loại ofsoftware kiểm tra hành vi ứng dụng, bản ghi, và các sự kiện cho hoạt động đáng ngờ?
A. TỔ
B. tường lửa dựa trên host
C. HIDS
D. Spyware
18. một người quản trị cơ sở dữ liệu yêu cầu một phương pháp mà hoạt động độc hại đối với một Microsoft SQLServer máy chủ cơ sở dữ liệu có thể được phát hiện. Tất cả lưu lượng mạng đến máy chủ cơ sở dữ liệu được mã hóa. Giải pháp gì Nếu bạn đề nghị?
A. HIDS
B. TỔ
C. IPSec
D. SSL
19. những điều sau đây là đúng liên quan đến ảo hóa? (Chọn hai.)
A. mỗi máy ảo có một hoặc nhiều địa chỉ MAC duy nhất.
B. hệ điều hành máy ảo không cần phải được vá.

C. máy ảo chạy trên cùng một máy chủ vật lý có thể thuộc về VLAN khác nhau.
D. một thỏa hiệp an ninh của một máy ảo có nghĩa là tất cả các máy ảo trên máy chủ vật lý được Thỏa hiệp.
20. Cloud máy tính cung cấp những lợi ích? (Chọn hai.)
A. đơn giản, khả năng mở rộng
B. ít hơn phần cứng mua hàng
C. tốt hơn mã hóa
D. địa phương lưu trữ dữ liệu
E. không yêu cầu cho phần mềm chống virus
21. Mitch chịu trách nhiệm cho ba payrollservers lưu trữ dữ liệu trên SAN. Giám đốc tài chính (CFO)
yêu cầu quan sát quyền truy cập vào một nhóm các tập tin ngân sách của một người dùng cụ thể. Mitch nên làm gì?
A. tạo tập tin hashes cho mỗi tập tin ngân sách.
B. mã hóa các tập tin ngân sách.
C. cấu hình một HIDS để giám sát các tập tin ngân sách.
D. cấu hình hệ thống tập tin kiểm toán.
22. công ty của bạn đã mua phần mềm bảo mật mà sẽ giám sát việc sử dụng ứng dụng trên tất cả các máy trạm.Trước khi phần mềm có thể hoạt động đúng, bạn phải có người dùng chạy các ứng dụng của họ khi họ bình thường sẽ trong một thời gian ngắn. Tại sao phần mềm bảo mật yêu cầu này phải được thực hiện?
A. để cập nhật các định nghĩa chống vi-rút cho các tập tin ứng dụng
B. để thiết lập một đường cơ sở sử dụng bình thường
C. để xác minh rằng phần mềm bảo mật có các quyền cần thiết để chạy
D. để xác minh rằng phần mềm được cấp phép đang được sử dụng
23. Kevin là một luật sư thử nghiệm ở miền Nam California. Ông yêu cầu an toàn, âm thanh chất lượng cao, giao tiếp với
khách hàng. Anh ta có thể làm gì?
A. sử dụng VoIP với mã hóa gói qua Internet.
B. sử dụng mã hóa giọng nói điện thoại di động.
C. chỉ sử dụng điện thoại cố định.
D. sử dụng điện thoại di động của mình trên một mạng thoại đặc biệt cho các chuyên gia pháp lý.
24. quản lý CNTT của bạn yêu cầu bạn đảm bảo rằng các thư e-mail và file đính kèm không chứa dữ liệu nhạy cảm có thể bị rò rỉ đối thủ cạnh tranh. Bạn nên đề xuất loại ofsolution nào?
A. phần mềm chống virus
B. TỔ
C. DLP
D. HIDS
25. hiệu suất máy chủ của bạn đã giảm kể từ khi giới thiệu ký điện tử và mã hóa tất cả
mạng lưới giao thông. Bạn muốn phát hành các máy chủ từ chức năng này. Bạn nên sử dụng thiết bị nào?
A. SmartCard
B. TPM
C. HSM
D. EFS

26. công ty của bạn đã quyết định rằng tất cả các phần cứng máy chủ mới sẽ có hỗ trợ TPM. Bạn nhận được một mới máy chủ, và bạn cho phép TPM thông qua các tiện ích CMOS và cho phép mã hóa ổ đĩa bằng cách sử dụng TPM trong Hệ điều hành. Bạn nên làm gì tiếp theo?
A. khởi động lại máy chủ.
B. kích hoạt EFS trên máy chủ.
C. kích hoạt IPSec.
D. sao lưu các phím TPM.
27. bạn cố gắng mã hóa một thư mục trên ổ D: sử dụng EFS, nhưng tùy chọn mã hóa không có sẵn. Cái gì bạn nên làm gì?
A. vấn đề chuyển đổi d:/FS: NTFS lệnh.
B. Thêm tài khoản của bạn vào nhóm người quản trị.
C. kích hoạt EFS thông qua nhóm chính sách.
D. kích hoạt TPM trong Tiện ích CMOS.
28. có khả năng hiện diện trong một thiết bị bảo mật tất cả-trong-một? (Chọn ba.)
A. URLfilter
B. kiểm tra nội dung
C. phần mềm độc hại kiểm tra
D. EFS
29. là người quản trị cơ sở dữ liệu cho công ty của bạn, bạn đang đánh giá các dịch vụ đám mây công cộng khác nhau để thử nghiệm
thay đổi lập trình cơ sở dữ liệu khách hàng. Trong đó thể loại của dịch vụ đám mây bạn nên nghiên cứu?
A. phần mềm như một dịch vụ
B. nền tảng như một dịch vụ
C. cơ sở hạ tầng như một dịch vụ
D. bảo mật như một dịch vụ
31. bạn đang triển khai Android dựa trên điện thoại thông minh cho nhân viên trong văn phòng Toronto của bạn. Vì những tính chất nhạy cảm của doanh nghiệp của bạn, bạn muốn sử dụng các cơ chế sẽ bảo vệ dữ liệu nhạy cảm mà có thể tồn tại trên điện thoại. Mà tập hợp các cơ chế bạn nên sử dụng?
A. mã hóa đầy đủ thiết bị, chạy máy ảo, tách các nhiệm vụ
B. từ xa lau, lockout, FTP App
C. màn hình khóa, GPS, dung lượng lớn hơn mini SD Card
D. hạn chế mà các ứng dụng có thể được cài đặt, phân đoạn hệ điều hành lưu trữ vị trí từ App lưu trữ vị trí,tắt tính năng không sử dụng, vô hiệu hoá mật khẩu mặc định
33. quản lý đã quyết định hỗ trợ một chính sách công ty BYOD. Bạn đã được yêu cầu đề nghị
điểm xem xét trước khi BYOD được đưa vào hiệu lực. Những điểm sau đây nên được
xem xét về BYOD? (Chọn ba.)
A. thêm dung lượng lưu trữ cho các máy chủ
B. Legalramifications
C. hạ tầng mạng thay đổi
D. vô hiệu hoá on-board camera/video và microphone bên ngoài các cuộc gọi

34. nào sau một cách chính xác xác định một hệ điều hành đáp ứng chính phủ cụ thể hoặc
tiêu chuẩn bảo mật quy định?
A. cứng OS
B. Trusted OS
C. hệ điều hành an ninh
D. Patched hệ điều hành
35. sử dụng hình 7-1 để phù hợp với tất cả các cá nhân bên trái dưới nhóm chính xác bên phải.
FIGURE7-1
Baselining và ảo hóa tập thể dục
36. một chính sách dữ liệu toàn diện bao gồm những điều sau đây?
A. lau, tháo, Giữ, lưu trữ
B. Disposing, Patching, lưu trữ lưu giữ
C. duy trì, lưu trữ, ảo hóa
D. lưu trữ, ảo hóa, tính đàn hồi
37. nào sau đây là một cách hợp lệ của việc xử lý dữ liệu lớn?
A. dữ liệu ở phần còn lại
B. NoSQL
C. EFS
D. lưu trữ đám mây
38. những tiêu chuẩn liên lạc cho phép các thiết bị để giao tiếp với một khoảng cách rất ngắn?
A. NFC
B. Cellular
C. SATCOM
D. ANT
39. bạn muốn một cảnh báo để được gửi qua email trực tiếp cho bạn khi một công ty thiết bị di động lá một khu vực xung quanh tòa nhà công ty. Công nghệ nào sẽ cho phép điều này?
A. hồng ngoại
B. Push thông báo dịch vụ
C. Geofxác
D. SMS/MMS
41. tiêu chuẩn cho phép một máy tính để khởi động chỉ với phần mềm trong danh sách trắng đáng tin cậy?
A. xác thực ngữ cảnh-Aware
B. phần cứng gốc của Trust
C. COPE
D. khởi động an toàn
42. một số điều cần giám sát cho trên thiết bị di động để ngăn chặn vấn đề an ninh là gì? (Chọn tất cả những gì áp dụng.)
A. CYOD
B. rooting
C. sinh trắc học

D. Sideloading

E. cửa hàng ứng dụng của bên thứ ba

43. bạn muốn kết nối Internet qua điện thoại vì máy tính bạn đang sử dụng không có khả năng WiFi. Cái này gọi là gì?

A. Tethering

B. Wi-Fi Direct/Ad hoc

C. mở khóa tàu sân bay

D. VDI

44. bạn nhận thấy rằng khi thiết bị di động được đưa đến các quán cà phê của công ty, kết nối Wi-Fi thường xuyên cắt ra. Điều này xảy ra không nơi nào khác trong tòa nhà. Nguyên nhân có thể nhất của điều này là gì?

A. MFDs

B. EMI

C. VDE

D. BIOS

48. người quản lý của bạn muốn chạy tất cả các ứng dụng một cách an toàn trên một hệ thống trong virtualserver riêng của mình. Đây là cái gì kỹ thuật được gọi là?

A. tính toàn vẹn đo lường

B. Cloud truy cập môi giới an ninh

C. VM thoát khỏi bảo vệ

D. container ứng dụng

49. phương pháp cho phép chạy một phiên bản chỉ đọc của một hệ điều hành mà reverts đến của nó originalstate trên mỗi khởi động?

A. cấu hình xác nhận

B. rollback cấu hình đã biết

C. Live khởi động phương tiện truyền thông

D. trở lại nhà nước được biết đến

50. những nhiệm vụ sau đây là ứng cử viên tự động hóa tốt? (Chọn tất cả những áp dụng.)

A. Giám sát liên tục

B. xác nhận cấu hình

C. VM sprawl tránh

D. purging

51. phương pháp hủy diệt dữ liệu và Media sanitization là gì? (Chọn tất cả những áp dụng.)

A. đốt cháy

B. độ đàn hồi

C. Shredding

D.Mất Degaussing

E. Pulping

CHAPTER 8

1. Bạn là khách tại một khách sạn cung cấp truy cập Wi-FiI Internet miễn phí cho khách. Bạn kết nối với mạng không dây ở mức đầy đủ và có được cấu hình TCP / IP hợp lệ. Khi bạn cố gắng truy cập các trang web Internet, một trang web sẽ hiển thị thay vì yêu cầu mã trước khi cho phép truy cập Internet. Loại thành phần mạng nào có liên quan đến việc cung cấp chức năng này?

C. Proxy server

2. Bạn đang định cấu hình bộ định tuyến không dây tại cửa hàng sửa chữa ô tô để khách hàng chờ đợi có thể kết nối Internet. Bạn muốn đảm bảo rằng các máy khách không dây có thể kết nối Internet nhưng không thể kết nối với các máy tính nội bộ thuộc sở hữu của cửa hàng sửa chữa ô tô. Bạn nên cắm bộ định tuyến không dây ở đâu?

D. DMZ

3. Điều gì sẽ phát hiện một mạng hoặc máy chủ xâm nhập và có hành động để ngăn chặn sự xâm nhập thành công?

A. IPS

4. Công nghệ nào sử dụng một địa chỉ IP bên ngoài duy nhất để đại diện cho nhiều máy tính trên mạng nội bộ?

C. NAT

5. Bạn phải mua một thiết bị mạng hỗ trợ lọc nội dung và phòng chống vi-rút cho mạng LAN của bạn. Bạn nên chọn cái gì?

C. Web security gateway

6. Bạn đã được yêu cầu bằng cách nào đó tách riêng lưu lượng truy cập mạng của bộ phận Kỹ thuật khỏi lưu lượng của bộ phận Kế toán vì thông lượng mạng giảm. Bạn nên dùng gì?

A. VLAN

7. Dựa trên bộ quy tắc tường lửa LAN sau đây, chọn mô tả đúng nhất:

C. LAN users can connect to external web servers. External users can use RDP to connect to LAN computers.

8. Công cụ nào sẽ cho phép bạn chụp và xem lưu lượng mạng?

C. Protocol analyzer

9. Bạn đang xem xét cấu hình bộ định tuyến để đảm bảo chúng tuân thủ các chính sách bảo mật của công ty. Bạn nhận thấy các bộ định tuyến được cấu hình để tải cấu hình của chúng bằng TFTP và cổng TCP 22 cũng được bật. Vấn đề bảo mật nào tồn tại với các bộ định tuyến này?

C. TFTP is an insecure protocol.

10. Một bộ định tuyến phải được cấu hình để chỉ cho phép lưu lượng truy cập từ một số máy chủ nhất định. Làm thế nào điều này có thể được thực hiện?

A. ACL

11. Những công nghệ cho phép phân tích lưu lượng mạng? (Chọn hai.)

B. Sniffer

D. NIDS

12. Thuật ngữ nào mô tả mạng giữa hai tường lửa, được hiển thị ở đây?

C. DMZ

13. Bạn đã nhận được một bộ tập trung VPN mới để cho phép người dùng đi du lịch truy cập vào LAN B. Bạn nên đặt bộ tập trung VPN ở đâu?

B. LAN B

14. Máy trạm của Sylvia xông đã được chuyển sang một tủ mới. Vào sáng thứ Hai, Sylvia báo cáo rằng mặc dù card mạng đã được cắm vào giắc cắm mạng, nhưng không có đèn liên kết trên card mạng. Vấn đề là gì?
D. Since the MAC address has changed, switch port security has disabled the port
15. Bạn cần một phương pháp xác thực máy trạm Windows trước khi cho phép truy cập mạng LAN cục bộ. Bạn nên dùng gì?
C. 802.1x-compliant switch
16. Kẻ tấn công gửi hàng ngàn gói TCP SYN có địa chỉ IP nguồn không thể truy cập đến máy chủ. Sau khi tiêu thụ tài nguyên máy chủ với lưu lượng này, lưu lượng hợp pháp không thể truy cập máy chủ được nữa. Điều gì có thể ngăn chặn kiểu tấn công này?
D. SYN flood protection
17. Một nhân viên IT cơ sở liên kết ba công tắc mạng với nhau sao cho mỗi công tắc kết nối với hai công tắc khác. Hậu quả là mạng tràn ngập lưu lượng vô dụng. Điều gì có thể ngăn chặn tình trạng này?
B. Loop protection
18. Sếp của bạn yêu cầu lưu lượng HTTP cụ thể được theo dõi và chặn. Bạn nên dùng gì?
A. Web application firewall
19. Một hiệu trưởng trường trung học khăng khăng ngăn chặn học sinh truy cập vào các trang web phần mềm độc hại đã biết. Điều này có thể giải quyết như thế nào?
B. URLfiltering
20. Kịch bản nào sau đây mô tả đúng nhất về sự từ chối ngầm?
C. Block network traffic unless specifically permitted.
21. Một sinh viên đại học có kết nối mạng có dây với mạng đại học hạn chế. Đồng thời, sinh viên được kết nối với điểm truy cập Wi-Fi cho một quán cà phê gần đó cho phép truy cập Internet không hạn chế. Vấn đề tiềm năng nào tồn tại trong trường hợp này?
A. The student computer could link coffee shop patrons to the university network
22. Thiết bị mạng nào mã hóa và giải mã lưu lượng mạng qua mạng không an toàn để cho phép truy cập vào mạng LAN riêng?
C. VPN concentrator
23. Bạn nghi ngờ hoạt động độc hại trên DMZ của bạn. Trong nỗ lực xác định người vi phạm, bạn đã cố tình cấu hình một máy chủ chưa được vá để thu hút sự chú ý hơn nữa. Thuật ngữ nào mô tả những gì bạn đã cấu hình?
D. Honeypot
24. NIDS của bạn báo cáo không chính xác lưu lượng truy cập mạng hợp pháp là đáng ngờ. Cái này được gọi là gì?
A. False positive
25. Chính sách truy cập mạng công ty của bạn nói rằng tất cả các thiết bị kết nối đều yêu cầu tường lửa dựa trên máy chủ, trình quét chống vi-rút và các bản cập nhật hệ điều hành mới nhất. Bạn muốn ngăn các thiết bị không tuân thủ kết nối với mạng của bạn. Giải pháp nào bạn nên xem xét?
B. NAC
26. Điều nào sau đây là đúng về NAT? (Chọn hai.)
A. The NAT client is unaware of address translation.
C. Internet hosts are unaware of address translation.

27. Bạn là một giám đốc bán hàng cho một công ty bất động sản. Một trong những khách hàng của bạn gọi cho bạn tự hỏi tại sao bạn chưa gửi email tài liệu quan trọng của cô ấy về việc bán hàng. Bạn kiểm tra chương trình thư của bạn để xác minh thư đã được gửi hai ngày trước. Bạn cũng xác minh tin nhắn không được gửi lại cho bạn là không thể gửi được. Bạn nói với khách hàng của bạn rằng trên thực tế bạn đã gửi tin nhắn. Điều gì tiếp theo bạn nên nói với khách hàng của bạn?

D. Check your junk mail; anti-spam software sometimes incorrectly identifies legitimate mail as spam.

28. Bạn là một nhà tư vấn mạng CNTT. Bạn cài đặt một mạng không dây mới cho một khách sạn. Bạn phải làm gì để ngăn người dùng mạng không dây truy cập quản trị vào bộ định tuyến không dây?

C. Change the admin password.

29. Bạn là một chuyên gia CNTT với một cơ quan thực thi pháp luật. Bạn đã theo dõi hoạt động Internet bất hợp pháp xuống địa chỉ IP. Các thám tử muốn liên kết một người với địa chỉ IP để đảm bảo lệnh bắt giữ. Điều nào sau đây là đúng về tình huống này? (Chọn hai.)

A. The IP address might be that of a NAT router or a proxy server

C. IP addresses can be traced to a regionalISP.

30. Giám đốc bảo mật CNTT của bạn yêu cầu bạn định cấu hình mã hóa gói cho mạng nội bộ của bạn. Cô bày tỏ mối quan tâm về cách các tường lửa lọc gói hiện tại có thể ảnh hưởng đến lưu lượng được mã hóa này. Làm thế nào bạn sẽ trả lời những mối quan tâm của cô ấy?

B. Encrypted packet headers could prevent outbound traffic from leaving the internal network

31. Vẽ một đường trong Hình 8-1 liên kết kết quả mong muốn được liệt kê ở bên trái với giải pháp đúng được liệt kê ở bên phải. See “In-Depth Answers.”

32. Bạn đang định cấu hình quy tắc tường lửa gửi đến trên máy chủ Linux. Bạn sẽ sử dụng công cụ dòng lệnh nào? iptables

33. Bạn đang định cấu hình quy tắc tường lửa gửi đến trên máy chủ Windows. Bạn sẽ sử dụng công cụ dòng lệnh nào? netsh

34. Acme Inc. đã thuê bạn thực hiện các giải pháp bảo mật theo khuyến nghị của kết quả kiểm toán an ninh mạng. Các trạm kết nối với mạng phải được bật tường lửa dựa trên máy chủ và phải cài đặt giải pháp chống vi-rút cập nhật. Bạn nên thực hiện những gì?

B. NAC

35. Acme Inc. đã thuê bạn thực hiện các giải pháp bảo mật theo khuyến nghị của kết quả kiểm toán an ninh mạng. Các trạm được sử dụng bởi nhân viên Kế toán sẽ không thể giao tiếp với các trạm khác trên mạng. Bạn nên thực hiện những gì?

D. VLAN

36. Acme Inc. đã thuê bạn thực hiện các giải pháp bảo mật theo khuyến nghị của kết quả kiểm toán an ninh mạng. Hiện tại, bất kỳ trạm nào được cắm vào một bộ chuyển mạch đều có thể giao tiếp trên mạng mà không cần bất kỳ

37. loại xác thực nào. Acme Inc. muốn hạn chế liên lạc qua mạng bằng cách kết nối các trạm cho đến khi chúng được xác thực. Bạn nên thực hiện những gì?

C. 802.1x

38. Acme Inc. đã thuê bạn thực hiện các giải pháp bảo mật theo khuyến nghị của kết quả kiểm toán an ninh mạng. Hiện tại, tất cả người dùng có quyền truy cập Đọc vào tệp dự án trên máy chủ tệp chính. Cấu hình của bạn phải đảm

bảo rằng chỉ các thành viên của nhóm Người quản lý dự án có quyền truy cập vào tệp dự án. Bạn nên thực hiện những gì?
A. ACLv
39. Thiết bị kết nối mạng nào sau đây? (Chọn hai.)
B. Bridge
D. Aggregation switch
40. Bạn đã nhận thấy rằng một máy chủ đã chậm đi đáng kể vì mã hóa được kích hoạt cho lưu lượng ra bên ngoài của nó. Điều gì sau đây là giải pháp tốt nhất để tăng tốc máy chủ?
C. SSL/TLS accelerator
41. Sếp của bạn tiếp cận bạn về việc gắn hệ thống PBX vào mạng Ethernet. Thiết bị nào sẽ cho phép điều này?
B. Media gateway
42. Làm thế nào các mạng khác nhau có thể được phân đoạn với nhau? (Chọn ba.)
A, Media gateway
C, Physically
D. Air gap
43. Loại thiết bị nào được sử dụng để giám sát môi trường vật lý mà mạng được đặt?
A. Sensors

CHAPTER 9

1. Trong khi xem xét nhật ký bộ định tuyến không dây, bạn nhận thấy việc sử dụng mạng không dây bởi các hệ thống lạ. Làm thế nào bạn có thể kiểm soát hệ thống nào kết nối với mạng không dây của bạn?
D. Enable MAC address filtering.
2. Kích hoạt WPA trên mạng WLAN cung cấp những gì? (Chọn hai.)
A. Confidentiality
B. Integrity
3. Ngoài lưu lượng không dây được mã hóa, bạn định cấu hình bộ định tuyến không dây của mình để yêu cầu kết nối người dùng để xác thực với máy chủ RADIUS. Bạn đã cấu hình loại bảo mật nào? D. WPA2 Enterprise
4. Bạn quyết định nắm bắt lưu lượng truy cập mạng bằng một trình thám thính trong khi kết nối với điểm truy cập Wi-Fi công cộng bận rộn. Sau vài phút, bạn nhận ra rằng bạn chỉ có thể thấy lưu lượng truy cập mạng của mình bên cạnh các chương trình phát sóng và phát đa hướng. Tại sao bạn không thể thấy ai khác lưu lượng truy cập mạng không dây?
D. Isolation mode is enabled
5. Một chuyên gia CNTT tò mò lái xe qua một khu công nghiệp vào đêm khuya trong khi quét các mạng không dây không bảo mật bằng máy PDA. Cái này gọi là gì?
B. War driving
6. EAP áp dụng những vấn đề bảo mật nào sau đây?
C. Network authentication
7. Cơ chế nào chỉ yêu cầu chứng chỉ PKI phía máy chủ để mã hóa lưu lượng xác thực người dùng?
B. PEAP

8. Bạn đang định cấu hình quyền truy cập vào mạng LAN không dây trên máy tính xách tay Windows 8.1. Khi bạn liệt kê các mạng không dây có sẵn, bạn sẽ nhận thấy nhiều danh sách của Mạng ẩn. Tùy chọn bộ định tuyến không dây nào được sử dụng cho các mạng ẩn này?

A. Disable SSID broadcast

9. Giao thức mã hóa không dây nào sử dụng chế độ truy cập để làm cho việc phát hiện mẫu khó khăn?

A. CCMP

10. Bạn đang thực hiện một cuộc khảo sát trang web không dây tại một trang web của khách hàng. Khách hàng bày tỏ mong muốn giữ an toàn truyền không dây. Có một bộ định tuyến không dây 802.11n duy nhất với ăng ten đa hướng trong phòng máy chủ ở một đầu của tòa nhà. WPA2 Enterprise và MAC lọc đã được cấu hình. Vấn đề bổ sung nào bạn nên giải quyết?

C. Move the wireless router to the center of the building

11. Có thể làm gì để bảo mật mạng không dây?

A. Decrease power transmission level to cover only the intended area.

12. Người dùng trong công ty của bạn đưa ra lệnh sau trên máy tính xách tay không dây của công ty họ: Netsh wlan đặt chế độ mạng được lưu trữ = allow ssid = AcmeWLAN key = password. Điều gì mô tả tốt nhất vấn đề bảo mật được tạo bởi người dùng này?

C. The user has created a rogue access point.

13. Bạn là quản trị viên mạng không dây. Người dùng báo cáo kết nối mạng không dây 802.11g không ổn định. Sau khi kiểm tra cẩn thận, bạn nhận ra điện thoại không dây 2,4 GHz và các thiết bị Bluetooth đang can thiệp vào Wi-Fisignal. Lựa chọn nào mang đến giải pháp tốt nhất?

D. Change the Wi-Fi channel used by your wireless router.

14. Một hacker cấu hình một điểm truy cập giả mạo để xuất hiện dưới dạng một điểm truy cập Wi-Fi hợp pháp. Thuật ngữ nào mô tả đúng nhất cấu hình này?

A. Evil twin

15. Điều nào sau đây đề cập đến các tin nhắn không mong muốn được gửi đến các thiết bị Bluetooth gần đó?

B. Bluejacking

16. Điều nào sau đây đề cập đến việc truy cập dữ liệu trái phép của thiết bị Bluetooth qua mạng không dây Bluetooth?

B. Bluesnarfing

17. Bạn đang làm việc tại một trang web của khách hàng để giải quyết các vấn đề về hiệu suất không dây. Khi làm như vậy, bạn nhận thấy WEP được cấu hình trên các bộ định tuyến không dây của máy khách. Loại tấn công nào mạng này có thể dễ bị ảnh hưởng?

B. IV attack

18. Làm thế nào bạn có thể kiểm soát liệu tất cả các thiết bị không dây sẽ nhìn thấy tên mạng WLAN của bạn?

A. Disable SSID broadcasting

19. Những mục nào sau đây có thể can thiệp vào mạng không dây 802.11g?

B. Microwave oven

20. Để bảo vệ mạng không dây, bạn quyết định kích hoạt EAP-TLS để ủy quyền truy cập máy khách không dây vào mạng LAN không dây. Bạn nên làm gì tiếp theo?

B. Install a smartcard on the client and a public key certificate on the server

21. TKIP được sử dụng chủ yếu theo tiêu chuẩn không dây nào?
C. WPA
22. Bạn là một chuyên gia về Wifi. Người dùng báo cáo rằng mạng 802.11g mới không chạy ở tốc độ 54Mbps được quảng cáo. Bạn nên nói gì với người dùng không dây?
C. Wi-Fi bandwidth is shared by all users connected to the same wireless network.
23. Tiêu chuẩn nào yêu cầu các trạm xác thực trước khi có quyền truy cập mạng?
C. 802.1x
24. Bạn đang bảo vệ cơ sở hạ tầng mạng Wi-Fi của mình. Bạn định cấu hình phần mềm giám sát mạng với danh sách MAC điểm truy cập không dây hợp lệ được phép trên mạng. Loại mối đe dọa này sẽ cho phép bạn phát hiện?
A. Rogue access points
25. Bạn đang cấu hình một mạng không dây cho văn phòng nhà bạn. Những tùy chọn được áp dụng cho một mạng gia đình? (Chọn hai.)
A. WPA2 PSK
D. WPA PSK
Một người dùng du lịch gọi bàn trợ giúp về vấn đề kết nối không dây của cô ấy. Khi cô ấy cố gắng kết nối với một mạng không dây có thể nhìn thấy ở mức tối đa, cuối cùng nó sẽ hết thời gian mà không có tin nhắn nào nữa. Vấn đề là gì?
B. MAC address filtering is blocking her wireless network card.
26. Bạn đang thưởng thức một tách cà phê tại quán cà phê địa phương thì đột nhiên điện thoại di động của bạn hiển thị một tin nhắn nặc danh khen ngợi bạn về chiếc áo Hawaii của bạn. Bạn là nạn nhân của cái gì?
C. Bluejacking
27. See “In-Depth Answers.” Khớp các điều khoản chính sách bảo mật với kịch bản chính xác

Security Policy Terms	Scenarios
Captive portal ____	**A.** You are upgrading wireless access points in your company. Your manager has asked that you purchase equipment that will increase wireless transmission speeds.
MIMO ____	**B.** To adhere to corporate security policies, you must ensure that Wi-Fi devices cannot access corporate network resources without additional authentication.
Directional antenna ____	**C.** To adhere to corporate security policies, you must ensure that Wi-Fi devices cannot access the Internet without first authenticating.
VPN ____	**D.** You are a network infrastructure technician for a university. Your colleague, Franco, is tweaking wireless connectivity between two buildings on campus using a specialized antenna on each wireless router. Franco is carefully adjusting the positioning of the antennae to cover the long distance between the two buildings.

28. Bạn là chủ sở hữu của Stacey từ Coffee Spot, một quán cà phê cung cấp cho khách hàng hương vị cà phê quốc tế trong một môi trường thư giãn. Để thu tiền thanh toán, bạn muốn triển khai một công nghệ, theo đó khách hàng của bạn có thể chỉ cần vẫy điện thoại thông minh của họ cách thiết bị thanh toán vài centimet. Bạn nên sử dụng công việc nào sau đây?
B. NFC
29. Phát biểu nào sau đây liên quan đến các cuộc tấn công phát lại là đúng?
D. They are conducted by capturing and resending wireless network traffic.

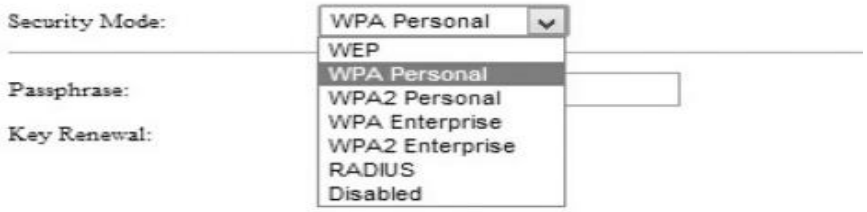
30. Bạn đang định cấu hình bộ định tuyến không dây mới và nhận thấy mã PIN ở mặt sau của bộ định tuyến không dây. Mục đích của mã PIN là gì?

A. It allows home users to secure a wireless network easily

31. Patchy-Adams là một cơ sở nghiên cứu y tế độc đáo chuyên sử dụng chất tẩy rửa và vitamin C để chữa bệnh. Bạn đã được Patchy-Adams thuê để đề xuất chiến lược triển khai mạng không dây tuân thủ các yêu cầu sau:

D. MIMO, WPA2 Enterprise, SSL, MAC filtering

32. WPA2 Personal.Bạn đang cấu hình một bộ định tuyến không dây tại nhà để sử dụng với thực hành y tế tại nhà của bạn. Mạng bao gồm hai máy tính để bàn Windows, iPhone và máy tính bảng dựa trên Android. Luật riêng tư quy định rằng tất cả các giao tiếp mạng không dây phải an toàn nhất có thể. Chế độ bảo mật nào trong Hình 9-1 bạn nên



cấu hình?

33. Đồng nghiệp phàn nàn rằng họ không thể kết nối với mạng không dây tại văn phòng và bạn nhận thấy rằng có rất nhiều nhiễu sóng không dây. Cuộc tấn công nào đang diễn ra?

B. Jamming attack

34. Sếp của bạn tiếp cận bạn về việc thực hiện một giải pháp không dây trong đó các ăng ten và bộ điều khiển được tách ra để dễ dàng nâng cấp. Những thuộc tính nào bạn đang tìm kiếm trong một điểm truy cập để đáp ứng các yêu cầu này? (Chọn hai.)

A. Thin

C. Controller-based

35. Nghiên cứu người dùng trong tổ chức của bạn yêu cầu quyền truy cập vào các ứng dụng web trong mạng riêng của tổ chức đối tác. Tổ chức của bạn hiện được định cấu hình là nhà cung cấp xác thực đáng tin cậy cho cả hai công ty. Việc xác minh thông tin đăng nhập của người dùng không nên được tiến hành bởi các thiết bị cạnh. Nên cấu hình cái gì?

B. RADIUS federation

CHƯƠNG 10

2. Người dùng đi du lịch của bạn yêu cầu truy cập từ xa an toàn đến các máy chủ cơ sở dữ liệu của công ty. Bạn nên làm gì cấu hình cho họ?

A. Modem

B. Mạng WLAN

C. VPN

D. Mạng nội bộ

3. Bạn là quản trị viên mạng cho một công ty tiếp thị quốc gia. Nhân viên có thời gian dài cuộc gọi điện thoại với các đồng nghiệp từ khắp đất nước. Để giảm chi phí, bạn đã yêu cầu đề xuất giải pháp điện thoại thay thế. Điều nào sau đây bạn có thể đề nghị?

A. Modem

B. VoIP

C. Trò chuyện qua văn bản trên Internet

D. E-mail

4. Bạn là một nhà tư vấn bảo mật CNTT đang kiểm tra một mạng. Trong khi bạn trình bày kết quả kiểm toán, một trong những khách hàng của bạn hỏi những gì có thể được sử dụng để ngăn chặn truy cập LAN trái phép. Làm thế nào để bạn trả lời câu hỏi?

A. NAC

B. Tường lửa lọc gói

C. PKI

D. SSL

5. Loại máy chủ nào xác thực người dùng trước khi cho phép truy cập mạng?

A. Máy chủ tệp

B. Thư mục hoạt động

C. RADIUS

D. Bộ điều khiển miền

6. Điều nào sau đây là ví dụ về máy khách RADIUS? (Chọn hai.)

A. Máy khách VPN

B. Công tắc có khả năng 802.1x

C. Bộ định tuyến không dây

D. Hệ điều hành Windows 7

E. Hệ điều hành Linux

7. Điều nào sau đây là đúng về TACACS +? (Chọn ba.)

A. Nó tương thích với TACACS. B. Nó tương thích với RADIUS.

C. Đây là một giao thức độc quyền của Cisco.

D. Nó có thể được sử dụng thay thế cho RADIUS.

E. TACACS + sử dụng TCP.

8. Bạn là quản trị viên mạng cho mạng UNIX. Bạn đang lên kế hoạch bảo mật mạng của bạn. Phải chọn một giao thức bảo mật để xác thực tất cả người dùng đăng nhập. Đó là xác thực hợp lệ Lựa chọn giao thức?

A. TCP

B. Mạng lưới

C. Kerberos

D. AES

9. Một khách hàng yêu cầu bạn đánh giá tính khả thi của môi trường hệ điều hành máy khách và máy chủ Linux. Các mối quan tâm chính là có một cơ sở dữ liệu trung tâm của tài khoản người dùng và máy tính có khả năng bảo mật xác thực. Những lựa chọn Linux nào bạn nên khám phá?

A. NFS

B. SSH

C. Samba

D. LDAP

10. Bạn đang định cấu hình thiết bị xác thực mạng của Cisco. Trong quá trình cấu hình, bạn được cung cấp một danh sách lựa chọn xác thực. Sự lựa chọn nào cung cấp bảo mật và độ tin cậy tốt nhất?
A. RADIUS
B. TACACS
C. TACACS
D. XtACACS
13. Một tập đoàn đã đầu tư rất nhiều vào việc phát triển một sản phẩm được nhiều người tìm kiếm. Để bảo vệ nó inveStment, công ty muốn đảm bảo rằng chỉ có nhân viên cụ thể có thể vào một cơ sở nghiên cứu.
Điều nào sau đây được coi là an toàn nhất?
A. Xây dựng thẻ truy cập
B. Quét giọng nói
C. Máy quét dấu vân tay
D. Máy quét võng mạc
16. Điều nào sau đây ngăn người dùng phải chỉ định thông tin đăng nhập khi truy cập nhiều các ứng dụng?
A. Đăng nhập một lần
B. Nhớ mật khẩu của tôi
C. Xác thực sinh trắc học
D. Hệ điều hành đáng tin cậy
17. Giao thức xác thực nào thay thế RADIUS?
A. TACACS
B. TACACS +
C. XtACACS
D. Đường kính
20. Ví dụ nào sau đây minh họa tốt nhất cho xác thực?
A. Một người dùng truy cập vào một thư mục dùng chung mà anh ta đã được cấp phép.
B. Một máy tính tự nhận dạng thành công máy chủ trước khi đăng nhập người dùng.
C. Một mạng chứa hai liên kết mạng đến một văn phòng từ xa trong trường hợp một lỗi.
D. Một thiết bị mạng mã hóa tất cả lưu lượng truy cập mạng trước khi truyền thêm.
21. Một kỹ thuật viên đang khắc phục sự cố truy cập của người dùng vào mạng không dây 802.1x có tên CORP. máy tính trước đây đã được cung cấp một địa chỉ IP trên mạng 10.17.7.0/24, nhưng bây giờ vì một số lý do, nó có địa chỉ IP trên mạng 10.16.16.0/24. DHCP hoạt động chính xác trên mạng. Các
kỹ thuật viên báo cáo máy gần đây đã được đánh giá lại và hình ảnh sử dụng DHCP. Nhiều khả năng là gì Nguyên nhân của vấn đề?
A. Máy trạm có địa chỉ IP tĩnh trên mạng 10.16.16.0/24.
B. Kỹ thuật viên cần ban hành lệnh ipconfig / refresh.
C. Thời gian máy trạm không chính xác.
D. Máy trạm cần được cài đặt lại chứng chỉ PKI.
22. Loại vấn đề bảo mật nào sẽ kiểm soát truy cập mạng (NAC) tốt nhất?
A. Từ điển tấn công
B. Ngộ độc bộ đệm ARP

C. WEP
D. Tấn công SQL SQL
23. Mạng nội bộ của công ty bao gồm nhiều máy chủ web nội bộ khác nhau, mỗi máy chủ sử dụng các cửa hàng xác thực khác nhau. Điều gì sẽ cho phép người dùng sử dụng cùng tên người dùng và mật khẩu cho tất cả các trang web nội bộ?
A. NAC
B. SSO
C. VPN
D. Thẻ thông minh
24. Trong khi chụp lưu lượng mạng, bạn nhận thấy thông tin văn bản rõ ràng đang được truyền đi. Sau khi điều tra Tiêu đề TCP, bạn nhận thấy cổng đích là 389. Đây là loại lưu lượng xác thực nào?
A. EAP
B. EAP-TLS
C. LDAP
D. CHAP
25. Bạn đang đánh giá các giải pháp lưu trữ đám mây công cộng. Người dùng sẽ được xác thực với một máy chủ cục bộ trên của bạn mạng sẽ cho phép họ truy cập vào bộ lưu trữ đám mây. Tiêu chuẩn liên đoàn nào có thể cấu hình để đạt được điều này?
A. LDAP
B. SSL
C. PKI
D. SAML
27. Bạn đã được một trường đại học thuê để giới thiệu các giải pháp CNTT. Hiện nay, sinh viên và giảng viên sử dụng thẻ gần để truy cập các tòa nhà trong khuôn viên trường sau nhiều giờ, và họ có tên người dùng và mật khẩu để lo g vào máy tính phòng thí nghiệm. Trường đại học muốn sử dụng thông tin PKI duy nhất cho mỗi người dùng để cho phép 188access đến các tòa nhà trong khuôn viên trường và đăng nhập vào các máy trạm trong phòng thí nghiệm. Bạn nên giới thiệu gì?
A. Mã thông báo phần cứng và mật khẩu
B. Thẻ truy cập thông thường
C. Khóa riêng PKI
D. Cơ quan cấp chứng chỉ PKI
29. ACL bộ định tuyến của bạn như sau:
ip access-group 55 out
access-list 55 permit host 199.126.129.8
access-list 55 permit host 199.126.129.9
Máy trạm, PC1, có địa chỉ IP là 199.126.129.10 cố gắng truy cập mạng từ xa và được ngăn chặn làm như vậy. Phát biểu nào mô tả chính xác kịch bản này?
A. PC1 rõ ràng đã bị từ chối truy cập vào mạng từ xa.
B. PC1 đã hoàn toàn bị từ chối truy cập vào mạng từ xa.
C. PC1 rõ ràng đã được cấp quyền truy cập vào mạng từ xa.

D. PC1 được cấp quyền truy cập vào mạng từ xa.
31. Bạn là quản trị viên Microsoft Active Directory cho một cơ quan chính phủ Mỹ. Hoạt động Miền thư mục ở Los Angeles được định cấu hình để tin cậy miền Active Directory ở Chicago, trong đó tin tưởng vào miền Active Directory ở Orlando. Thuật ngữ nào mô tả chính xác mối quan hệ tin cậy Giữa Los Angeles và Orlando?
A. Niềm tin bắc cầu
B. Tin tưởng mạng diện rộng
C. NTLM
D. NTLMv2
32. Điều nào sau đây là khung xác thực / ủy quyền? (Chọn tất cả các áp dụng.)
A. Kết nối OpenID
B. Liên đoàn
C. TIẾNG ANH
D. Shibboleth
E. Mã thông báo an toàn

CHƯƠNG 11

1. Quản trị viên mạng phải cấp quyền mạng phù hợp cho nhân viên mới. Mà Sau đây là chiến lược tốt nhất?
A. Cung cấp cho tài khoản người dùng nhân viên mới các quyền và quyền cần thiết.
B. Thêm tài khoản người dùng nhân viên mới vào một nhóm. Đảm bảo rằng nhóm có các quyền cần thiết và quyền.
C. Cung cấp cho nhân viên mới quyền quản trị mạng.
D. Hỏi nhân viên mới những quyền mà cô ấy muốn.
4. James là quản trị viên mạng chi nhánh của ABC, Inc. Gần đây, trụ sở công ty đã yêu cầu kiểm toán an ninh mạng, vì vậy James đã tự thực hiện kiểm toán bằng các công cụ Linux có sẵn miễn phí. Những gì là vấn đề với hành động của James lòng?
A. ABC, Inc., nên đã gửi một quản trị viên mạng từ trụ sở chính để thực hiện kiểm toán.
B. Nhân viên an ninh nên đã tiến hành kiểm toán.
C. Các công cụ có sẵn tự do không đáng tin cậy và không nên được sử dụng.
D. Một bên thứ ba nên được thuê để tiến hành kiểm toán.
5. Một môi trường điện toán an toàn ghi nhãn dữ liệu với các phân loại bảo mật khác nhau. Người dùng xác thực phải có giải phóng mặt bằng để đọc dữ liệu phân loại này. Loại mô hình kiểm soát truy cập này là gì?
A. Kiểm soát truy cập bắt buộc
B. Kiểm soát truy cập tùy ý
C. Kiểm soát truy cập dựa trên vai trò
D. Kiểm soát truy cập thời gian trong ngày
7. Linda tạo một thư mục có tên Dự đoán ngân sách trong tài khoản nhà của mình và chia sẻ nó với các đồng nghiệp trong bộ phận. Điều nào sau đây mô tả đúng nhất về loại hệ thống kiểm soát truy cập này?
A. Kiểm soát truy cập bắt buộc
B. Kiểm soát truy cập tùy ý
C. Kiểm soát truy cập dựa trên vai trò

D. Kiểm soát truy cập thời gian trong ngày
8. Bạn yêu cầu người dùng không được đăng nhập vào mạng sau 6 giờ chiều. trong khi bạn phân tích lưu lượng mạng trong giờ không kinh doanh. Những gì bạn nên làm?
A. Rút phích cắm các trạm của họ khỏi mạng.
B. Yêu cầu người dùng nhấn ctrl-alt-del để khóa các trạm của họ.
C. Định cấu hình các giới hạn thời gian trong ngày để đảm bảo không ai có thể đăng nhập sau 6 giờ chiều.
D. Vô hiệu hóa tài khoản người dùng lúc 6 giờ chiều
11. Thiết bị VPN của bạn được định cấu hình để không cho phép xác thực người dùng trừ khi người dùng hoặc nhóm được liệt kê là
được phép Liên quan đến người dùng bị chặn, những gì mô tả tốt nhất cấu hình này?
A. Cho phép ngầm
B. Từ chối ngầm
C. Cho phép rõ ràng
D. Từ chối rõ ràng
12. Margaret là trưởng phòng nhân sự của Emrom, Inc. Một nhân viên không muốn sử dụng hàng năm phân bổ kỳ nghỉ, nhưng Margaret khẳng định đó là bắt buộc. Lợi ích CNTT có được là gì từ bắt buộc kỳ nghỉ?
A. Sự bất thường trong nhiệm vụ công việc có thể được nhận thấy khi một nhân viên khác hoàn thành vai trò đó.
B. Người dùng cảm thấy được sạc lại sau thời gian nghỉ.
C. Emrom, Inc., sẽ không phạm tội vi phạm lao động.
D. Có ít rủi ro bảo mật hơn khi có ít người dùng hơn trên mạng.
14. Hợp đồng chính phủ yêu cầu máy tính của bạn tuân thủ các phương pháp kiểm soát truy cập bắt buộc và bảo mật đa cấp. Bạn nên làm gì để duy trì tuân thủ hợp đồng này?
A. Vá hệ điều hành hiện tại của bạn.
B. Mua phần cứng mạng mới.
C. Sử dụng hệ điều hành đáng tin cậy.
D. Mua thiết bị mã hóa mạng.
15. Thuật ngữ nào được xác định tốt nhất là danh sách đối tượng của người dùng, nhóm, quy trình và quyền của họ?
A.
B. ACL
C. Thư mục hoạt động
D. Nhật ký truy cập
16. Người dùng phàn nàn rằng họ phải nhớ mật khẩu cho vô số tài khoản người dùng để truy cập phần mềm cần thiết cho công việc của họ. Làm thế nào điều này có thể được giải quyết?
A. SSO
B. ACL
C. PKI
D. Độ phức tạp của mật khẩu
21. Một bộ định tuyến mạng có ACL sau:

ip access-group 101 in
access-list 101 permit tcp any any eq 20
access-list 101 permit tcp any any eq 21
access-list 101 permit tcp any any eq 3389
Chọn mô tả chính xác của cấu hình ACL.
A. SMTP, SNMP và RDP được cho phép rõ ràng; tất cả những thứ khác đều bị từ chối ngầm.
B. SMTP, SNMP và RDP được cho phép hoàn toàn; tất cả những thứ khác bị từ chối rõ ràng.
C. FTP và RDP được cho phép rõ ràng; tất cả những thứ khác đều bị từ chối ngầm.
D. FTP và RDP được cho phép ngầm; tất cả những thứ khác bị từ chối rõ ràng.
23. Một kỹ thuật viên thông báo các máy tính trái phép truy cập vào một mạng được bảo vệ nhạy cảm. Những giải pháp
Kỹ thuật viên có nên cân nhắc?
A. Mật khẩu mạnh hơn
B. Mã hóa mạng
C. VPN
D. NAC
24. Quản trị viên mạng, Justin, phải cấp cho nhiều bộ phận khác nhau quyền truy cập vào thư mục Corp_Pol khâu và cấp cho các bộ phận khác đọc và ghi quyền truy cập vào thư mục Current_Projects. Chiến lược nào nên Justin tuyển dụng?
A. Thêm tất cả người dùng bộ phận vào ACL thư mục dùng chung với các quyền thích hợp.
B. Tạo một nhóm, thêm thành viên và thêm nhóm vào ACL thư mục phù hợp
quyền.
C. Tạo nhóm người dùng và nhóm quản trị viên với các thành viên chính xác. Thêm các nhóm vào ACL thư mục với các quyền thích hợp.
D. Tạo một nhóm cho mỗi bộ phận và thêm thành viên vào các nhóm. Thêm các nhóm vào thư mục ACL với các quyền thích hợp.
27. Sự khác biệt giữa giải phóng mặt bằng bảo mật và nhãn phân loại là gì? (Chọn hai.)
A. Không có sự khác biệt.
B. Nhãn phân loại xác định độ nhạy dữ liệu.
C. Giải phóng mặt bằng bảo mật xác định độ nhạy dữ liệu.
D. Giải phóng mặt bằng an ninh được so sánh với nhãn phân loại.
31. Một tin nhắn e-mail hợp pháp cuối cùng bị gắn cờ là thư rác. Thuật ngữ nào mô tả đúng nhất tình huống này?
A. Sai dương tính
B. Âm tính thật
C. Sai âm
D. Đúng tích cực
33. Loại bộ điều khiển truy cập nào mà bộ định tuyến sử dụng để cho phép hoặc từ chối lưu lượng mạng?
A. Kiểm soát truy cập dựa trên vai trò
B. Kiểm soát truy cập bắt buộc
C. Kiểm soát truy cập tùy ý

D. Kiểm soát truy cập dựa trên quy tắc

34. Là quản trị viên máy chủ, bạn định cấu hình cài đặt bảo mật sao cho mật khẩu phức tạp ít nhất tám ký tự dài phải được sử dụng bởi tất cả các tài khoản người dùng. Đây là loại thực hành quản lý nào?

A. Hết hạn

B. Phục hồi

C. Thông tin xác thực

D. Tàn phế

35. Bạn là một chuyên gia kiểm toán an ninh. Sau khi đánh giá mức độ sử dụng máy chủ và máy chủ Linux, bạn xác định rằng các thành viên của nhóm quản trị CNTT thường xuyên đăng nhập vào máy chủ Linux bằng tài khoản gốc trong khi thực hiện các tác vụ máy tính thông thường. Những khuyến nghị nào bạn nên đưa ra dựa trên những phát hiện của bạn? (Chọn ba.)

A. Không cho phép nhiều người dùng sử dụng thông tin chung.

B. Tiến hành đánh giá truy cập người dùng định kỳ.

C. Giám sát máy chủ Linux sử dụng liên tục.

D. Mã hóa tất cả các tệp trên máy chủ Linux.

39. Ana là quản trị viên Windows Server cho bộ phận chính phủ liên bang. Tất cả các máy chủ Windows của bộ phận được nối với một miền Active Directory. Các quy định mới yêu cầu lịch sử mật khẩu người dùng được giữ lại để ngăn việc sử dụng lại mật khẩu. Sử dụng ít nỗ lực quản trị nhất, làm thế nào Ana có thể thực thi các cài đặt mới cho tất cả người dùng bộ phận?

A. PowerShell

B. Chính sách nhóm

C. Chính sách nhóm cục bộ

D. Tệp hàng loạt

CHƯƠNG 12

3. Người quản lý CNTT yêu cầu bạn đề xuất giải pháp mã hóa LAN. Các giải pháp phải hỗ trợ hiện tại và phần mềm trong tương lai không có mã hóa của riêng nó. Bạn nên giới thiệu gì?

A. SSL

B. SSH

C. IPSec

D. VPN

4. Giao thức nào thay thế SSL?

A. TLS

B. SSO

C. TKIP

D. VPN

10. Bạn quyết định rằng các máy tính LAN của bạn sẽ sử dụng mã hóa bất đối xứng với IPSec để bảo mật lưu lượng LAN.

Trong khi đánh giá làm thế nào điều này có thể được thực hiện, bạn được trình bày với một loạt các lựa chọn mã hóa. Chọn

việc phân loại chính xác các tiêu chuẩn mật mã.
A. Không đối xứng: RSA, AES
Đối xứng: DES, 3DES
B. Đối xứng: 3DES, DES
Không đối xứng: Cá nóc, RSA
C. Đối xứng: 3DES, DES
Không đối xứng: RC4, RSA
D. Đối xứng: AES, 3DES
Không đối xứng: RSA
12. Mật mã khối đối xứng nào thay thế cho blowfish?
A. Twofish
B. Cá bốn màu
C. RSA
D. PKI
13. Một người dùng kết nối với một trang web ngân hàng trực tuyến bảo mật. Phát biểu nào sau đây không đúng?
A. Khóa công khai của máy trạm được sử dụng để mã hóa dữ liệu được truyền đến máy chủ web. Máy chủ web
khóa riêng thực hiện việc giải mã.
B. Khóa phiên của máy trạm được mã hóa bằng khóa chung của máy chủ và được truyền tới web máy chủ. Khóa riêng của máy chủ web thực hiện giải mã.
C. Khóa phiên do máy trạm tạo được sử dụng để mã hóa dữ liệu được gửi đến máy chủ web.
D. Khóa phiên do máy trạm tạo được sử dụng để giải mã dữ liệu mà máy chủ web nhận được.
14. Thuật ngữ nào mô tả quá trình che giấu tin nhắn trong một tập tin?
A. Trojan
B. Steganography
C. Mã hóa
D. Chữ ký số
17. Cách tiếp cận mật mã nào sử dụng các điểm trên một đường cong để xác định các cặp khóa công khai và riêng tư?
A. RSA
B. DES
C. ECC
D. PKI
20. Điều nào sau đây là đúng về mật mã? (Chọn hai.)
A. Chặn mật mã phân tích các mẫu dữ liệu và chặn dữ liệu độc hại được mã hóa**.**
B. Luồng mã hóa dữ liệu mã hóa một byte mỗi lần.
C. Khối mật mã mã hóa dữ liệu.
D. Dòng mật mã mã hóa lưu lượng phương tiện truyền thông.
25. Khi làm cứng VPN, bạn nên cân nhắc điều gì? (Chọn hai.)
A. Kích hoạt PAP
B. Vô hiệu hóa PAP

C. Vô hiệu hóa EAP-TLS

D. Kích hoạt EAP-TLS

26. Mã hóa và ký điện tử e-mail bằng khóa công khai và khóa riêng có thể được thực hiện với công nghệ nào?

A. 3DES

B. DES

C. Cá thổi

D. PGP

27. Điều nào sau đây được coi là kém an toàn nhất?

A. MS-CHAP v2

B. NTLM v2

C. EAP-TLS

D. PAP

29. Điều nào sau đây là đúng khi nói về khóa riêng của người dùng? (Chọn hai.)

A. Nó được sử dụng để mã hóa tin nhắn đã gửi.

B. Nó được sử dụng để giải mã tin nhắn nhận được.

C. Nó được sử dụng để tạo chữ ký số.

D. Nó được sử dụng để xác minh chữ ký số.

31. Điều nào sau đây mô tả đúng nhất về giao thức Diffie-Hellman?

A. Đây là một giao thức trao đổi khóa để mã hóa bất đối xứng.

B. Đó là một thuật toán mã hóa đối xứng.

C. Đây là một giao thức trao đổi khóa để mã hóa đối xứng.

D. Đây là một thuật toán băm.

32. Điều nào sau đây áp dụng cho các phím đối xứng? (Chọn hai.)

A. Khóa công khai được sử dụng để mã hóa.

B. Khóa riêng được sử dụng để giải mã.

C. Khóa tương tự được sử dụng để mã hóa và giải mã.

D. Chúng được trao đổi ngoài băng.

33. Hai giao thức đàm phán phổ biến nào sau đây được TLS sử dụng? (Chọn hai.)

A. Mật mã học lượng tử

B. DHE

C. RSA

D. ECDhe

35. Trong cuộc họp CNTT hàng tháng tại văn phòng của bạn, người quản lý CNTT của bạn, Julia, bày tỏ mối quan tâm về người dùng yếu mật khẩu trên các máy chủ của công ty và làm thế nào chúng có thể dễ bị tấn công bằng mật khẩu.

Khi làm phiền Julia về mối quan tâm của cô ấy, bạn có thể sử dụng thuật ngữ nào?

A. Rèn chìa khóa

B. Ký quỹ chính

C. Kéo dài khóa

D. Chuyển tiếp chính

37. Sau khi xem xét kết quả kiểm toán an ninh mạng, nhóm CNTT của bạn quyết định triển khai kiểm toán viên 224 khuyến nghị để đảm bảo lưu lượng truy cập nội bộ. Giải pháp nào giải quyết vấn đề ngộ độc tên hồ sơ máy chủ giải quyết?

A. IPsec

B. DNSSEC

C. SSL

D. TLS

39. Ban quản lý đã yêu cầu bạn, người đứng đầu bộ phận bảo mật CNTT, thực hiện một mối đe dọa CNTT tập trung và thống nhất hệ thống quản lý cho tất cả sáu văn phòng, được lan rộng khắp Tây Âu. Có một ngân sách bảo mật CNTT hạn chế có sẵn. Giải pháp nào có thể bảo mật đúng sáu vị trí với mức tối thiểu
Giá cả?

A. Mua phần cứng và giấy phép phù hợp cho từng vị trí. Cấu hình giải pháp để giám sát
các mối đe dọa tại mỗi trang web.

B. Sử dụng dịch vụ dựa trên đăng ký.

C. Mua phần cứng và giấy phép phù hợp cho từng vị trí. Cấu hình giải pháp để giám sát
các mối đe dọa ở tất cả các trang web.

D. Cập nhật phần mềm chống phần mềm độc hại trên thiết bị ở tất cả sáu địa điểm.

40. Chế độ mã hóa khối nào sử dụng phương thức mã hóa dựa trên phản hồi để đảm bảo rằng kết quả dữ liệu lặp đi lặp lại. Trong văn bản mật mã độc đáo?

A. ECB

B. CTM

C. GCM

D. CBC

42. Thuật ngữ nào mô tả chính xác nhất về thẻ thông minh?

A. Công suất thấp

B. Một cái gì đó bạn biết

C. Một cái gì đó bạn là

D. Cơ quan cấp chứng chỉ PKI

CHƯƠNG 13

1. Sau khi nhập tệp chứng chỉ người dùng vào chương trình e-mail, người dùng thấy cô ấy không thể ký điện tử gửi thư điện tử. Một số lý do có thể cho việc này là gì? (Chọn hai.)

A. Khóa công khai không có trong chứng chỉ.

B. Khóa riêng không có trong chứng chỉ.

C. Chứng chỉ không được tạo để sử dụng e-mail.

D. PKI không có trong chứng chỉ.

2. Điều nào sau đây sẽ không được tìm thấy trong một chứng chỉ kỹ thuật số?

A. Khóa công khai

B. Khóa riêng

C. Chữ ký số phát hành CA

D. Địa chỉ IP của máy chủ PKI

4. Là một kiểm toán viên bảo mật, bạn đang tập trung vào việc làm cứng PKI hiện có. Bạn nên làm điều nào sau đây xem xét? (Chọn hai.)
A. Đi CA nhé.
B. Không làm cho khóa công khai có thể truy cập.
C. Cấu hình một tác nhân phục hồi.
D. Mã hóa tất cả các chứng chỉ kỹ thuật số.
5. Đồng nghiệp của bạn báo cáo rằng có một khung thời gian ngắn trong đó chứng chỉ bị thu hồi vẫn có thể được sử dụng. Tại sao lại thế này?
A. CRL được xuất bản định kỳ.
B. CRL được xuất bản ngay lập tức nhưng phải sao chép tới tất cả các máy chủ.
C. Danh sách CRL chỉ thu hồi số sê-ri chứng chỉ và không được sử dụng dưới bất kỳ hình thức nào.
D. CRL phụ thuộc vào băng thông mạng.
6. Điều nào sau đây mô tả đúng nhất về thuật ngữ ký quỹ chính?
A. Bên thứ ba đáng tin cậy có khóa giải mã trong trường hợp khóa gốc đã hết hạn
B. Một bên thứ ba đáng tin cậy với các bản sao của khóa giải mã bên cạnh các khóa gốc hiện có
C. Một tài khoản có thể được sử dụng để mã hóa khóa riêng
D. Một tài khoản có thể được sử dụng để mã hóa dữ liệu cho bất kỳ người dùng nào
7. Thành phần PKI nào xác minh danh tính của người yêu cầu chứng chỉ trước khi chứng chỉ được cấp?
A. Khóa công khai
B. RA
C. PKI
D. CRL
8. Một người dùng báo cáo rằng cô ấy không thể xác thực với VPN công ty khi đi du lịch. Bạn có đã cấu hình VPN để yêu cầu xác thực chứng chỉ người dùng X.509. Sau khi điều tra vấn đề, bạn le arn rằng chứng chỉ người dùng đã hết hạn Điều nào sau đây trình bày giải pháp an toàn nhanh nhất?
A. Tạo chứng chỉ người dùng mới và định cấu hình nó trên máy tính người dùng.
B. Vô hiệu hóa xác thực chứng chỉ X.509 cho VPN của bạn.
C. Giảm tần suất xuất bản CRL.
D. Đặt ngày trở lại trên thiết bị VPN thành trước khi chứng chỉ người dùng hết hạn.
9. Khi người dùng kết nối với máy chủ mạng nội bộ bằng cách nhập https: //intranet.acme.local, trình duyệt web của họ hiển thị một thông báo cảnh báo cho biết trang web không đáng tin cậy. Làm thế nào thông điệp cảnh báo này có thể được loại bỏ trong khi duy trì an ninh?
A. Định cấu hình máy chủ web để sử dụng HTTP thay vì HTTPS.
B. Cài đặt khóa riêng của máy chủ mạng nội bộ trên tất cả các máy trạm của khách hàng.
C. Sử dụng cổng TCP 443 thay vì cổng TCP 80.
D. Cài đặt chứng chỉ gốc đáng tin cậy trong trình duyệt web của máy khách cho nhà phát hành máy chủ mạng nội bộ chứng chỉ.
10. Một bảo mật máy chủ web đang được cấu hình, như trong Hình 13-1. Xác định lỗi cấu hình.
A. Đường dẫn trang web vật lý không nên nằm trên ổ C:.
B. Các trang web HTTPS phải sử dụng cổng 443.

C. Cổng 444 phải được sử dụng cho HTTP, không phải HTTPS**. D. Phải chọn chứng chỉ SSL.**
11. Một trang web được bảo mật HTTPS yêu cầu khả năng hạn chế các máy trạm nào có thể tạo kết nối.
Lựa chọn nào là an toàn nhất?
A. Định cấu hình trang web để chỉ cho phép kết nối từ địa chỉ IP của các máy trạm hợp lệ.
B. Định cấu hình trang web để chỉ cho phép kết nối từ địa chỉ MAC của các máy trạm hợp lệ.
C. Cấu hình trang web để sử dụng xác thực người dùng.
D. Cấu hình trang web để yêu cầu chứng chỉ phía máy khách.
12. Điều nào sau đây là không đúng sự thật về chứng chỉ có chứa khóa riêng?
A. Chúng có thể được sử dụng để mã hóa thư gửi cho người khác.
B. Chúng có thể được sử dụng để mã hóa nội dung đĩa cứng.
C. Chúng nên được bảo vệ bằng mật khẩu.
D. Chúng có thể được sử dụng để ký điện tử gửi thư cho người khác.
13. Chứng chỉ số máy tính sẽ được sử dụng cho mục đích gì? (Hay chọn đap an đung nhât.)
A. Kiểm soát truy cập mạng
B. IPSec
C. Cả A và B
D. Không có điều nào ở trên
14. Bạn chịu trách nhiệm cho phép SSL trên một trang web thương mại điện tử. Bạn nên làm gì đầu tiên?
A. Cài đặt chứng chỉ kỹ thuật số máy chủ web.
B. Kích hoạt SSL trên máy chủ web.
C. Tạo CSR và gửi nó cho CA.
D. Cấu hình máy chủ web để sử dụng cổng 443.
15. Trong khi tạo yêu cầu ký chứng chỉ cho một trang web, bạn nhập thông tin được liệt kê ở đây. Người dùng sẽ kết nối với trang web bằng cách gõ https://www.acme.com. Xác định lỗi cấu hình.
Hết hạn: 12 tháng
Độ dài bit: 2048
Tên thường gọi: 215.66.77.88
Tổ chức: Acme Inc.
NGOÀI: Bán hàng
Quốc gia: Mỹ
Nhà nước: TN
Thành phố: Memphis
A. Ngày hết hạn là một năm.
B. Độ dài bit phải là 128.
C. Tên chung phải là www.acme.com.
D. Trường trạng thái không được viết tắt.
16. Một công ty quốc gia có trụ sở tại Dallas, Texas, đang thực hiện PKI. Có công ty
lo
cation ở 12 thành phố lớn khác của Hoa Kỳ. Mỗi địa điểm đó có một quản trị viên mạng cao cấp.
Lựa chọn nào trình bày giải pháp PKI tốt nhất?

A. Cài đặt CA gốc ở Dallas. Tạo các CA cấp dưới cho mỗi thành phố và sử dụng chúng để cấp chứng chỉ cho người dùng và máy tính trong thành phố đó. Lấy CA gốc nhé.
B. Cài đặt CA gốc ở Dallas. Cấp giấy chứng nhận cho người dùng và máy tính ở tất cả các địa điểm.
C. Cài đặt CA gốc ở Dallas. Cấp giấy chứng nhận cho người dùng và máy tính ở tất cả các địa điểm. Lấy gốc CA nhé.
D. Cài đặt một CA gốc ở Dallas và mỗi thành phố. Cấp giấy chứng nhận cho người dùng và máy tính sử dụng mỗi thành phố
CA gốc. Lấy CA gốc nhé.
17. Một đồng nghiệp đã gửi cho bạn một tệp chứng chỉ kỹ thuật số để cài đặt trên máy tính của bạn để bạn có thể mã hóa
e-mail nhắn tin cho anh. Lỗi nào được tạo ra trong Hình 13-2 khi tệp được tạo?
A. Không nên có mật khẩu khóa riêng.
B. Không nên chia sẻ khóa riêng với người khác.
C. Tùy chọn Kích hoạt Bảo vệ Khóa Riêng tư Mạnh phải được bật.
D. Tùy chọn Bao gồm tất cả các thuộc tính mở rộng phải được tắt
18. Để bảo mật máy chủ của bạn, bạn muốn đảm bảo dữ liệu ổ cứng của máy chủ không thể được truy cập nếu cứng đĩa bị đánh cắp. Những gì bạn nên làm?
A. Cấu hình EFS.
B. Cấu hình TPM với các khóa mã hóa PKI.
C. Cấu hình bảo mật NTFS.
243D. Cấu hình mật khẩu bật nguồn.
20. Công ty của bạn, Acme, Inc., tiến hành kinh doanh với một nhà cung cấp, Widgets, Inc. Cả hai công ty đều có một
PKI hiện có với các CA cấp dưới của bộ phận. Một số bộ phận Widgets yêu cầu quyền truy cập vào
các máy chủ web Acme được bảo mật cụ thể yêu cầu chứng chỉ phía máy khách trước khi quyền truy cập được cấp. Gì
Giải pháp nào bạn nên đề xuất?
A. Các quản trị viên Acme nên tạo một CA gốc mới cho Widgets và cấp chứng chỉ cho những người đó
nhân viên cần truy cập vào máy chủ web Acme.
B. Quản trị viên Acme nên tạo một CA cấp dưới mới cho Widgets và cấp chứng chỉ cho những người đó
nhân viên cần truy cập vào máy chủ web Acme.
C. Các máy chủ web Acme phải được chứng nhận chéo với các CA cấp dưới Widgets thích hợp.
D. Các CA thích hợp của Widgets và Acme phải được chứng nhận chéo.
22. Chữ ký CA tồn tại trong tất cả các chứng chỉ kỹ thuật số mà nó cấp. CA sử dụng khóa nào để tạo
Chữ ký?
A. Riêng tư
B. Công cộng
C. Đối xứng
D. Không đối xứng
23. Trong PKI, CA đóng vai trò gì? (Chọn hai.)

A. Thu hồi giấy chứng nhận
B. Sử dụng khóa riêng của nó để ký chứng chỉ số
C. Sử dụng khóa chung của nó để ký chứng chỉ số
D. Kiểm soát truy cập vào mạng bằng chứng chỉ
24. Tiêu chuẩn X.509 được áp dụng theo cách nào sau đây?
A. LDAP
B. Chứng chỉ PKI
C. Xác thực sinh trắc học
D. Một loại vận tải mạng
25. Sử dụng Hình 13-3, khớp thuật ngữ thích hợp được liệt kê ở bên trái với yêu cầu được liệt kê ở bên phải. (Không phải tất cả các điều khoản sẽ được sử dụng.)
1-Key Escrow 2-CSR 3-OSCP
26. Bạn đang phát triển các tập lệnh Microsoft PowerShell để tự động hóa các tác vụ quản trị mạng. .PS1 tập tin tập lệnh cần phải được ký điện tử và tin cậy để chạy trên máy tính trong môi trường của bạn. Bạn có đã có được chứng chỉ PKI ký mã. Bạn cần sao lưu khóa riêng của mình. Tập tin nào
Bạn nên chọn định dạng nào trong quá trình xuất? (Chọn hai.)
A. DER
B. PEM
C. PFX
D. CER
E. P12
F.P7B
27. Kỹ thuật bảo mật nào liên kết máy chủ với khóa công khai liên quan của nó?
A. CRL
B. OSCP
C. Ghim chứng chỉ
D. FQDN

CHƯƠNG 14

1. Điều gì có thể được thực hiện cục bộ để bảo mật các thiết bị chuyển mạch và bộ định tuyến? (Chọn hai.)
A. Khóa cáp.
B. Sử dụng SSH thay vì Telnet.
C. Đặt mật khẩu cổng giao diện điều khiển.
D. Vô hiệu hóa các cổng không sử dụng.
4. Trong trường hợp vi phạm an ninh vật lý, bạn có thể làm gì để bảo mật dữ liệu trong phòng máy chủ của mình? (Chọn số ba.)
A. Lắp đặt bộ lưu điện.
B. Sử dụng TPM.
C. Ngăn chặn khởi động từ các thiết bị loại bỏ.
D. Khóa khung máy chủ.
6. Làm thế nào nhân viên bảo vệ có thể xác minh xem ai đó có được phép truy cập một cơ sở không? (Chọn hai.**)**

A. Huy hiệu ID nhân viên
B. Tên đăng nhập và mật khẩu
C. Danh sách truy cập
D. Thẻ thông minh
7. Điều nào sau đây là bước đầu tiên trong việc ngăn chặn các vi phạm an ninh vật lý?
A. Tường lửa
B. ID
C. Hàng rào chu vi và cổng
D. Khóa bàn phím cửa
9. Những lợi thế nào để nhân viên bảo vệ con người có được trên các hệ thống giám sát camera video? (Chọn hai.)
A. Nhân viên bảo vệ con người có bộ nhớ chi tiết hơn giám sát video đã lưu.
B. Nhân viên bảo vệ con người có thể nhận thấy tình huống bất thường.
C. Nhân viên bảo vệ con người có thể phát hiện mùi.
D. Nhân viên bảo vệ con người có thể nhớ lại âm thanh chính xác hơn so với giám sát video đã lưu.
10. Giám đốc CNTT của trung tâm dữ liệu yêu cầu khả năng phân tích các vi phạm an ninh vật lý của cơ sở sau khi họ có xảy ra. Điều nào sau đây trình bày các giải pháp tốt nhất? (Chọn hai.)
A. Nhật ký cảm biến chuyển động
B. Hệ thống an ninh laser
C. Thần **chú**
D. Hệ thống giám sát video phần mềm
12. Bạn muốn giảm thiểu sự gián đoạn đối với cơ sở hạ tầng CNTT của mình. Môi trường nào sau đây yếu tố bạn nên theo dõi? (Chọn ba**.)**
A. Luồng khí
B. Sao lưu băng
C. Máy chủ mã hóa ổ cứng
D. Độ ẩm
E. Sức mạnh
13. Công ty của bạn đã chuyển đến một địa điểm mới, nơi một phòng máy chủ đang được xây dựng. Phòng máy chủ hiện có hệ thống phun nước trong trường hợp hỏa hoạn. Liên quan đến việc dập lửa, bạn nên làm gì đề nghị?
A. Giữ hệ thống phun nước hiện có.
B. Mua một hệ thống chữa cháy không khói nước phát hiện khói.
C. Giữ hệ thống phun nước hiện có và lắp đặt sàn nâng.
D. Đặt bình chữa cháy trong phòng máy chủ
14. Quản trị viên trung tâm dữ liệu sử dụng hình ảnh nhiệt để xác định các điểm nóng trong một trung tâm dữ liệu lớn. Cô ấy rồi sắp xếp các hàng máy chủ được gắn trên giá sao cho không khí mát được dẫn đến cửa vào của máy chủ và không khí nóng là Kiệt sức ra khỏi tòa nhà. Điều khoản nào sau đây xác định đúng nhất kịch bản này?
A. HVAC
B. Hình thức bao thanh toán
C. Lối đi nóng và lạnh
D. Trung tâm dữ liệu thở

15. Phương pháp kiểm soát truy cập nào ghi nhật ký điện tử vào một cơ sở?
A. Chứng minh thư
B. Bảo vệ và sổ nhật ký
C. IPSec
D. Thẻ gần
16. Bạn đã được giao nhiệm vụ giám sát việc xây dựng phòng máy chủ mới của công ty bạn. Các nhà thầu đã cung cấp cho bạn các kế hoạch bao gồm các chi tiết sau đây. Mục nào nên được thêm inve stigated để có khả năng tối đa hóa an ninh phòng máy chủ? Chủ đề: Xây dựng phòng máy chủ mới Chào Glen Tuần của bạn ở Defcon ở Vegas thế nào? Nhà thầu của chúng tôi đã cung cấp các chi tiết sau đây về cấu hình và cấu hình phòng máy chủ. Nếu bạn đồng ý, bạn có thể vui lòng đăng nhập và trả lại cho tôi không? Dân
A. Khóa mật mã cho cửa phòng máy chủ
B. Hoàn thiện sàn chống tĩnh
C. Sàn nâng với phân phối không khí dưới sàn
D. Loại bỏ các cửa sổ duy nhất được bao phủ bởi tường
E. Điện thoại IP gắn tường
F. Bảo tồn trần thả
G. UPS
H. Kiểm soát môi trường phòng máy chủ
I. Cửa phòng máy chủ tám chân
17. Một tòa nhà phòng thí nghiệm nghiên cứu dược phẩm tuyệt mật sử dụng hệ thống cáp mạng CAT 6. Công ty không yêu cầu gián đoạn hoặc chặn truyền phát Bluetooth, mạng hoặc màn hình video. Gì Công ty có nên cân nhắc?
A. Mạng không dây với WPA2 Enterprise
B. EMI che chắn cho tòa nhà
C. Cáp quang
D. IPSec

19. Trong tháng qua, các máy chủ đã ngừng hoạt động một cách bí ẩn mà không có lý do rõ ràng. Máy chủ khởi động lại bình thường chỉ để tắt một lần nữa cuối cùng. Máy chủ được vá đầy đủ, và máy quét vi-rút lên đến nay. Điều nào sau đây là lý do có khả năng nhất cho những thất bại này?
A. Nhiệt độ phòng máy chủ quá nóng.
B. Nhiệt độ phòng máy chủ quá mát.
C. Các máy chủ bị nhiễm virus.
D. Các máy chủ có lỗi hệ điều hành.
20. Nên làm gì trong bãi đỗ xe của cơ sở để đảm bảo an toàn cho nhân viên?
A. Cài đặt một chướng ngại vật.
B. Lắp đặt ánh sáng thích hợp.
C. Cài đặt một dấu hiệu thoát.
D. Lắp đặt bộ sơ cứu.
21. Phát biểu nào sau đây liên quan đến mạng có dây là đúng? (Chọn hai.)
A. Chúng chậm hơn mạng không dây.

B. Chúng nhanh hơn mạng không dây.
C. Chạy cáp nên được cài đặt trong ống dẫn.
D. Chạy cáp phải được tiếp xúc để tạo điều kiện xử lý sự cố.
22. Bạn đang xem xét các tùy chọn để bảo vệ các cửa sổ trong cơ sở của bạn. Điều nào sau đây bạn có thể xem xét?
A. WPA
B. PDS
C. Cảm biến mạch kín
D. Huy hiệu ID
E. Camera quan sát

Chương 15

Câu 1 Bạn đang tiến hành phân tích rủi ro cho một công ty môi giới chứng khoán ở Miami, Florida. Những yếu tố bạn nên xem xét? (Chọn hai.)
A. Thời gian ngừng hoạt động của máy chủ do động đất
B. Phá hủy các tài liệu quy định của chính phủ vì hỏa hoạn
C. Thời gian ngừng hoạt động của máy chủ vì mất điện
D. Dữ liệu hóa đơn của khách hàng bị phá hủy vì hỏa hoạn

Câu 2: Bạn chịu trách nhiệm hoàn thành báo cáo vật sở hửu CNTT cho công ty của bạn. Thiết bị và dữ liệu liên quan đến AllIT phải được xác định và đưa ra một giá trị. Thuật ngữ nào mô tả đúng nhất những gì bạn phải làm tiếp theo?
A. Nhận dạng tài sản
B. Đánh giá rủi ro
C. Giảm thiểu rủi ro
D. Phân tích mối đe dọa

Câu 5: Một khách hàng truyền đạt mối quan tâm của cô ấy với bạn về người dùng Internet độc hại có quyền truy cập vào tài nguyên công ty. Loại đánh giá nào bạn sẽ thực hiện để xác định khả năng này?
A. Đánh giá mối đe dọa
B. Phân tích rủi ro
C. Nhận dạng tài sản
D. Tổng chi phí sở hữu

Câu 8: Khi xác định cách tốt nhất để giảm thiểu rủi ro, bạn nên cân nhắc những mặt hàng nào? (Chọn hai.)
A. Bảo hiểm
B. Số lượng đĩa cứng máy chủ
C. CPU trong máy tính mới sẽ nhanh như thế nào
D. Băng thông mạng

Câu 9: Bạn đang liệt kê các biện pháp phòng ngừa cho tiềm năng. Phát biểu nào sau đây bạn sẽ tài liệu giúp bạn (Chọn ba.)
A. Màn hình phẳng lớn hơn
B. Sao lưu dữ liệu
C. Đào tạo nhân viên

D. So sánh độ tin cậy của các thiết bị cân bằng tải mạng

Câu 10: Một công ty bảo hiểm tính thêm 200 đô la phí bảo hiểm hàng tháng cho bảo hiểm thiên tai cho trang web doanh nghiệp của bạn. Con số nào bạn phải so sánh với điều này để xác định xem có nên chấp nhận bảo hiểm bổ sung này không?

A. ALE

B. ROI

C. Tổng chi phí sở hữu

D. Tổng phí bảo hiểm hàng tháng

Câu 11: 11. Điều nào sau đây là đúng khi phân tích rủi ro định tính?

A. Chỉ xem xét dữ liệu số.

B. ALE phải được tính toán.

C. Các mối đe dọa phải được xác định.

D. ROI phải được tính toán.

Câu 12. Những giá trị nào phải được tính toán để rút ra kỳ vọng tổn thất hàng năm? (Chọn hai.)

A. Kỳ vọng mất mát duy nhất

B. Hàng năm xảy ra

C. Kỳ vọng mất hàng tháng

D. Kỳ vọng mất hàng quý

Câu 13. Bạn là chuyên gia máy chủ cho một công ty điện toán đám mây có tên Cloud Nine Computing. Quản lý sẽ muốn dành quỹ để đáp ứng với rủi ro ngừng hoạt động của máy chủ. Sử dụng dữ liệu lịch sử, bạn xác định rằng xác suất ngừng hoạt động của máy chủ là 17%. Dữ liệu trong quá khứ cho thấy máy chủ sẽ ngừng hoạt động trung bình trong một giờ và có thể kiếm được 3000 đô la doanh thu trong một giờ. Bạn phải tính toán tuổi thọ hàng năm (ALE). Chọn ALE chính xác.

A. $ 300

B. $ 510

C. $ 3000

D. 36.000 đô la

Câu 14. Sếp của bạn yêu cầu bạn tính toán công ty mất bao nhiêu tiền khi các nhân viên quan trọng yêu cầu nhân viên nghỉ việc trong hai giờ. Bạn đã xác định rằng xác suất của điều này xảy ra là 70 phần trăm. Công ty có 25 nhân viên, mỗi người kiếm được 18,50 đô la mỗi giờ. Chọn giá trị chính xác.

A. 12,95 đô la

B. $ 18,50

C. $ 647,50

D. $ 3885

Câu 15: Công ty của bạn đang xem xét việc có máy chủ e-mail được lưu trữ bởi Hosted Solutions, Inc., để giảm chi phí kỹ thuật viên phần cứng và máy chủ tại địa phương. Loại tài liệu chính thức nêu rõ độ tin cậy và truy đòi nếu độ tin cậy không được đáp ứng?

A. BPA

B. MOU

C. SLA

D. ISA

Câu 16. Thuật ngữ nào mô tả đúng nhất các khoản tiền dành để giảm thiểu tác động mà các mối đe dọa và điều kiện không thuận lợi có kinh doanh không?

A. Quản lý rủi ro

B. Kiểm toán bảo mật

C. Hạn chế về ngân sách

D. Phân tích tác động

Câu 17. Phương pháp phân tích rủi ro nào sử dụng ALE?

A. Kết quả tốt nhất có thể

B. Định lượng

C. ROI

D. Định tính

Câu 18: Bạn đang trình bày dữ liệu tại một cuộc họp phân tích rủi ro. Trong bài thuyết trình của bạn, bạn sẽ hiển thị một danh sách các giá trị ALE được xếp hạng theo số tiền. Bob, một người tham gia cuộc họp, hỏi số lượng đáng tin cậy được sử dụng để tính ALE là. Bạn có thể nói gì vớiBob?

A. Các con số đáng tin cậy 100 phần trăm.

B. Những con số đáng tin cậy 50 phần trăm.

C. ALE được tính bằng các giá trị xác suất khác nhau.

D. ALE được tính bằng tỷ lệ phần trăm và chính xác.

Câu 19: Điều nào sau đây nên được thực hiện khi tiến hành đánh giá rủi ro định tính? (Chọn hai.)

A. Định giá tài sản

B. ARO

C. SLE

D. Xếp hạng các mối đe dọa tiềm năng

Câu 20: Bạn là nhà phân tích bảo mật CNTT cho Big John ăn Gourmet Food. John John có kế hoạch mở một nhà máy ở Oranjestad, Aruba, vào năm tới. Bạn đang họp với một ủy ban kế hoạch trong tuần tới và phải có đưa ra các câu hỏi để hỏi ủy ban về địa điểm mới để bạn có thể chuẩn bị phân tích rủi ro bài báo cáo. Câu hỏi nào sau đây sẽ là câu hỏi phù hợp nhất? (Chọn hai.)

A. Mùa hè nóng như thế nào?

B. Sức mạnh địa phương đáng tin cậy như thế nào?

C. Những loại bảo mật tiền đề vật lý được đặt ra?

D. Đường cao tốc gần nhất như thế nào?

Câu 22. Điều nào sau đây liên quan đến quản lý rủi ro là đúng?

A. Các quỹ đầu tư vào quản lý rủi ro có thể kiếm được nhiều lợi nhuận hơn nếu có ở nơi khác.

B. ALE chỉ là ước tính và có thể không chính xác.

C. Rủi ro bảo mật CNTT đều được xử lý bởi tường lửa của công ty.

D. Kết quả phân tích rủi ro định tính được thể hiện bằng số tiền.

23. Đối thủ của bạn đang cung cấp một sản phẩm mới được dự đoán sẽ bán tốt. Sau nhiều lần thận trọng, công ty của bạn đã quyết định không cho ra mắt một sản phẩm cạnh tranh vì sự không chắc chắn của thị trường và đầu tư rất lớn cần thiết. Thuật ngữ nào mô tả đúng nhất về quyết định của công ty bạn?

A. Phân tích rủi ro
B. Chuyển giao rủi ro
C. Tránh rủi ro
D. Tránh sản phẩm

25. Gần đây trung tâm dữ liệu của bạn được đặt tại Albuquerque, New Mexico. Vì sự thu hẹp của công ty, thiết bị của trung tâm dữ liệu đã được chuyển đến một văn phòng hiện có ở Santa Fe. Phòng máy chủ ở Santa Fe không được thiết kế để chứa tất cả các máy chủ mới đến từ Albuquerque và nhiệt độ phòng máy chủ rất ấm áp. Bởi vì đây là một giải pháp tạm thời cho đến khi một cơ sở trung tâm dữ liệu mới được xây dựng, ban quản lý đã quyết định không trả tiền cho một hệ thống điều hòa không khí cập nhật. Thuật ngữ nào mô tả đúng nhất kịch bản này?

A. Chuyển giao rủi ro
B. Tránh rủi ro
C. Chấp nhận rủi ro
D. Giảm rủi ro

Câu 26: Yếu tố nào sau đây có thể ảnh hưởng đến chiến lược quản lý rủi ro của bạn?

A. Quy định của chính phủ
B. Chuyển hoạt động sang một tòa nhà mới
C. Việc mua một tường lửa mới hơn
D. Không có điều nào ở trên
E. Tất cả những điều trên

Câu 27: Bạn là thành viên của nhóm dự án CNTT. Nhóm đang thực hiện phân tích rủi ro CNTT và đã xác định các tài sản cũng như các giá trị của chúng cũng như các mối đe dọa và các giải pháp giảm thiểu mối đe dọa. Phải làm gì tiếp theo?

A. Thực hiện phân tích lợi ích chi phí của các giải pháp rủi ro được đề xuất.
B. Tính các giá trị ALE.
C. Quyết định lỗ hổng nào tồn tại.
D. Không còn gì để làm.

Câu 28: Để giảm khả năng thực tập, một tổ chức thực hiện các chính sách để đảm bảo rằng nhiều người chịu trách nhiệm cho một giao dịch tài chính từ đầu đến cuối. Điều nào sau đây mô tả đúng nhất kịch bản này?

A. Xác suất
B. Giải pháp giảm thiểu
C. Phân tích tác động
D. Phân tích mối đe dọa

Câu 29: Sự khác biệt giữa đánh giá rủi ro và quản lý rủi ro là gì?

A. Chúng giống nhau.
B. Đánh giá rủi ro xác định và ưu tiên rủi ro; quản lý rủi ro là quản lý rủi ro để giảm thiểu tác động của họ.
C. Quản lý rủi ro xác định và ưu tiên rủi ro; đánh giá rủi ro là quản lý rủi ro để giảm thiểu tác động của họ.
D. Đánh giá rủi ro xác định các mối đe dọa; quản lý rủi ro kiểm soát những mối đe dọa.

Câu 30: Xác định hai nhược điểm để phân tích rủi ro định lượng so với phân tích rủi ro định tính. (Chọn hai.)

A. Phân tích rủi ro định lượng đòi hỏi phải tính toán phức tạp.

B. Rủi ro không được ưu tiên bởi giá trị tiền tệ.

C. Phân tích định lượng tốn nhiều thời gian hơn phân tích định tính.

D. Rất khó để xác định phân bổ bao nhiêu tiền để giảm rủi ro

D. Quyền truy cập tệp NTFS

Câu 32: Là quản trị viên CNTT, bạn có trách nhiệm tạo tài khoản người dùng cho nhân viên mới được tuyển dụng. Những người tuyển dụng mới phải có ID hình ảnh để có được tài khoản mạng / e-mail và họ phải được cấp thẻ PKI mà họ gán mã PIN. Thuật ngữ nào áp dụng cho quy trình được mô tả?

A. On boarding

B. Off boarding

C. Quyền sở hữu dữ liệu

D. Thêm người dùng

Chương 16

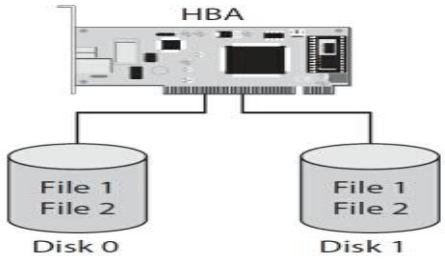
Câu 1. Trong trường hợp máy chủ bị lỗi ổ cứng, bạn đã được yêu cầu định cấu hình đĩa cứng máy chủ như mô tả trong hình 16-1. Đây là loại cấu hình đĩa nào?

A. RAID 0

B. RAID 1

C. RAID 5

D. RAID 5 + 1



Câu 3. Một cơ quan thực thi pháp luật đô thị thuê một không gian mới ở một phần khác của thị trấn, hoàn thành với một mạng máy tính hoạt động phản ánh các trang web trực tiếp hiện tại. Một liên kết mạng tốc độ cao liên tục đồng bộ hóa dữ liệu giữa hai trang web. Loại trang web nào là vị trí thuê mới?

A. trang web sương giá

B. Nơi lạnh

C. Trang web ấm áp

D. Trang web nóng

Câu 4. Một cơ quan thực thi pháp luật đô thị thuê một không gian mới ở một phần khác của thị trấn, hoàn thành với một mạng máy tính hoạt động phản ánh các trang web trực tiếp hiện tại. Sao lưu dữ liệu từ trang web chính là sao chép vào vị trí thuê mới hai ngày một lần. Loại trang web nào là vị trí thuê mới?

A. trang web sương giá

B. Nơi lạnh

C. Trang web ấm áp

D. Trang web nóng

Câu 5. Turtle Airlines đã thuê bạn để đảm bảo rằng hệ thống đặt phòng của khách hàng luôn trực tuyến. Phần mềm chạy và lưu trữ dữ liệu cục bộ trên hệ điều hành Linux. Những gì bạn nên làm?

A. Cài đặt hai máy chủ Linux trong một cụm. Phân cụm phần mềm hàng không, với dữ liệu được ghi vào lưu trữ chia sẻ.

B. Cài đặt máy chủ Linux mới. Đảm bảo rằng phần mềm hàng không chạy từ máy chủ đầu tiên. Lịch trình hãng hàng không
dữ liệu để sao chép vào máy chủ Linux mới hàng đêm.

C. Cấu hình máy chủ Linux với RAID 5.

D. Cấu hình máy chủ Linux với RAID 1.

Câu 8. Thói quen sao lưu máy chủ của bạn bao gồm sao lưu toàn bộ vào mỗi tối thứ Sáu và sao lưu hàng đêm tất cả dữ liệu đã thay đổi kể từ thứ sáu sao lưu. Loại lịch trình sao lưu này là gì?

A. Đầy đủ

B. Đầy đủ và gia tăng

C. Đầy đủ và khác biệt

D. Gia tăng hoàn toàn

Câu 9. Giám đốc an ninh tại một chuỗi ngân hàng quốc gia sẽ nghỉ hưu vào năm tới và một nhân viên an ninh CNTT phải được chải chuốt để lấp đầy vị trí đó. Thuật ngữ nào bao gồm thủ tục này?

A. Nghỉ hưu

B. Luân chuyển công việc

C. Kế hoạch kế nhiệm

D. Phục hồi thảm họa

Câu 10. Bạn là kỹ sư mạng cho một công ty luật ở San Francisco. Sau trận động đất năm 1989, một sự nhấn mạnh vào tiếp tục hoạt động kinh doanh sau khi các trận động đất trong tương lai thống trị trong kinh doanh San Francisco cộng đồng. Loại kế hoạch nào tập trung vào việc đảm bảo rằng nhân sự, khách hàng và hệ thống CNTT ảnh hưởng tối thiểu sau thảm họa?

A. Quản lý rủi ro

B. Chịu lỗi

C. Phục hồi thảm họa

D. Liên tục kinh doanh

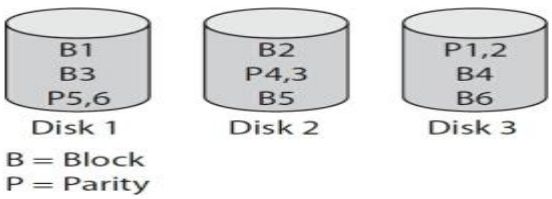
Câu 11 Một máy chủ được cấu hình với ba đĩa cứng theo Hình 16-2. Đây là loại cấu hình gì?

A. RAID 0

B. RAID 1

C. RAID 5

D. RAID 5 + 1



Câu 12. Sao lưu Windows Server 2012 được lên lịch như sau: sao lưu toàn bộ vào Thứ Bảy lúc 3 giờ sáng và sao lưu gia tăng số tuần vào lúc 9 giờ Viết xác minh đã được kích hoạt. Băng dự phòng được lưu trữ ngoại vi tại một địa điểm của bên thứ ba. Nên làm gì để đảm bảo tính toàn vẹn và bảo mật của Sao lưu? (Chọn hai.)

A. Có một người khác với nhà điều hành sao lưu phân tích nhật ký sao lưu dữ liệu mỗi ngày.

B. Đảm bảo người dùng thực hiện sao lưu là thành viên của nhóm Quản trị viên.

C. Mã hóa phương tiện sao lưu.

D. Sử dụng SSL để mã hóa phương tiện sao lưu.

Câu 14. Những mặt hàng nào cần được xem xét khi đảm bảo tính sẵn sàng cao cho một trang web thương mại điện tử? (Chọn hai.)

A. Sử dụng TPM để mã hóa ổ cứng máy chủ

B. Sử dụng các liên kết Internet dư thừa

C. Cân bằng tải mạng

D. Nâng cấp CMOS máy chủ lên phiên bản mới nhất

Câu 15. Điều nào sau đây cần được xem xét khi tạo một kế hoạch khắc phục thảm họa? (Chọn ba.)

A. Xác định loại địa chỉ IP nào đang được sử dụng.

B. Xếp hạng rủi ro.

C. Vô hiệu hóa các cổng chuyển đổi không sử dụng.

D. Phân công nhiệm vụ phục hồi cho nhân sự.

E. Thiết lập một địa điểm thay thế để tiếp tục hoạt động kinh doanh.

Câu 18. Xác định các lỗi kế hoạch khắc phục thảm họa. (Chọn hai.)

A. Thực hiện phân tích tác động kinh doanh trước.

B. Dựa vào DRP của bạn trên một mẫu đã tải xuống.

C. Sao lưu dữ liệu không bao giờ được kiểm tra; nó làm cho công ty tốn quá nhiều tiền

D. Giữ các giải pháp sao lưu hiện có ngay cả khi phần mềm đã hết hai phiên bản.

Câu 19. Bạn đang tạo DRP cho một đại lý xe hơi nhỏ, độc lập. Có bốn nhân viên mỗi người sử dụng Cửa sổ máy tính; không có máy chủ Tất cả dữ liệu của công ty được lưu trữ trên bốn máy tính. Một đơn DSLlink tốc độ cao được chia sẻ bởi tất cả người dùng. Các giải pháp DRP tốt nhất là gì? (Chọn hai.)

A. Lưu trữ dữ liệu với một dịch vụ lưu trữ dữ liệu trực tuyến.

B. Đảm bảo nhân viên biết chính xác phải làm gì trong trường hợp xảy ra thảm họa.

C. Mua máy tính để bàn nhanh hơn.

D. Mua một máy chủ tập tin.

Câu 21. Bạn đang làm việc với ban quản lý để biện minh cho chi phí của một trang web ấm áp so với một trang web lạnh. Những yếu tố có thể giúp biện minh cho chi phí của một trang web ấm áp? (Chọn hai.)

A. Mất doanh thu lớn trong thời gian ngừng hoạt động ngắn

B. Mất mát nhỏ trong thời gian dài

C. Hợp đồng của khách hàng chịu đựng không quá 8 giờ ngừng hoạt động

D. Hợp đồng của khách hàng chịu đựng không quá 72 giờ ngừng hoạt động

Câu 22. Quản trị viên mạng cấp cao của bạn đã quyết định rằng năm máy chủ vật lý tại địa điểm của bạn sẽ là ảo hóa và chạy trên một máy chủ vật lý duy nhất. Năm khách ảo sẽ sử dụng các đĩa cứng vật lý trong máy chủ vật lý. Máy chủ vật lý có các đĩa cứng được cấu hình với RAID 1. Xác định lỗ hổng trong kế hoạch này.

A. Máy chủ vật lý nên sử dụng RAID 5.
B. Các đĩa cứng vật lý không được nằm trong máy chủ vật lý.
C. Bạn không thể chạy năm máy ảo trên máy chủ vật lý cùng một lúc.
D. Vật chủ là một điểm thất bại duy nhất.

Câu 25. Bạn là quản trị viên cho Máy chủ Windows 2012 ảo chạy Dịch vụ miền Active Directory (AD DS). Hành vi của Abnormalserver và cuối cùng là máy chủ đóng băng khiến bạn tin rằng máy chủ có nhiễm virus. Những gì bạn nên làm?

A. Hoàn nguyên về ảnh chụp nhanh của máy ảo trước khi bị nhiễm vi-rút.
B. Định dạng đĩa cứng, cài đặt lại máy chủ và khôi phục từ băng.
C. Tham khảo DRP của bạn.
D. Tham khảo ARP của bạn.

Câu 26. Mục đích của kế hoạch khắc phục thảm họa là gì? (Chọn hai.)

A. Để giảm thiểu thiệt hại kinh tế
B. Có phản ứng trước với những sai lầm ngớ ngẩn trong quan hệ công chúng
C. Để đặt niềm tin vào cổ đông
D. Để kiếm được tỷ lệ lợi nhuận cao hàng năm

Câu 27. Điều nào sau đây sẽ xuất hiện trên DRP?

A. Danh sách ưu tiên của các hệ thống máy tính quan trọng
B. Điểm đơn thất bại
C. Ngày sinh của nhân viên
D. Giá trị đồng đô la liên quan đến một giờ ngừng hoạt động

Câu 28. Bạn là quản trị viên mạng cho một công ty tư vấn smallIT. Allservers được đặt tại trang web duy nhất. Sau khi kiểm tra DRP và nhận được phê duyệt quản lý, bạn gửi e-mail một bản sao cho tất cả nhân viên cho họ tài liệu tham khảo trong trường hợp thảm họa. Xác định vấn đề.

A. Các e-mailshould đã được mã hóa.
B. Thư điện tử đã được ký điện tử.
C. Chỉ có giám đốc điều hành nên đã nhận được tin nhắn.
D. Máy chủ thư có thể không khả dụng trong trường hợp xảy ra thảm họa.

Câu 29. Bạn là quản trị viên mạng cho một công ty tư vấn smallIT. Allservers được lưu trữ bên ngoài. Sau phân tích các mối đe dọa, tạo DRP và nhận phê duyệt quản lý, bạn gửi e-mail một bản sao cho tất cả nhân viên để họ tham khảo trong trường hợp thảm họa. Xác định vấn đề.

A. Các e-mailshould đã được mã hóa.
B. DRP không được thử nghiệm.
C. Các e-mailshould đã được ký điện tử.
D. Chỉ có giám đốc điều hành nên đã nhận được tin nhắn.

Câu 30. Điều nào sau đây liên quan đến khắc phục thảm họa là đúng? (Chọn hai.)

A. Một khi kế hoạch hoàn thành, nó không bao giờ cần phải xem lại.
B. Sau khi kế hoạch hoàn thành, nó phải có sự phê duyệt của ban quản lý.
C. Kế hoạch không bao giờ hoàn thành; nó phải phát triển với doanh nghiệp.
D. Kế hoạch chỉ nên bao gồm các hệ thống CNTT.

Câu 32. Bạn là một quản trị viên trang web. Bạn cần giảm thiểu thời gian ngừng hoạt động của trang web trong trường hợp xảy ra thảm họa hoặc
thỏa hiệp an ninh. Điều khoản nào sau đây mô tả đúng nhất độ tin cậy của đĩa cứng?
A. MTBF
B. MTTF
C. MTTR
D. RPO
Câu 34. Laurel là người đứng đầu an ninh CNTT cho một bộ phận chính phủ. Vi phạm an ninh lặp đi lặp lại gần đây liên quan đến phần mềm độc hại trên phương tiện di động khiến cô lo ngại về các sự cố trong tương lai, vì vậy cô đánh giá phản ứng sự cố trong quá khứ để xác định cách thức xảy ra như vậy có thể được ngăn chặn và cách phản ứng có thể được được cải thiện. Vòng nguyệt quế nên chuẩn bị loại tài liệu nào?
A. Báo cáo sau hành động
B. MOU
C. SLA
D. Người đánh giá rủi ro

Chương 17

Câu 2. Sau khi thu giữ thiết bị máy tính được cho là có liên quan đến tội phạm, nó được đặt trong hành lang không giám sát trong mười phút trong khi các sĩ quan khuất phục một nghi phạm bạo lực. Các thiết bị bị tịch thu không còn Chấp nhận làm bằng chứng vì vi phạm gì?
A. Thứ tự biến động
B. Kiểm soát thiệt hại
C. Chuỗi hành trình sản phẩm
D. Thời gian bù
Câu 3. Lệnh đã được ban hành để điều tra một máy chủ được cho là sử dụng bởi tội phạm có tổ chức để hoán đổi tín dụng thẻ thông tin. Theo thứ tự biến động, bạn nên thu thập dữ liệu nào trước?
A. Bộ nhớ điện tử (RAM)
B. Đĩa cứng
C. Ổ đĩa flash USB
D. CMOS
Câu 4. Một máy chủ được cấu hình với mảng RAID 5 phải được tạo ảnh đúng cách để giữ nguyên bản gốc của dữ liệu. Bạn quyết định chống lại hình ảnh mỗi đĩa cứng vật lý trong mảng. Bạn phải thực hiện hai nhiệm vụ nào biểu diễn?
(Chọn hai.)
A. Thay đổi thứ tự khởi động CMOS của máy chủ.
B. Hình ảnh mảng như một đĩa logic đơn.
C. Đảm bảo rằng giải pháp hình ảnh của bạn hỗ trợ RAID.
D. Cập nhật chương trình cơ sở cho bộ điều khiển RAID.
Câu 5. Trong khi chụp lưu lượng mạng, bạn nhận thấy số lượng gói tin gửi đi quá mức bất thường. Để xác định xem đây có phải là sự cố yêu cầu leo thang hoặc báo cáo hay không, bạn nên làm gì khác
hỏi ý kiến?

A. Nội dung hộp thư đến của bạn
B. Nhật ký máy chủ
C. Tài liệu mailserver
D. Nhật ký máy chủ web

Câu 6. Bạn quyết định làm việc muộn vào tối thứ bảy để thay thế hệ thống dây điện trong phòng máy chủ của bạn. Khi đến nơi, bạn nhận ra đã có một đột nhập và băng dự phòng máy chủ dường như bị thiếu. Bạn nên làm gì cán bộ thực thi pháp luật đến nơi?

A. Dọn dẹp phòng máy chủ.
B. Phác thảo một hình ảnh của các cơ sở đột nhập vào một notepad.
C. Cảnh báo các quan chức rằng tiền đề có video giám sát.
D. Kiểm tra khu vực xung quanh để tìm hung thủ.

Câu 8. Chọn thứ tự biến động chính xác khi thu thập bằng chứng kỹ thuật số:

A. Đĩa cứng, DVD-R, RAM, tập tin hoán đổi
B. Hoán đổi tập tin, RAM, DVD-R, đĩa cứng
C. RAM, DVD-R, tập tin trao đổi, đĩa cứng
D. RAM, tập tin trao đổi, đĩa cứng, DVD-R

Câu 9. Nhà phân tích pháp y có thể làm gì để giảm số lượng tệp phải phân tích trên đĩa bị tịch thu?

A. Viết một kịch bản VisualBasic.
B. Xóa các tệp được cho là tệp hệ điều hành.
C. Đảm bảo rằng đĩa gốc còn nguyên sơ và sử dụng bảng băm trên bản sao của các tệp.
D. Đảm bảo rằng đĩa gốc còn nguyên sơ và sử dụng tập lệnh để xử lý bản sao của tệp.

Câu 10. Một chuyên gia có mặt tại thời điểm thu thập chứng cứ có thể được triệu tập để xuất hiện tại tòa án hoặc chuẩn bị một báo cáo về những phát hiện của cô để sử dụng tại tòa án. Người này gọi là gì?

A. Nguyên đơn
B. Bị cáo
C. Kiểm toán viên
D. Nhân chứng pháp y

Câu 11. Điều nào sau đây mô tả đúng nhất về chuỗi hành trình sản phẩm?

A. Ủy thác thu thập chứng cứ cho cấp trên của bạn
B. Bảo quản, bảo vệ và ghi chép bằng chứng
C. Chụp ảnh hệ thống sang đĩa khác
D. Chụp nội dung bộ nhớ trước nội dung đĩa cứng

Câu 12. Trong khi làm việc với một trường hợp giao dịch nội gián, bạn được yêu cầu chứng minh rằng một thông điệp email là xác thực và đã được gửi cho một nhân viên khác. Những mặt hàng bạn nên xem xét? (Chọn hai.)

A. Tin nhắn có được mã hóa không?
B. Tin nhắn có được ký điện tử không?
C. Khóa công khai của người dùng có được bảo vệ đúng cách không?
D. Khóa riêng của người dùng có được bảo vệ đúng cách không?

Câu 14. Mục đích của phần mềm pháp y đĩa là gì? (Chọn hai.)

A. Sử dụng mã hóa tập tin để đảm bảo dữ liệu sao chép dữ liệu gốc
B. Sử dụng băm tập tin để đảm bảo dữ liệu sao chép dữ liệu gốc
C. Bảo vệ dữ liệu trên các đĩa gốc
D. Tạo băm tập tin trên các đĩa gốc

Câu 15. Bạn đang chuẩn bị thu thập bằng chứng từ một chiếc điện thoại di động. Điều nào sau đây là sai?

A. Thiết bị CDMAmobile không sử dụng thẻ SIM.
B. Điện thoại CDMA lưu trữ dữ liệu người dùng trực tiếp trên thiết bị di động.
C. Thiết bị di động GSM không sử dụng thẻ SIM.
D. Thiết bị di động GSM sử dụng thẻ SIM.

Câu 16. Bạn phải phân tích dữ liệu trên bộ nhớ trong của máy ảnh kỹ thuật số. Bạn có kế hoạch kết nối máy tính pháp y của bạn đến máy ảnh bằng cáp USB. Bạn nên làm gì để đảm bảo bạn không sửa đổi dữ liệu trên máy ảnh?

A. Đảm bảo máy ảnh đã tắt.
B. Đánh dấu tất cả các tệp trên máy ảnh ở chế độ chỉ đọc.
C. Đăng nhập bằng tài khoản không phải quản trị viên trên máy tính pháp y.
D. Sử dụng thiết bị chặn ghi USB.

Câu 18. Robin làm việc như một kỹ thuật viên mạng tại một công ty môi giới chứng khoán. Để kiểm tra việc bắt giữ pháp y mạng Phần mềm, cô cắm máy tính xách tay của mình vào một bộ chuyển mạch Ethernet và bắt đầu nắm bắt lưu lượng mạng. Trong thời gian sauphân tích, cô nhận thấy một số gói tin quảng bá và phát đa hướng cũng như mạng máy tính của riêng mình giao thông. Tại sao cô ấy không thể nắm bắt tất cả lưu lượng truy cập mạng trên thiết bị chuyển mạch?

A. Cô ấy phải kích hoạt chế độ lăng nhăng trên NIC của mình.
B. Cô ấy phải vô hiệu hóa chế độ lăng nhăng trên NIC của mình.
C. Mỗi cổng chuyển đổi là một miền va chạm bị cô lập.
D. Mỗi cổng chuyển đổi là một miền phát sóng bị cô lập.

Câu 19. Thiết bị phát hiện xâm nhập mạng chiếm được lưu lượng truy cập mạng trong khi thực hiện tội phạm trên mạng. Bạn nhận thấy các gói NTP và TCP từ tất cả các máy chủ mạng trong bản chụp. Bạn phải tìm cách để tương quan các gói bị bắt với ngày và thời gian để đảm bảo việc bắt gói sẽ được xem xét chấp nhận làm bằng chứng. Những gì bạn nên làm? (Chọn hai.)

A. Không có gì. NTP giữ thời gian đồng bộ hóa trên mạng.
B. Không có gì. Chụp gói được đóng dấu thời gian.
C. Không có chữ số, ngày và giờ không thể được xác thực.
D. Không có mã hóa, ngày và giờ không thể được xác thực.

Câu 21. Bạn được yêu cầu kiểm tra một đĩa cứng để tìm các đoạn hội thoại nhắn tin tức thời cũng như bị xóa các tập tin. Làm thế nào bạn nên làm điều này?

A. Sử dụng các công cụ sao chép dòng bit.
B. Đăng nhập vào máy tính và sao chép nội dung ổ cứng ban đầu sang ổ cứng USB ngoài.
C. Ánh xạ một ổ đĩa qua mạng vào ổ cứng ban đầu và sao chép nội dung vào USB bên ngoài
ổ cứng.
D. Xem tệp nhật ký.

Câu 22. Loại tệp nào có khả năng chứa dữ liệu liên quan nhất?
A. Tệp Microsoft Word được bảo vệ bằng mật khẩu
B. Tệp Microsoft Word được mã hóa
C. Tệp Microsoft Word được ký điện tử
D. Tệp băm của tệp Microsoft Word
Câu 23. Làm thế nào một nhà phân tích pháp y có thể hưởng lợi từ việc phân tích siêu dữ liệu? (Chọn ba.)
A. Siêu dữ liệu JPEG có thể tiết lộ các cài đặt máy ảnh cụ thể.
B. Siêu dữ liệu Microsoft Word có thể tiết lộ tên tác giả.
C. Siêu dữ liệu Microsoft Excel có thể tiết lộ địa chỉ MAC của bạn.
D. Siêu dữ liệu PDF có thể tiết lộ tên công ty đã đăng ký.
Câu 24. Quy tắc nào sau đây phải được tuân theo khi thực hiện phân tích pháp y? (Chọn hai.)
A. Chỉ làm việc với dữ liệu xác thực ban đầu.
B. Chỉ làm việc với một bản sao của dữ liệu.
C. Tìm kiếm sự cho phép hợp pháp để tiến hành phân tích.
D. Tìm kiếm sự cho phép của người quản lý của bạn để tiến hành phân tích.
Câu 26. Giám đốc CNTT đang tạo ra ngân sách năm sau. Bạn được yêu cầu nộp số liệu pháp y cho nhóm phản ứng sự cố mạng của bạn. Những mặt hàng nào bạn không nên gửi?
A. Chi phí đi lại
B. Chi phí theo giờ
C. Chi phí đào tạo
D. Số tiền ALE
Câu 27. Người dùng báo cáo lúc 9:30 sáng, hiệu suất mạng bị suy giảm nghiêm trọng kể từ ngày làm việc bắt đầu lúc 8 giờ sáng. Sau khi phân tích mạng và thảo luận nhanh với nhóm bảo mật CNTT của bạn, bạn kết luận virus sâu đã lây nhiễm mạng của bạn. Bạn nên làm gì để kiểm soát thiệt hại? (Chọn hai.)
A. Xác định mức độ nghiêm trọng của vi phạm an ninh.
B. Rút phích cắm thiết bị SAN.
C. Tắt tất cả máy chủ.
D. Tắt các công tắc Ethernet.
Câu 28. Một nghi phạm sẽ xóa các tập tin liên quan và làm trống thùng rác Windows. Điều nào sau đây báo cáo là đúng liên quan đến việc xóa? (Chọn hai.)
A. Các tập tin không thể được phục hồi.
B. Các tập tin có thể được phục hồi.
C. Các tệp đã xóa chứa tất cả dữ liệu gốc của chúng cho đến khi đĩa cứng chứa đầy dữ liệu khác.
D. Các tệp đã xóa chứa tất cả dữ liệu gốc của chúng cho đến khi đĩa cứng được phân mảnh.
Câu 29. Cảnh sát địa phương nghi ngờ một phụ nữ đang sử dụng máy tính của mình để thực hiện hành vi lừa đảo trực tuyến, nhưng cô ta mã hóa đĩa cứng với cụm mật khẩu mạnh. Thực thi pháp luật muốn truy cập dữ liệu trên mã hóa đĩa để lấy bằng chứng pháp y. Những nhiệm vụ nên được thực hiện? (Chọn hai.)
A. Khai thác sức mạnh xử lý của hàng ngàn máy tính Internet và cố gắng bẻ khóa
mật khẩu mã hóa.
B. Nhận lệnh.

C. Cài đặt gói sniffer trên mạng nghi ngờ.
D. Cài đặt keylogger để nắm bắt cụm mật khẩu.

Câu 30. Một ổ đĩa flash USB bị thu giữ chỉ chứa hình ảnh tự nhiên. Nhân viên thực thi pháp luật đã bị thuyết phục dữ liệu liên quan đã được lưu trữ trên ổ flash USB. Những gì khác nên được thực hiện?

A. Giải mã ổ flash USB.
B. Định dạng ổ flash USB.
C. Kiểm tra dữ liệu ẩn steganographic.
D. Phân tích nhật ký ổ đĩa flash USB.

Chương 18

Câu 1. Là một phần của kiểm toán bảo mật của bạn, bạn muốn xem loại lưu lượng truy cập mạng nào đang được truyền đi mạng Những loại công cụ bạn nên sử dụng?

A. Phân tích giao thức
B. Máy quét cổng
C. Máy quét lỗ hổng
D. Mật khẩu bẻ khóa

Câu 2. Một mạng gồm 250 máy tính. Bạn phải xác định máy nào an toàn và máy nào không phải. Những loại công cụ bạn nên sử dụng?

A. Phân tích giao thức
B. Máy quét cổng
C. Máy quét lỗ hổng
D. Mật khẩu bẻ khóa

Câu 3. Bạn muốn tập trung và theo dõi hoạt động độc hại đến một máy chủ cụ thể trong DMZ của bạn. Bạn nên làm gì cấu hình?

A. Honeynet
B. Honeypot
C. Trình theo dõi DMZ
D. Máy chủ web

Câu 4. Bạn sẽ sử dụng cách nào sau đây để xác định cổng TCP và UDP nào trên máy chủ đang mở?

A. Máy quét lỗ hổng
B. Gói sniffer
C. Giám sát hiệu suất
D. Máy quét cổng

Câu 5. Quy trình nào xác định tài sản, các mối đe dọa và rủi ro và cũng xác định các phương pháp để giảm thiểu tác động của những mối đe dọa này?

A. Phân tích rủi ro
B. Đánh giá tính dễ bị tổn thương
C. Quét cổng
D. Bản đồ mạng

Câu 6. Một kỹ thuật viên phải xác định độ lệch so với hoạt động mạng bình thường. Nhiệm vụ nào trước tiên cô phải thực hiện?

A. Phân tích xu hướng

B. Phân tích cơ bản

C. Giám sát hiệu suất

D. Phân tích rủi ro

312

Câu 7. Một nhà phát triển phân tích mã nguồn để đảm bảo không có lỗi hoặc rủi ro bảo mật tiềm năng. Thuật ngữ nào xác định tốt nhất hoạt động này?

A. Đánh giá rủi ro

B. Quản lý bản vá

C. Gỡ lỗi

D. Xem lại mã

Câu 8. Máy tính AWindows chưa được vá và các dịch vụ không cần thiết chưa bị vô hiệu hóa. Mà tuyên bố nào sau đây là đúng về bảo mật?

A. Máy tính sẽ hoạt động nhanh hơn.

B. Máy tính có bề mặt tấn công lớn.

C. Máy tính có bề mặt tấn công nhỏ.

D. Máy tính sẽ hoạt động chậm hơn.

Câu 9. Một kiểm toán viên an ninh mạng mô phỏng các cuộc tấn công mạng khác nhau chống lại một mạng công ty. Thuật ngữ nào xác định tốt nhất thủ tục này?

A. Phân tích tính dễ bị tổn thương

B. Ánh xạ mạng

C. Thử nghiệm thâm nhập

D. Đánh giá rủi ro

Câu 10. Người quản lý của bạn yêu cầu bạn định cấu hình bộ sưu tập các máy chủ dễ bị tổn thương trong DMZ cho mục đích này theo dõi các nỗ lực hack. Thuật ngữ nào mô tả đúng nhất những gì bạn đang cấu hình?

A. Honeynet

B. Honeypot

C. Tường lửa

D. Máy chủ proxy

Câu 11. Bạn chạy quét lỗ hổng trên mạng con 192.168.1.0/24. Các kết quả trạng thái cổng TCP 135 đến 139 là mở trên hầu hết các máy chủ. Điều này" nói đến cái gì?

A. Chia sẻ tệp và in

B. Máy chủ web

C. Máy chủ thư

D. Giao thức máy tính từ xa

Câu 12. Bạn là nhà tư vấn mạng phụ trách việc tạo cơ sở hạ tầng mạng không dây cho khách sạn. Hướng tới Kết thúc thực hiện, nhóm của bạn đánh giá dự án để đảm bảo rằng nó đáp ứng được bản gốc yêu cầu. Cái này gọi là gì?

A. Kiểm tra thâm nhập

B. Đánh giá rủi ro

C. Đánh giá thiết kế

D. Xem lại mã

Câu 13. Sau khi kiểm tra nhật ký cẩn thận, bạn nhận ra ai đó đã xâm nhập vào mạng không dây được bảo mật WEP của bạn mạng. Bạn có thể làm gì để bảo mật lưu lượng không dây?

A. Sử dụng doanh nghiệp WPA2.

B. Sử dụng WPA2 PSK.

C. Vô hiệu hóa phát SSID.

D. Thay đổi tên SSID.

Câu 15. Điều nào sau đây được coi là thử nghiệm bảo mật thụ động?

A. Lưu lượng truy cập mạng

B. Tấn công bằng mật khẩu

C. Giải mã đĩa dựa trên từ điển

D. Dấu vân tay hệ điều hành

Câu 16. Từ danh sách sau, xác định cấu hình sai bảo mật:

A. Tài khoản quản trị miền được sử dụng làm tài khoản dịch vụ.

B. Tài khoản Active Directory được sử dụng làm tài khoản dịch vụ.

C. Các trạm Windows nhận được cập nhật từ máy chủ WSUS thay vì Internet.

D. Tài khoản Windows Guest bị vô hiệu hóa.

Câu 17. Một nhóm kiểm toán an ninh đã được thuê để tiến hành các thử nghiệm thâm nhập mạng đối với mạng. Các nhóm đã không được cung cấp bất kỳ dữ liệu liên quan đến mạng hoặc bố trí của nó. Nhóm thử nghiệm sẽ làm gì biểu diễn?

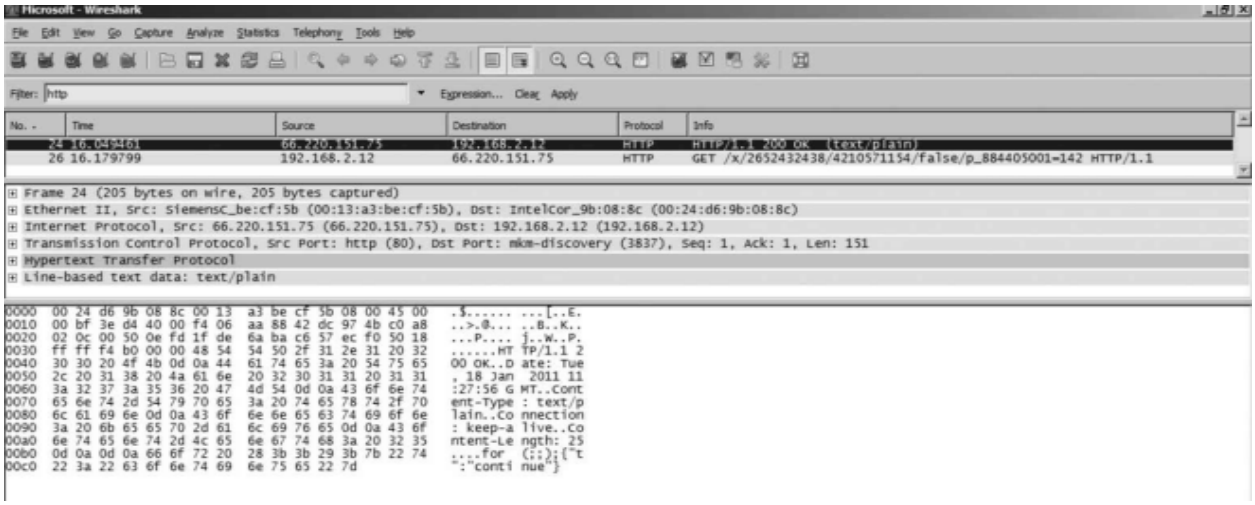
A. Hộp đen

B. Hộp trắng

C. Hộp màu xám

D. Hộp màu xanh

Câu 18. Tham khảo hình 18-1. Khẳng định nào sau đây là đúng? (Chọn hai.)



A. Địa chỉ IP của máy chủ web là 66.220.151,75.

B. Địa chỉ IP của máy chủ web là 192.168.2.12.

C. Trang web không sử dụng SSL.

D. Gói số 24 sẽ vào trang web.

Câu 19. Bạn đang gặp sự cố ping máy chủ 192.168.17.45; không có câu trả lời Một trong những người dùng của bạn phải sử dụng Giao thức máy tính để bàn từ xa (RDP) đối với máy chủ để chạy ứng dụng. Bạn không thể kiểm tra RDP cho người dùng, bởi vì bạn hiện đang đăng nhập cục bộ vào máy chủ Linux chỉ bằng một dòng lệnh. Những gì có thể bạn sử dụng để xác định nhanh chóng liệu RDP có chạy trên 192.168.17.45 không?

A. Gói sniffer

B. Máy quét virus

C. Máy quét không dây

D. Máy quét cổng

Câu 20. Sau khi tiến hành kiểm toán bảo mật, bạn thông báo cho chủ sở hữu mạng rằng bạn đã phát hiện ra hai không được mã hóa mạng không dây. Khách hàng của bạn hỏi làm thế nào tốt nhất để bảo đảm lưu lượng không dây. Điều nào sau đây là mã hóa mạng không dây an toàn nhất?

A. WEP

B. WPA

C. WPA2

D. WPA3

Câu 21. Tham khảo hình 18-2. Kiểm toán bảo mật sẽ tìm thấy lỗi cấu hình nào?

A. Tài khoản Administrator cần được xóa.

B. Tài khoản Administrator được kích hoạt và chưa được đổi tên.

C. Tài khoản Guest được bật.

D. Tài khoản Guest nên bị xóa.

Câu 22. Kiểm toán viên bảo mật phải xác định loại máy chủ nào đang chạy trên mạng. Loại công cụ nào nên được sử dụng?

A. Bản đồ mạng

B. Phân tích giao thức

C. Máy quét cổng

D. Máy quét virus

Câu 23. Một kiểm toán viên an ninh phát hiện ra các mạng không dây mở. Cô phải đề xuất một giải pháp an toàn. Mà

Sau đây là giải pháp không dây an toàn nhất?

A. 802.1x

B. WEP

C. PSK WPA

D. Vô hiệu hóa phát SSID

Câu 24. Điều nào sau đây sẽ không được xem xét trong quá trình kiểm toán bảo mật?

A. Phòng máy chủ bị khóa

B. Mã hóa không dây đang sử dụng

C. Trạng thái bản vá của tất cả máy chủ

D. Giá giấy phép máy chủ

Câu 25. Trong khi kiểm tra môi trường Windows Active Directory, bạn phát hiện ra rằng các tài khoản quản trị làm chưa có cấu hình chính sách khóa tài khoản. Điều nào sau đây là mối quan tâm bảo mật? (Chọn hai.)

A. Nếu khóa tài khoản được bật, tài khoản quản trị có thể bị khóa do lặp lại mật khẩu thử.

B. Nếu khóa tài khoản không được bật, tài khoản quản trị có thể bị tấn công bằng mật khẩu.

C. Nếu khóa tài khoản được bật, tài khoản quản trị có thể bị tấn công bằng mật khẩu.

D. Nếu khóa tài khoản không được bật, tài khoản quản trị có thể bị khóa do kết quả của nhiều lần thử mật khẩu.

Câu 26. Loại kiểm tra bảo mật nào cung cấp thông tin cấu hình mạng cho người kiểm tra?

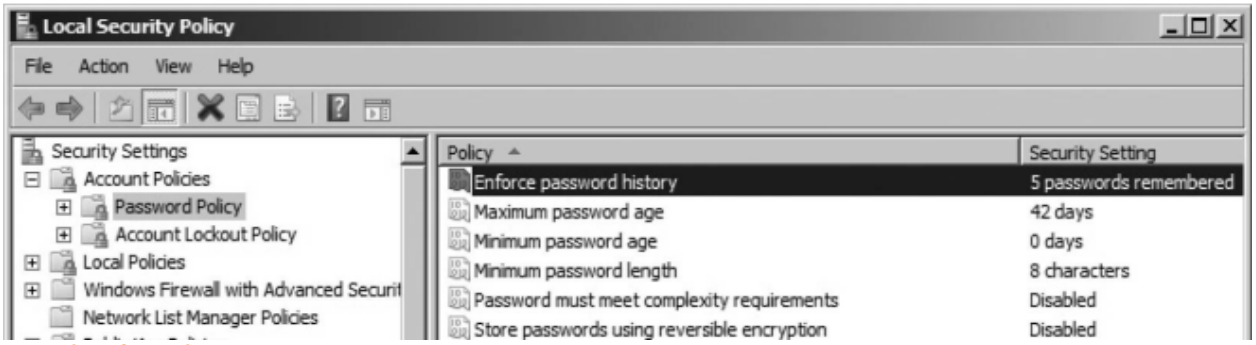
A. Hộp trắng

B. Hộp đen

C. Hộp màu xám

D. Hộp màu xanh

Câu 27. Bạn đang xem xét các chính sách mật khẩu trong quá trình kiểm toán bảo mật. Tham khảo hình 18-3 và xác định hai vấn đề an ninh. (Chọn hai.)



A. Tuổi mật khẩu tối thiểu là 0 ngày.

B. Lịch sử mật khẩu được đặt thành chỉ 5.

C. Mật khẩu lưu trữ sử dụng tùy chọn mã hóa đảo ngược bị vô hiệu hóa.

D. Mật khẩu không đáp ứng yêu cầu phức tạp.

Câu 28. Loại công cụ nào cho các mối đe dọa bảo mật đã biết trên một nhóm máy tính?

A. Gói sniffer

B. Máy quét lỗ hổng

C. Máy quét rủi ro

D. Máy quét cổng

Câu 29. Bạn muốn một máy chủ không sử dụng đăng nhập hoạt động khai thác zero-day. Bạn nên cấu hình cái gì?

A. Máy chủ vá

B. Honeynet

C. Honeypot

D. Máy quét virus

Câu 30. Một mạng không dây lớn hiện đang sử dụng WPA PSK. Là một phần của kết quả kiểm toán mạng của bạn, bạn đề nghị một tùy chọn xác thực không dây tập trung. Bạn nên giới thiệu gì?

A. RADIUS

B. WEP

C. WPA2 PSK

D. TKIP

Câu 31. Bạn đang thực hiện kiểm tra thâm nhập mạng cho khách hàng. Từ một dấu nhắc lệnh, bạn đưa ra lệnh telnet smtp1.acme.com 25 để xem thông tin nào được trả về. Thuật ngữ nào đề cập đến những gì bạn đã làm?

A. Từ chối dịch vụ

B. Quét cổng

C. Biểu ngữ lấy

D. Lấy thư

Câu 32. Công ty của bạn đã thuê một nhà tư vấn để triển khai giải pháp VPN an toàn bằng chứng chỉ PKI và xác thực thẻ thông minh. Mark, sếp của bạn, đã yêu cầu bạn đánh giá việc thực hiện để đảm bảo rằng các giải pháp giải quyết nhu cầu ban đầu. Thuật ngữ nào mô tả đúng nhất những gì bạn sẽ làm?

A. Đánh giá thiết kế

B. Đánh giá kiến trúc bảo mật ứng dụng

C. Đánh giá VPN

D. Đánh giá mạng

Câu 33. Tribbled Inc. gần đây đã thuê một công ty tư vấn bảo mật để thực hiện kiểm toán bảo mật mạng của mình Vulcan, Alberta, địa điểm. Một đoạn trích của kết quả kiểm toán được liệt kê ở đây:

```
Date: March 6, 2013 4:53am EST
Task performed: Network vulnerability scan
Performed by: Lennard Kneemoy
IP Subnet: 14.65.0.0 / 16
Credential used: Tribbles\Administrator
Results: We were able to connect to most hosts without specifying a password.
Recommendation: Harden network hosts.
```

What is wrong with the audit findings?

A. Mặt nạ mạng con không chính xác.

B. Phạm vi địa chỉ IP không chính xác.

C. Chuyên gia tư vấn đã tiến hành quét không xác định.

D. Chuyên gia tư vấn đã tiến hành quét thông tin xác thực.

Câu 34. Một người dùng phàn nàn rằng các tin nhắn e-mail hợp pháp từ một số khách hàng bị gắn cờ không đúng là spam ởi các máy chủ của công ty. Làm thế nào bạn có thể giải thích những gì đang xảy ra với người dùng của bạn?

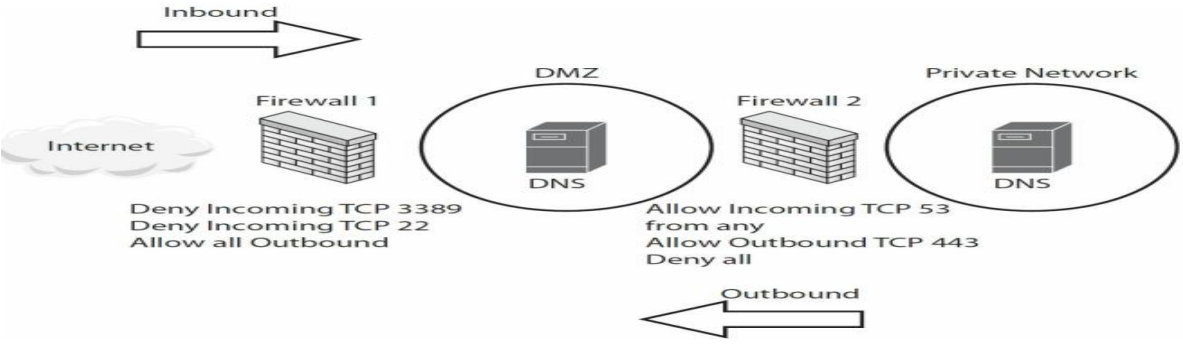
A. Các tin nhắn e-mail trong câu hỏi đang tạo ra dương tính giả.

B. Các dương tính giả đang tạo ra thông điệp email.

C. Thông điệp email trong câu hỏi đang tạo ra âm bản giả.

D. Các tiêu cực sai đang tạo ra thông điệp email.

Câu 36. Bạn là nhân viên an ninh mới được thuê cho Jokers Inc. Một sơ đồ mạng hiện có cho Halifax vị trí đã được cung cấp, như trong Hình 18-5. Bạn nên đưa ra khuyến nghị nào bảo mật cơ sở hạ tầng mạng? (Chọn hai.)



A. Không cho phép tất cả lưu lượng truy cập đi qua tường lửa.

B. Chỉ cho phép lưu lượng truy cập sao chép DNS giữa các máy chủ DNS cụ thể.

C. Không đặt máy chủ DNS trong DMZ.

D. Không cho phép lưu lượng truy cập TCP 443 đi.

Câu 37. Acme Inc. sử dụng dải địa chỉ mạng 199.126.129.0/24 trong DMZ của mình. Bạn đang cấu hình tường lửa phân tách DMZ từ mạng riêng để lưu lượng truy cập từ máy chủ DMZ được phép vào Mạng riêng tư. Bạn phát hành bộ định tuyến lệnh (config) # access-list 45 cho phép 192.168.1.0 0,0.0.255. Vấn đề với cấu hình này là gì?

A. Danh sách truy cập 55 phải được sử dụng.

B. 192.168.1.0 là một địa chỉ mạng riêng được bảo lưu.

C. Mặt nạ mạng con trong lệnh bộ định tuyến không chính xác.

D. Bộ định tuyến cần được khởi động lại.

Câu 38. Máy tính xách tay của nhân viên phải được bảo mật khi nhân viên đi công tác. Bạn có thể làm gì
Làm cứng máy tính xách tay?

A. Đặt mật khẩu CMOS.

B. Cấu hình phản chiếu đĩa.

C. Tạo băm tập tin cho tất cả các tập tin đĩa cứng.

D. Cho phép ghi nhật ký chi tiết.

Câu 39. Khi nào thì báo cáo cơ sở hữu ích?

A. Khi tiến hành kiểm tra thâm nhập

B. Khi làm cứng máy chủ DNS

C. Khi làm cứng máy chủ HTTPS

D. Khi so sánh hoạt động bình thường với hoạt động hiện tại

Câu 40. Tại sao các xét nghiệm thâm nhập đôi khi không được khuyến khích?

A. Họ có thể xác định các mối đe dọa an ninh.

B. Họ có thể làm giảm hiệu suất mạng.

C. Họ có thể tạo quá nhiều dữ liệu đăng nhập.

D. Chúng đắt tiền.

Câu 41. Bạn cần xác minh xem máy chủ DNS có cho phép chuyển vùng DNS sang tất cả máy chủ không. Hoạt động tích hợp nàoBạn nên sử dụng lệnh hệ thống?

A. netstat

B. arp

C. ping

D. nslookup

E. tracert

Chương 19

Câu 1. Điều nào sau đây có thể ngăn chặn các cuộc tấn công đang diễn ra trên mạng của bạn?

A. NIDS

B. NIPS

C. Máy chủ proxy

D. Tường lửa lọc gói

Câu 2. Quản trị viên có thể sử dụng cách nào sau đây để xác định xem có sử dụng trái phép không
của một mạng LAN không dây?

A. Phân tích giao thức
B. Máy chủ proxy
C. Giám sát hiệu suất
D. Nhật ký điểm truy cập không dây

Câu 3. Bạn chịu trách nhiệm quản lý một máy chủ FTP nội bộ. Một người dùng báo cáo rằng các tệp có sẵn trên máy chủ ngày hôm qua không còn nữa Bạn có thể nhìn vào đâu để xác định điều gì đã xảy ra với các tệp bị thiếu?

A. Nhật ký tường lửa
B. Nhật ký truy cập FTP
C. Nhật ký tải xuống FTP
D. Nhật ký tải lên FTP

Câu 4. Là quản trị viên máy chủ Windows cho máy chủ ALPHA, bạn định cấu hình kiểm toán để bạn có thể theo dõi ai xóa các tập tin trên tập tin chia sẻ SALES. Bạn sẽ xem kết quả kiểm toán ở đâu?

A. Nhật ký bảo mật
B. Nhật ký kiểm toán
C. Nhật ký ứng dụng
D. Nhật ký xóa

Câu 5. Người quản lý của bạn yêu cầu bạn định cấu hình honeypot để theo dõi hoạt động của người dùng độc hại. Bạn cài đặt máy chủ trong DMZ không có bất kỳ bản vá nào và cấu hình một trang web và máy chủ SMTP trên đó. Bạn đã cấu hìnhkhông có gì khác trên máy chủ Xác định một vấn đề với cấu hình này.

A. Honeypot cần phải được vá.
B. Honeypots không nên chạy một trang web.
C. Nhật ký Honeypot không được chuyển tiếp đến một máy chủ bảo mật khác.
D. Honeypots không nên chạy các dịch vụ SMTP.

Câu 6. Điều nào sau đây là đúng khi giám sát mạng dựa trên hành vi? (Chọn hai.)

A. Một đường cơ sở của hành vi bình thường phải được thiết lập.
B. Độ lệch từ hoạt động chấp nhận được không thể được theo dõi.
C. Các mối đe dọa mới có thể bị chặn.
D. Một cơ sở dữ liệu về các kiểu tấn công đã biết được tham khảo.

Câu 7. Bạn đã định cấu hình thiết bị NIPS để ngăn chặn các cuộc tấn công ngang qua thư mục máy chủ web. Loại gì

cấu hình này là gì?
A. Dựa trên hành vi
B. Dựa trên chữ ký
C. Dựa trên sự bất thường
D. Dựa trên web

Câu 8. Quản trị viên báo cáo rằng máy chủ tệp Windows đang hoạt động chậm hơn bình thường. Các máy chủ được vá đầy đủ và có một trình quét virus cập nhật. Bạn mở một kết nối RDP đến máy chủđể điều tra vấn đề. Bạn nên sử dụng loại nào sau đây?

A. Máy quét virus

B. Máy quét cổng
C. Điểm khôi phục hệ thống
D. Giám sát hiệu suất

Câu 9. Bạn được thừa hưởng trách nhiệm quản lý một mạng văn phòng mà không có tài liệu nào. Khi bạn thực hiện các nhiệm vụ hỗ trợ máy tính để bàn theo thời gian, bạn nhận thấy nhiều người dùng dường như có nhiều đặc quyền hơn trên mạng hơn họ cần. Những gì bạn nên làm?

A. Xóa và tạo lại tất cả các tài khoản người dùng.
B. Tiến hành đánh giá quyền truy cập và quyền của người dùng.
C. Kiểm tra nhật ký kiểm toán máy chủ.
D. Thực thi mật khẩu người dùng mạnh hơn.

Câu 10. Để tuân thủ các nguyên tắc bảo mật mới của công ty, các văn phòng chi nhánh của bạn phải theo dõi chi tiết về việc truy cập các trang web. Bạn nên cài đặt cái gì?

A. VPN
B. Máy chủ proxy
C. Tường lửa lọc gói
D. NIDS

Câu 11. Bạn muốn biết khi nào tài khoản người dùng được sửa đổi theo bất kỳ cách nào. Bạn nên cấu hình cái gì?

A. Keylogger trên tất cả các trạm người dùng
B. Kiểm toán tường lửa
C. Kiểm toán tài khoản người dùng
D. Personalfirewall trên tất cả các trạm người dùng

Câu 12. Điều nào sau đây là đúng về NIDS? (Chọn hai.)

A. Lưu lượng mạng được phân tích cho các gói độc hại.
B. Cảnh báo và thông báo có thể được cấu hình.
C. Các gói độc hại bị rơi.
D. Máy tính xách tay được bảo vệ khi ngắt kết nối mạng LAN.

Câu 13. Điều nào sau đây là đúng về HIDS?

A. Lưu lượng truy cập đáng ngờ vào mạng có thể bị chặn.
B. Truyền mã hóa không thể được theo dõi.
C. Nó phải được cài đặt trên mỗi hệ thống khi cần thiết.
D. Các tệp nhật ký không được phân tích.

Câu 14. Công ty của bạn muốn chuẩn hóa thời gian lưu giữ và xóa các loại tài liệu khác nhau. Điều gì là cần thiết để làm điều này?

A. Chính sách lưu trữ
B. RAID 0
C. Chính sách khắc phục thảm họa
D. RAID 1

Câu 15. Bạn được yêu cầu phân tích các sự kiện trong nhật ký tường lửa xảy ra sáu tháng trước. Khi bạn phân tích nhật ký tập tin, bạn thông báo sự kiện trở lại chỉ hai tháng. Vấn đề là gì?

A. Bạn phải có quyền truy cập quản trị vào nhật ký.

B. Kích thước tệp nhật ký quá nhỏ.

C. Tường lửa không thể giữ nhật ký trong hơn hai tháng.

D. Tường lửa không được vá.

Câu 16. Quản trị viên AWindows phải theo dõi các số liệu hiệu suất chính cho một nhóm máy chủ Windows đã được kiểm chứng.

Cô ấy nên làm gì?

A. Chạy màn hình hiệu suất trên mỗi máy chủ.

B. RDP vào từng máy chủ và chạy Performance Monitor.

C. RDP vào từng máy chủ và kiểm tra nhật ký Trình xem sự kiện.

D. Chạy Performance Monitor trên máy của cô ấy và thêm bộ đếm từ bảy máy chủ khác.

Câu 17. Bạn là quản trị viên thiết bị tường lửa cho công ty của bạn. RDP trước đây bị hạn chế các gói hiện đang tiếp cận thành công các máy chủ bên ngoài và bạn không định cấu hình trợ cấp tường lửa này. Bạn nên tìm ở đâu để xem ai đã làm tường lửa thay đổi và khi nào?

A. Nhật ký bảo mật

B. Nhật ký tường lửa

C. Nhật ký kiểm toán

D. Nhật ký trình xem sự kiện

Câu 18. Khi xem xét nhật ký tường lửa của bạn, bạn nhận thấy một số lượng lớn các trạm của bạn kết nối với www.freetripsforyou.com và tải xuống tệp EXE, đôi khi vào giữa đêm. Người dùng của bạn Nhà nước họ đã không truy cập trang web. Tường lửa của bạn không cho phép bất kỳ gói gửi đến nào được khởi tạo từ Internet. Điều này cho thấy gì?

A. Các trạm người dùng đang kết nối với Windows Update để áp dụng các bản vá.

B. Các trạm người dùng đã bị tấn công và đang tải phần mềm độc hại.

C. Các trạm người dùng bị nhiễm chương trình bẻ khóa mật khẩu.

D. Các trạm người dùng đang được kiểm soát từ Internet thông qua RDP.

Câu 19. Một đường cơ sở mạng công ty đã được thiết lập trong suốt hai tuần. Sử dụng đường cơ sở này dữ liệu, bạn định cấu hình hệ thống ngăn chặn xâm nhập của bạn để thông báo cho bạn về hoạt động mạng bất thường. Một cái mới sáng kiến bán hàng yêu cầu nhân viên bán hàng chạy các ứng dụng băng thông cao trên Internet. Như một kết quả là, bạn bắt đầu nhận được cảnh báo bảo mật liên quan đến hoạt động mạng bất thường. Điều nào sau đây loại cảnh báo nào bạn nhận được?

A. dương tính giả

B. Âm tính giả

C. Tích cực thực sự

D. Phủ định đúng

Câu 20. Có thể làm gì để ngăn người dùng độc hại giả mạo tệp nhật ký? (Chọn ba.)

A. Lưu trữ tệp nhật ký trên máy chủ ghi nhật ký tập trung bảo mật.

B. Mã hóa tệp nhật ký lưu trữ.

C. Chạy Windows Update.
D. Tạo băm tập tin cho các tập tin nhật ký.
Câu 21. Bạn đã được yêu cầu xác định bất kỳ sự bất thường nào từ đoạn trích nhật ký máy chủ web sau đây:
199.0.14.202, -, 15/03/09, 8:33:12, W3SVC2, SERVER, 192.168.1.1, 4502
12.168.12.79, -, 15/03/09, 8:34:09, W3SVC2, SERVER, 192.168.1.1, 3455
12.168.12.79, -, 15/03/09, 17:02:26, W3SVC2, SERVER, 192.168.1.1, 4302
192.16.255.202, -, 15/03/09, 17:03:11, W3SVC2, SERVER, 192.168.1.1, 4111
A. 199.0.14.202 không phải là địa chỉ IP hợp lệ.
B. 192.16.255.202 không phải là địa chỉ IP hợp lệ.
C. Máy chủ web không thể sử dụng 192.168.1.1.
D. Nhật ký bị thiếu các mục trong một thời gian dài.
Câu 22. Bạn là quản trị viên máy chủ Windows cho một cửa hàng quần áo ở Manhattan, New York. Sáu Windows Máy tính Active Directory Server 2008 được sử dụng thường xuyên. Các tập tin đang được sửa đổi trên các máy chủ trong giờ không kinh doanh. Bạn muốn kiểm toán hệ thống để xác định ai đã thực hiện các thay đổi và khi nào. Những gì là phương pháp nhanh nhất để triển khai cài đặt kiểm toán của bạn?
A. Định cấu hình cài đặt kiểm toán bằng Chính sách nhóm.
B. Cấu hình mỗi máy chủ với các cài đặt kiểm toán thích hợp.
C. Định cấu hình một máy chủ một cách thích hợp, xuất các cài đặt và nhập chúng vào năm máy chủ khác.
D. Giao nhiệm vụ cấu hình kiểm toán cho sáu quản trị viên khác.
Câu 23. Sự khác biệt giữa sniffer gói và NIDS là gì?
A. Không có sự khác biệt.
B. Trình thám thính gói đặt card mạng ở chế độ lăng nhăng.
C. NIDS đặt card mạng ở chế độ lăng nhăng.
D. Người đánh hơi gói không phân tích lưu lượng truy cập bị bắt.
Câu 24. Người quản lý của bạn đã yêu cầu bạn xác định máy tính khách nội bộ nào đã được kiểm soát bằng RDP từ trên mạng. Những gì bạn nên làm?
A. Kiểm tra nhật ký trên mỗi máy tính.
B. Kiểm tra nhật ký trên các máy chủ RDP của bạn.
C. Kiểm tra nhật ký tường lửa của bạn.
D. Liên hệ với ISP của bạn và yêu cầu họ kiểm tra nhật ký của họ.
Câu 25. Vấn đề tiềm ẩn khi cho phép ghi nhật ký chi tiết trên máy chủ trong thời gian dài là gì?
A. Không có vấn đề gì.
B. Nó gây suy giảm hiệu suất.
C. Băng thông mạng được tiêu thụ.
D. Ghi nhật ký Verbose tiêu thụ giấy phép người dùng.
Câu 26. Một người dùng, Jeff, báo cáo trạm Windows 8 của khách hàng của anh ta đã chậm và không ổn định kể từ thứ ba tuần trước. Gì bạn nên làm gì trước
A. Sử dụng Khôi phục Hệ thống để hoàn nguyên trạng thái máy tính vào Thứ Hai tuần trước.
B. Kiểm tra các mục nhật ký cho Thứ Hai và Thứ Ba trên máy tính Jeff.
C. Chạy Windows Update.

D. Đánh giá lại máy tính của Jeff.

Câu 27. Máy trạm của người dùng trên mạng của bạn kết nối thông qua NAT với DMZ nơi chu vi Internet của bạn tường lửa tồn tại. Vào tối thứ Sáu, một người dùng kết nối với một trang web không phù hợp. Bạn đã có đã chiếm được tất cả lưu lượng truy cập mạng trên DMZ tại thời điểm đó. Làm thế nào bạn có thể theo dõi máy trạm người dùng nào truy cập trang web? (Chọn hai.)

A. Xem nhật ký trên bộ định tuyến NAT.

B. Xem nhật ký trên tường lửa chu vi.

C. Xem gói chụp của bạn.

D. Xem tất cả lịch sử trình duyệt máy trạm.

Câu 28. Một quản trị viên đang lên lịch sao lưu cho các máy chủ Windows. Cô chọn sao lưu trạng thái hệ thống như cũng như các thư mục dữ liệu người dùng trên ổ D: Những gì cô ấy nên có trong bản sao lưu?

A. Lái xe C:

B. Tệp nhật ký

C. Hình nền

D. Đăng ký

Câu 30. Bạn đang theo dõi hiệu suất trên máy chủ UNIX có tên Alpha. Alpha được sử dụng để lưu trữ đồng thời phiên từ xa cho người dùng. Bạn nhận thấy rằng thời gian dài hoạt động đĩa máy chủ dữ dội trên Alpha trùng khớp với người dùng từ xa làm việc với các tài liệu lớn được lưu trữ trên một máy chủ UNIX riêng có tên Bravo. Gì có thể gây ra hiệu suất xuống cấp trên Alpha?

A. Có quá nhiều lưu lượng mạng.

B. CPU quá chậm.

C. Các đĩa quá chậm.

D. Không đủ RAM.

Câu 31. Một máy chủ, Charlie, chạy một ứng dụng cơ sở dữ liệu quan trọng. Ứng dụng mã hóa tất cả dữ liệu từ kết nối máy trạm của khách hàng. Bạn muốn theo dõi Charlie về hoạt động đáng ngờ và ngăn chặn mọi hoạt động các cuộc tấn công tiềm năng. Bạn nên triển khai cái gì?

A. Honeynet

B. Hips

C. NIDS

D. PKI

Câu 32. Bạn đang xem xét các mục nhật ký được chuyển tiếp cho thiết bị tường lửa đối mặt với Internet của bạn. Năm ngoái, của bạn công ty đã thực hiện một số tái cấu trúc IP và bắt đầu sử dụng không gian địa chỉ 172.16.0.0/16 trong nội bộ. Bạn nhận thấy lưu lượng lớn bất thường trong một khung thời gian ngắn đến từ thiết bị tường lửa. giao diện công cộng, 172.16,29.97, dành cho cổng UDP 53. Bạn có thể kết luận điều nào sau đây từ thông tin này?

A. 172.16,29.97 là một địa chỉ IP không hợp lệ.

B. 172.16,29.97 là một địa chỉ IP giả mạo.

C. Các nhật ký trên thiết bị tường lửa đã bị giả mạo.

D. Một cuộc tấn công từ chối dịch vụ HTTP đang được tiến hành.

Câu 33. Một người dùng phàn nàn rằng hiệu suất máy của anh ta đã suy giảm kể từ khi anh ta tải xuống một tệp miễn phí phục hồi tiện ích. Bạn muốn loại trừ khả năng có bất kỳ dịch vụ mạng độc hại nào đang chạy trong nền bằng cách xem số cổng hoạt động trên máy. Bạn nên sử dụng lệnh Windows nào để làm điều này? Ngày

Câu 34. Làm thế nào để đăng nhập và kiểm toán khác nhau?

A. Ghi nhật ký theo dõi không chỉ là sự kiện bảo mật; theo dõi kiểm tra các sự kiện bảo mật được cấu hình cụ thể.

B. Kiểm toán theo dõi không chỉ là sự kiện bảo mật; theo dõi các sự kiện bảo mật được cấu hình cụ thể.

C. Ghi nhật ký có thể theo dõi các sự kiện phần cứng; kiểm toán không thể.

D. Kiểm toán có thể theo dõi các sự kiện phần cứng; đăng nhập không thể.

Câu 35. Mạng của bạn bao gồm các PLC điều khiển máy móc cũng như máy chủ Linux và Windows máy tính để bàn. Quản trị viên phàn nàn rằng có quá nhiều sự kiện nhật ký tương tự trong các báo cáo và thông báo qua thư điện tử. Một giải pháp có thể tổng hợp các sự kiện tương tự là cần thiết. Bạn nên đề nghị gì?

A. PowerShell

B. SIEM

C. SCCM

D. Chính sách nhóm