An toan thong tin_ Nhom 09

Bắt đầu vào lúc	Thứ Ba, ngày 12 tháng 1 năm 2021, 12:15 CH
Tiểu bang	Đã kết thúc
Kết thúc lúc	Thứ Ba, ngày 12 tháng 1 năm 2021, 12:15 CH
Thời gian thực hiện	9 giây
Điểm	0,00/62,00
Điểm	**0,00** trên 10,00 (**0** %)

Câu hỏi 1

Không trả lời

Đạt điểm 1,00

Quản trị viên bảo mật cần triển khai một hệ thống phát hiện các xâm nhập có thể xảy ra dựa trên danh sách do nhà cung cấp cung cấp. Điều nào sau đây TỐT NHẤT mô tả loại IDS này?

Chọn một:

- a. Dựa trên hành vi
- b. Heuristic
- c. Dựa trên chữ ký
- d. Dựa trên dị thường

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Dựa trên chữ ký

Câu hỏi 2

Không trả lời

Đạt điểm 1,00

Ann, một kỹ thuật viên bảo mật, đang xem xét các tệp nhật ký IDS. Cô nhận thấy một số lượng lớn các cảnh báo cho các gói đa hướng từ các thiết bị chuyển mạch trên mạng. Sau khi điều tra, cô phát hiện ra rằng đây là hoạt động bình thường đối với mạng của cô. Điều nào sau đây TỐT NHẤT mô tả những kết quả này?

Chọn một:

- a. Phủ định sai
- b. Mặt tích cực thực sự
- c. Phủ định thực sự
- d. Dương tính giả

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Sai

Câu hỏi 3

Không trả lời

Đạt điểm 1,00

Điều nào sau đây nên được triển khai để ngăn việc truyền lưu lượng độc hại giữa các máy ảo được lưu trữ trên một thiết bị vật lý đơn lẻ trên mạng?

Chọn một:

- a. HIPS trên mỗi máy ảo
- b. NIDS trên mạng
- c. NIPS trên mạng
- d. HIDS trên mỗi máy ảo

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: HIPS trên mỗi máy ảo

Câu hỏi 4

Không trả lời

Đạt điểm 1,00

Một người dùng có một số cửa sổ trình duyệt ngẫu nhiên đang mở trên máy tính của họ. Chương trình nào sau đây có thể được cài đặt trên máy của anh ấy để giúp ngăn điều này xảy ra?

Chọn một:

- a. Antivirus
- b. Trình chặn phần mềm gián điệp
- c. Trình chặn cửa sổ bật lên
- d. Chống thư rác

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Trình chặn cửa sổ bật lên

Câu hỏi 5

Không trả lời

Đạt điểm 1,00

Joe, quản trị viên bảo mật, có thể thực hiện điều nào sau đây trên mạng của mình để nắm bắt thông tin chi tiết về cuộc tấn công đang xảy ra đồng thời bảo vệ mạng sản xuất của mình?

Chọn một:

- a. Nhật ký bảo mật
- b. Nhật ký kiểm tra
- c. Máy phân tích giao thức
- d. Hũ mật ong

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Honeypot

Câu hỏi 6

Không trả lời

Đạt điểm 1,00

Một số nhân viên đã nhấp vào một liên kết trong một tin nhắn độc hại đã vượt qua bộ lọc thư rác và kết quả là PC của họ bị nhiễm phần mềm độc hại. Điều nào TỐT NHẤT sau đây ngăn tình trạng này xảy ra trong tương lai?

Chọn một:

- a. Đào tạo nâng cao nhận thức về an ninh
- b. Chữ ký điện tử
- c. Thực thi mật khẩu phức tạp
- d. Ngăn ngừa mất dữ liệu

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Đào tạo nâng cao nhận thức về an ninh

Câu hỏi 7

Không trả lời

Đạt điểm 1,00

Người ta đã phát hiện ra một chương trình lây nhiễm sang hệ thống Windows quan trọng có thể thực thi được và nằm im trong bộ nhớ. Khi điện thoại di động Windows được kết nối với máy chủ, chương trình sẽ lây nhiễm bộ nạp khởi động của điện thoại và tiếp tục nhắm mục tiêu đến các máy tính hoặc điện thoại Windows bổ sung. Danh mục phần mềm độc hại nào sau đây mô tả TỐT NHẤT chương trình này?

Chọn một:

- a. Không ngày
- b. Trojan
- c. Virus
- d. Rootkit

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Virus

Câu hỏi 8

Không trả lời

Đạt điểm 1,00

Điều nào sau đây sẽ giúp ngăn chặn các cuộc tấn công của Smurf?

Chọn một:

- a. Tắt các dịch vụ không sử dụng trên tường lửa cổng
- b. Cho phép các gói UDP cần thiết trong và ngoài mạng
- c. Flash BIOS với phần sụn mới nhất
- d. Tắt phát trực tiếp trên bộ định tuyến biên giới

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Tắt tính năng phát trực tiếp trên bộ định tuyến biên giới

Câu hỏi 9

Không trả lời

Đạt điểm 1,00

Loại tấn công ứng dụng nào sau đây sẽ được sử dụng để xác định phần mềm độc hại gây ra vi phạm bảo mật mà CHƯA được xác định bởi bất kỳ nguồn đáng tin cậy nào?

Chọn một:

- a. Đưa vào XML
- b. LDAP tiêm
- c. Truyền thư mục
- d. Không ngày

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Zero-day

Câu hỏi 10

Không trả lời

Đạt điểm 1,00

Sara, một người dùng, tải xuống keygen để cài đặt phần mềm vi phạm bản quyền. Sau khi chạy keygen, hiệu suất của hệ thống cực kỳ chậm và nhiều cảnh báo chống vi-rút được hiển thị. Điều nào sau đây TỐT NHẤT mô tả loại phần mềm độc hại này?

Chọn một:

- a. Phần mềm quảng cáo
- b. Bom logic
- c. Sâu
- d. Trojan

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Trojan

Câu hỏi 11

Không trả lời

Đạt điểm 1,00

Quản trị viên bảo mật nên thực hiện điều nào sau đây để hạn chế lưu lượng truy cập web dựa trên quốc gia xuất xứ? (Chọn BA).

Chọn một hoặc nhiều:

- a. Lọc URL
- b. Cân bằng tải
- c. Proxy
- d. NEST
- Là. Bộ lọc thư rác
- f. Bức tường lửa
- g. Antivirus

Câu trả lời của bạn là không chính xác.

Các câu trả lời đúng là: Proxy, Tường lửa, lọc URL

Câu hỏi 12

Không trả lời

Đạt điểm 1,00

Mặc dù báo cáo quét lỗ hổng cho thấy không có lỗ hổng nào được phát hiện, nhưng một thử nghiệm thâm nhập tiếp theo cho thấy lỗ hổng trên mạng. Điều nào sau đây đã được báo cáo bởi quá trình quét lỗ hổng bảo mật?

Chọn một:

- a. Quét thụ động
- b. Dương tính giả
- c. Phủ định sai
- d. Quét hoạt động

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Sai phủ định

Câu hỏi 13

Không trả lời

Đạt điểm 1,00

Cờ nào sau đây được sử dụng để thiết lập kết nối TCP? (Chọn HAI).

Chọn một hoặc nhiều:

- a. URG
- b. PA
- c. THỊ GIÁC
- d. KẾT THÚC
- Là. ACK

Câu trả lời của bạn là không chính xác.

Các câu trả lời đúng là: ACK, SYN

Câu hỏi 14

Không trả lời

Đạt điểm 1,00

Một người dùng, Ann, đang báo cáo với nhóm hỗ trợ CNTT của công ty rằng màn hình máy trạm của cô ấy trống ngoài một cửa sổ có thông báo yêu cầu thanh toán nếu không ổ cứng của cô ấy sẽ bị định dạng. Loại phần mềm độc hại nào sau đây trên máy trạm của Ann?

Chọn một:

- a. Phần mềm gián điệp
- b. Phần mềm quảng cáo
- c. Ransomware
- d. Trojan

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Ransomware

Câu hỏi 15

Không trả lời

Đạt điểm 1,00

Một nhân viên báo cáo công việc đang được hoàn thành trên máy tính xách tay của công ty sử dụng điểm phát sóng không dây công cộng. Một màn hình bật lên xuất hiện và người dùng đóng cửa sổ bật lên. Vài giây sau, nền màn hình được thay đổi thành hình ảnh ổ khóa với thông báo yêu cầu thanh toán ngay lập tức để khôi phục dữ liệu. Loại phần mềm độc hại nào sau đây CÓ THỂ gây ra sự cố này nhất?

Chọn một:

- a. Ransomware
- b. Rootkit
- c. Phần mềm gián điệp
- d. Scareware

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Ransomware

Câu hỏi 16

Không trả lời

Đạt điểm 1,00

Quản trị viên bảo mật đang quan sát hành vi mạng bất thường từ một máy trạm. Máy trạm đang giao tiếp với một điểm đến độc hại đã biết qua một đường hầm được mã hóa. Quá trình quét chống vi-rút đầy đủ, với tệp định nghĩa chống vi-rút được cập nhật, không cho thấy bất kỳ dấu hiệu lây nhiễm nào. Điều nào sau đây đã xảy ra trên máy trạm?

Chọn một:

- a. Ăn cắp cookie
- b. Chiếm quyền điều khiển phiên
- c. Nhiễm phần mềm độc hại đã biết
- d. Cuộc tấn công Zero-day

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Zero-day attack

Câu hỏi 17

Không trả lời

Đạt điểm 1,00

Pete, một nhà phân tích bảo mật, đã được giao nhiệm vụ giải thích các loại phần mềm độc hại khác nhau cho các đồng nghiệp của mình. Hai loại phần mềm độc hại mà nhóm có vẻ quan tâm nhất là mạng botnet và vi rút. Điều nào sau đây giải thích sự khác biệt giữa hai loại phần mềm độc hại này?

Chọn một:

- a. Virus là một tập hợp con của botnet được sử dụng như một phần của các cuộc tấn công SYN.
- b. Botnet được sử dụng trong DR để đảm bảo thời gian hoạt động của mạng và vi rút không
- c. Botnet là một tập hợp con của phần mềm độc hại được sử dụng như một phần của các cuộc tấn công DDoS
- d. Virus là một loại phần mềm độc hại tạo ra các lỗ hổng ẩn trong một hệ điều hành

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Botnet là một tập hợp con của phần mềm độc hại được sử dụng như một phần của các cuộc tấn công DDoS

Câu hỏi 18

Không trả lời

Đạt điểm 1,00

Phương pháp tấn công phổ biến nào được sử dụng để áp đảo các dịch vụ khỏi lưu lượng truy cập từ nhiều nguồn Internet?

Chọn một:

- a. Từ chối dịch vụ phân tán
- b. Từ chối dịch vụ
- c. Giả mạo địa chỉ IP
- d. Chiếm quyền điều khiển phiên

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Từ chối dịch vụ phân tán

Câu hỏi 19

Không trả lời

Đạt điểm 1,00

Trong quá trình kiểm tra máy chủ, quản trị viên bảo mật không nhận thấy hoạt động bất thường. Tuy nhiên, một nhà phân tích an ninh mạng nhận thấy các kết nối đến các cổng trái phép từ bên ngoài mạng công ty. Sử dụng các công cụ chuyên dụng, nhà phân tích an ninh mạng cũng nhận thấy các tiến trình ẩn đang chạy. Điều nào sau đây có khả năng được cài đặt nhiều nhất trên máy chủ?

Chọn một:

- a. SPIM
- b. Rootkit
- c. Bom logic
- d. Cửa sau

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Rootkit

Câu hỏi 20

Không trả lời

Đạt điểm 1,00

Một quản trị viên mạng đã mua hai thiết bị sẽ hoạt động như các thiết bị dự phòng cho nhau. Khái niệm này minh họa TỐT NHẤT trong số các khái niệm nào sau đây?

Chọn một:

- a. Chính trực
- b. Xác thực
- c. Bảo mật
- d. khả dụng

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là:

Câu hỏi 21

Không trả lời

Đạt điểm 1,00

Phương pháp nào sẽ ngăn chặn việc giả mạo dữ liệu khi chuyển tiếp?

Chọn một:

- a. Mã hóa dữ liệu
- b. Giảm thiểu giả mạo
- c. Danh sách kiểm soát truy cập
- d. Lớp ổ cắm an toàn

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Lớp cổng bảo mật

Câu hỏi 22

Không trả lời

Đạt điểm 1,00

Bộ phận tài chính vừa mua một ứng dụng phần mềm cần giao tiếp ngược lại với máy chủ của nhà cung cấp thông qua SSL. Kỹ sư bảo mật phải mở cổng mặc định nào sau đây trên tường lửa để thực hiện tác vụ này?

Chọn một:

- a. 130
- b. 80
- c. 443
- d. 3389

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: 443

Câu hỏi 23

Không trả lời

Đạt điểm 1,00

Joe đã thuê một số quản trị viên bảo mật mới và giải thích thiết kế mạng của công ty. Ông đã mô tả vị trí và các mô tả về tường lửa, cảm biến IDS, máy chủ chống vi-rút, DMZ và HIPS của công ty. Điều nào sau đây mô tả đúng nhất sự kết hợp của các yếu tố này?

Chọn một:

- a. Cân bằng tải
- b. Thiết bị bảo mật UTM
- c. Phân đoạn mạng
- d. Phòng thủ theo chiều sâu

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Phòng thủ theo chiều sâu

Câu hỏi 24

Không trả lời

Đạt điểm 1,00

Một công ty thay thế một số thiết bị bằng một thiết bị di động, kết hợp một số chức năng. Mô tả nào sau đây phù hợp với triển khai mới này? (Chọn HAI).

Chọn một hoặc nhiều:

- a. Điện toán đám mây
- b. Cân bằng tải
- c. Thiết bị tất cả trong một
- d. Ảo hóa
- Là. Một điểm thất bại

Câu trả lời của bạn là không chính xác.

Các câu trả lời đúng là: Thiết bị tất cả trong một, Điểm hỏng duy nhất

Câu hỏi 25

Không trả lời

Đạt điểm 1,00

Kỹ thuật phổ biến nhất được sử dụng để bảo vệ khỏi sự tấn công của vi rút là gì?

Chọn một:

- a. Đảm bảo toàn vẹn dữ liệu
- b. Phát hiện chữ ký
- c. Tái tạo tự động
- d. Phát hiện Heuristic

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Phát hiện chữ ký

Câu hỏi 26

Không trả lời

Đạt điểm 1,00

Quản trị viên bảo mật sẽ thực hiện điều nào sau đây để phát hiện ra các mối đe dọa bảo mật toàn diện trên mạng?

Chọn một:

- a. Đánh giá thiết kế
- b. Quét lỗ hổng bảo mật
- c. Báo cáo cơ sở
- d. Đánh giá mã

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Quét lỗ hổng bảo mật

Câu hỏi 27

Không trả lời

Đạt điểm 1,00

Điểm truy cập không dây rouge được tạo bằng SSID giống như SSID của công ty.
Kẻ tấn công yêu cầu nhân viên kết nối với SSID và xem thông tin khi nó được chuyển tiếp đến SSID ban đầu. Loại tấn công nào được mô tả ở đây?

Chọn một:

- a. Xì trum tấn công
- b. Sniffer tấn công
- c. Người đàn ông giữa cuộc chiến
- d. Cuộc tấn công bằng phím được thỏa hiệp

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Man in the middle attack

Câu hỏi 28

Không trả lời

Đạt điểm 1,00

Câu nào ĐÚNG NHẤT sau đây mô tả khu phi quân sự?

Chọn một:

- a. Một vùng đệm giữa mạng được bảo vệ và không được bảo vệ.
- b. Một phân đoạn mạng vô trùng, biệt lập với danh sách truy cập.
- c. Mạng riêng được bảo vệ bởi tường lửa và VLAN.
- d. Một mạng mà tất cả các máy chủ tồn tại và được giám sát.

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Một vùng đệm giữa mạng được bảo vệ và không được bảo vệ.

Câu hỏi 29

Không trả lời

Đạt điểm 1,00

Người dùng đã báo cáo rằng họ nhận được các email không được yêu cầu trong hộp thư đến của họ, thường là các liên kết độc hại được nhúng vào. Điều nào sau đây nên được thực hiện để chuyển hướng các thông báo này?

Chọn một:

- a. Tường lửa ứng dụng
- b. Bộ lọc thư rác
- c. Máy chủ proxy
- d. Tường lửa mạng

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Bộ lọc thư rác

Câu hỏi 30

Không trả lời

Đạt điểm 1,00

Khi xử lý tường lửa, thuật ngữ mạng tin cậy được sử dụng để mô tả điều gì?

Chọn một:

- a. Internet
- b. DMZ
- c. Mạng nội bộ
- d. Mạng có SSL

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Mạng nội bộ

Câu hỏi 31

Không trả lời

Đạt điểm 1,00

Kỹ thuật viên tường lửa đã được hướng dẫn để tắt tất cả các cổng không an toàn trên tường lửa của công ty. Kỹ thuật viên đã chặn giao thông trên các cổng 21, 69, 80 và 137-139. Kỹ thuật viên đã cho phép lưu lượng truy cập trên các cổng 22 và 443. Điều nào sau đây liệt kê đúng các giao thức bị chặn và được phép?

Chọn một:

- a. Bị chặn: FTP, HTTP, HTTPS; Được phép: SFTP, SSH, SCP, NetBIOS
- b. Bị chặn: TFTP, HTTP, NetBIOS; Được phép: HTTPS, FTP
- c. Bị chặn: FTP, TFTP, HTTP, NetBIOS; Được phép: SFTP, SSH, SCP, HTTPS
- d. Bị chặn: SFTP, TFTP, HTTP, NetBIOS; Được phép: SSH, SCP, HTTPS

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Bị chặn: FTP, TFTP, HTTP, NetBIOS; Được phép: SFTP, SSH, SCP, HTTPS

Câu hỏi 32

Không trả lời

Đạt điểm 1,00

Giám đốc Thông tin (CIO) nhận được một tin nhắn đe dọa ẩn danh có nội dung "hãy cẩn thận với ngày đầu tiên của năm". CIO nghi ngờ tin nhắn có thể là từ một cựu nhân viên bất mãn đang lên kế hoạch tấn công. CIO nên quan tâm đến điều nào sau đây?

Chọn một:

- a. Smurf Attack
- b. Trojan
- c. Bom logic
- d. Virus

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Bom logic

Câu hỏi 33

Không trả lời

Đạt điểm 1,00

Loại phần mềm độc hại nào sau đây có thể yêu cầu sự tương tác của người dùng, không tự ẩn và thường được nhận dạng bằng cửa sổ bật lên tiếp thị dựa trên thói quen duyệt web?

Chọn một:

- a. Phần mềm quảng cáo
- b. Virus
- c. Botnet
- d. Rootkit

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Phần mềm quảng cáo

Câu hỏi 34

Không trả lời

Đạt điểm 1,00

Thiết bị nào sau đây chắc chắn nhất sẽ có giao diện DMZ?

Chọn một:

- a. Công tắc điện
- b. Ủy quyền
- c. Cân bằng tải
- d. Bức tường lửa

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Tường lửa

Câu hỏi 35

Không trả lời

Đạt điểm 1,00

Cuộc tấn công nào có thể được sử dụng trên một VLAN gốc?

Chọn một:

- a. Gắn thẻ kép
- b. Popping thân cây
- c. Từ chối dịch vụ
- d. Truyền tải VLAN

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Gắn thẻ kép

Câu hỏi 36

Không trả lời

Đạt điểm 1,00

Một người dùng tình cờ duyệt Internet được chuyển hướng đến một trang web warez nơi một số cửa sổ bật lên xuất hiện. Sau khi nhấp vào cửa sổ bật lên để hoàn thành khảo sát, quá trình tải xuống từng ổ diễn ra. Nội dung nào sau đây có khả năng chứa nhiều nhất trong bản tải xuống?

Chọn một:

- a. Xì trum
- b. DDoS
- c. Phần mềm gián điệp
- d. Bom logic
- Là. Cửa sau

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Phần mềm gián điệp

Câu hỏi 37

Không trả lời

Đạt điểm 1,00

Một trojan gần đây đã được phát hiện trên một máy chủ. Hiện có nhiều lo ngại rằng đã có một lỗ hổng bảo mật cho phép những người không được phép truy cập dữ liệu. Quản trị viên nên tìm kiếm sự hiện diện của a / an:

Chọn một:

- a. Rootkit
- b. Ứng dụng phần mềm quảng cáo
- c. Bom logic
- d. Cửa sau

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Backdoor

Câu hỏi 38

Không trả lời

Đạt điểm 1,00

Cuộc tấn công nào sau đây thường được bắt đầu từ mạng botnet?

Chọn một:

- a. Một cuộc tấn công thúc đẩy chiến tranh
- b. Từ chối dịch vụ phân tán
- c. Đưa vào tiêu đề HTTP
- d. Tấn công kịch bản trên nhiều trang web

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Từ chối dịch vụ phân tán

Câu hỏi 39

Không trả lời

Đạt điểm 1,00

Câu lệnh nào là ĐÚNG về hoạt động của trình kiểm tra gói tin?

Chọn một:

- a. Nó phải được đặt trên một giao diện LAN ảo duy nhất.
- b. Chúng được yêu cầu để vận hành tường lửa và kiểm tra trạng thái.
- c. Nó chỉ có thể có một giao diện trên một mạng quản lý.
- d. Thẻ Ethernet phải được đặt ở chế độ quảng cáo

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Thẻ Ethernet phải được đặt ở chế độ không hoạt động

Câu hỏi 40

Không trả lời

Đạt điểm 1,00

Joe, Giám đốc kỹ thuật (CTO), lo ngại về việc phần mềm độc hại mới được đưa vào mạng công ty. Ông đã giao nhiệm vụ cho các kỹ sư bảo mật triển khai một công nghệ có khả năng cảnh báo cho nhóm khi có lưu lượng truy cập bất thường trên mạng. Loại công nghệ nào sau đây sẽ giải quyết TỐT NHẤT tình huống này?

Chọn một:

- a. IDS dựa trên bất thường
- b. IDS chữ ký
- c. Tường lửa proxy
- d. Tường lửa ứng dụng

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: IDS dựa trên dị thường

Câu hỏi 41

Không trả lời

Đạt điểm 1,00

Phần mềm nào sau đây cho phép quản trị viên mạng kiểm tra tiêu đề giao thức để khắc phục sự cố mạng?

Chọn một:

- a. Lính bắn tỉa
- b. Bộ lọc URL
- c. Công tắc điện
- d. Bộ lọc thư rác

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Trình đánh hơi gói

Câu hỏi 42

Không trả lời

Đạt điểm 1,00

Giám đốc Tài chính (CFO) đã yêu cầu Giám đốc Thông tin (CISO) cung cấp các câu trả lời cho một báo cáo kiểm toán gần đây nêu chi tiết những khiếm khuyết trong các biện pháp kiểm soát an ninh của tổ chức. Giám đốc tài chính muốn biết các cách mà tổ chức có thể cải thiện các biện pháp kiểm soát ủy quyền của mình. Theo yêu cầu của Giám đốc tài chính, CISO nên tập trung vào các biện pháp kiểm soát nào sau đây trong báo cáo? (Chọn Ba)

Chọn một hoặc nhiều:

- a. Đặc quyền cho thuê
- b. Hệ thống sinh trắc học
- c. Mật khẩu một lần
- d. Mã thông báo phần cứng
- Là. Chính sách về độ phức tạp của mật khẩu
- f. Dấu hiệu duy nhất trên
- g. Xác thực đa yếu tố
- h. Quyền dựa trên vai trò
- Tôi. Tách nhiệm vụ

Câu trả lời của bạn là không chính xác.

Các câu trả lời đúng là: Quyền dựa trên vai trò, Phân tách nhiệm vụ, Đặc quyền cho thuê

Câu hỏi 43

Không trả lời

Đạt điểm 1,00

Một tổ chức gần đây đã chuyển từ giải pháp email dựa trên đám mây sang máy chủ email nội bộ. Tường lửa cần được sửa đổi để cho phép gửi và nhận email. Cổng nào sau đây nên được mở trên tường lửa để cho phép lưu lượng email? (Chọn BA).

Chọn một hoặc nhiều:

- a. TCP 23
- b. TCP 22
- c. TCP 25
- d. TCP 53
- Là. TCP 143
- f. TCP 445
- g. TCP 110

Câu trả lời của bạn là không chính xác.

Các câu trả lời đúng là: TCP 25, TCP 110, TCP 143

Câu hỏi 44

Không trả lời

Đạt điểm 1,00

Phần tử kiến trúc bảo mật nào sau đây cũng có chức năng trình thám thính? (Chọn HAI).

Chọn một hoặc nhiều:

- a. IPS
- b. IDS
- c. HSM
- d. Trình tăng tốc SSL
- Là. WAP

Câu trả lời của bạn là không chính xác.

Các câu trả lời đúng là: IPS, IDS

Câu hỏi 45

Không trả lời

Đạt điểm 1,00

Loại thiết bị nào có thể ngăn chặn sự xâm nhập vào mạng của bạn?

Chọn một:

- a. IDS
- b. Chậu mật ong
- c. HIDS
- d. IPS

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: IPS

Câu hỏi 46

Không trả lời

Đạt điểm 1,00

Một công ty muốn ngăn người dùng cuối cắm điện thoại thông minh chưa được phê duyệt vào PC và truyền dữ liệu. Điều nào sau đây sẽ là biện pháp kiểm soát TỐT NHẤT để triển khai?

Chọn một:

- a. IDS
- b. HỒNG
- c. MDM
- d. DLP

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: DLP

Câu hỏi 47

Không trả lời

Đạt điểm 1,00

Điều quan trọng nhất là đảm bảo rằng tường lửa được cấu hình để thực hiện điều nào sau đây?

Chọn một:

- a. Quản lý cảnh báo về khả năng xâm nhập.
- b. Báo cho quản trị viên về khả năng xâm nhập.
- c. Từ chối tất cả lưu lượng truy cập dựa trên các chữ ký đã biết.
- d. Từ chối tất cả giao thông và chỉ cho phép theo ngoại lệ.

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Từ chối tất cả giao thông và chỉ cho phép theo ngoại lệ.

Câu hỏi 48

Không trả lời

Đạt điểm 1,00

Quy tắc tường lửa nào sau đây chỉ từ chối chuyển vùng DNS?

Chọn một:

- a. từ chối tcp bất kỳ cổng nào 53
- b. từ chối tất cả các gói dns
- c. từ chối ip bất kỳ
- d. từ chối udp bất kỳ cổng nào 53

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: từ chối tcp bất kỳ cổng nào 53

Câu hỏi 49

Không trả lời

Đạt điểm 1,00

Sau khi lướt Internet, Joe, một người dùng, thức dậy và phát hiện tất cả các tệp của mình đã bị hỏng. Hình nền của anh ấy đã được thay thế bằng một thông báo cho biết các tập tin đã được mã hóa và anh ấy cần chuyển tiền ra nước ngoài để khôi phục chúng. Joe là nạn nhân của:

Chọn một:

- a. phần mềm gián điệp
- b. ransomware
- c. một quả bom logic
- d. một keylogger

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: ransomware

Câu hỏi 50

Không trả lời

Đạt điểm 1,00

Thành phần thiết kế nào sau đây được sử dụng để cách ly các thiết bị mạng như máy chủ web?

Chọn một:

- a. VPN
- b. VLAN
- c. ĐỆM
- d. DMZ

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: DMZ

Câu hỏi 51

Không trả lời

Đạt điểm 1,00

Một quản trị viên hệ thống đã nhận thấy các vấn đề về hiệu suất mạng và muốn thu thập dữ liệu hiệu suất từ bộ định tuyến cổng. Cách nào sau đây có thể được sử dụng để thực hiện hành động này?

Chọn một:

- a. iSCSI
- b. IPSec
- c. SMTP
- d. SNMP

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: SNMP

Câu hỏi 52

Không trả lời

Đạt điểm 1,00

Máy tính chạy Windows bị nhiễm phần mềm độc hại và chạy quá chậm để khởi động và chạy trình quét phần mềm độc hại. Cách nào sau đây là cách TỐT NHẤT để chạy trình quét phần mềm độc hại?

Chọn một:

- a. Khởi động từ CD / USB
- b. Tắt kết nối mạng
- c. Diệt tất cả các quy trình hệ thống
- d. Bật tường lửa

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Khởi động từ CD / USB

Câu hỏi 53

Không trả lời

Đạt điểm 1,00

Dấu thời gian và số thứ tự đóng vai trò là biện pháp đối phó với loại tấn công nào sau đây?

Chọn một:

- a. phát lại
- b. Từ
- c. Thăm viếng
- d. Xì trum

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là:

Câu hỏi 54

Không trả lời

Đạt điểm 1,00

Một cuộc tấn công từ chối dịch vụ phân tán có thể được mô tả TỐT NHẤT là:

Chọn một:

- a. Nhiều máy tính tấn công một mục tiêu trong một nỗ lực có tổ chức để làm cạn kiệt tài nguyên của nó.
- b. Người dùng cố gắng nhập dữ liệu ngẫu nhiên hoặc không hợp lệ vào các trường trong ứng dụng trình duyệt web.
- c. Các ký tự không hợp lệ được nhập vào một trường trong ứng dụng cơ sở dữ liệu.
- d. Nhiều kẻ tấn công cố gắng đạt được các đặc quyền nâng cao trên hệ thống mục tiêu.

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Nhiều máy tính tấn công một mục tiêu trong một nỗ lực có tổ chức để làm cạn kiệt tài nguyên của nó.

Câu hỏi 55

Không trả lời

Đạt điểm 1,00

Điều nào sau đây mà kỹ sư bảo mật sẽ đặt làm mặt nạ mạng con cho các máy chủ bên dưới để sử dụng địa chỉ máy chủ lưu trữ trên các miền quảng bá riêng biệt?
Máy chủ 1: 192.168.100.6
Máy chủ 2: 192.168.100.9
Máy chủ 3: 192.169.100.20

Chọn một:

- a. /30
- b. /28
- c. /24
- d. /29
- Là. /27

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: / 29

Câu hỏi 56

Không trả lời

Đạt điểm 1,00

Theo mặc định, mục nào sau đây sử dụng cổng TCP 22? (Chọn BA).

Chọn một hoặc nhiều:

- a. SSL
- b. FTPS
- c. TLS
- d. SSH
- Là. SCP
- f. SFTP
- g. HTTPS
- h. STELNET

Câu trả lời của bạn là không chính xác.

Các câu trả lời đúng là: SCP, SSH, SFTP

Câu hỏi 57

Không trả lời

Đạt điểm 1,00

Quản trị viên bảo mật muốn chặn truy cập trái phép vào máy chủ web bằng chương trình phần mềm được cài đặt cục bộ. Quản trị viên nên triển khai điều nào sau đây?

Chọn một:

- a. NEST
- b. NIPS
- c. HÔNG
- d. HIDS

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: HIPS

Câu hỏi 58

Không trả lời

Đạt điểm 1,00

Loại phần mềm độc hại nào sau đây, cố gắng tránh việc phát hiện phần mềm độc hại bằng cách cố gắng che giấu vị trí thực của nó trên hệ thống bị nhiễm?

Chọn một:

- a. Trojan
- b. Keylogger
- c. Virus bọc thép
- d. Ransomware

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Trojan

Câu hỏi 59

Không trả lời

Đạt điểm 1,00

Pete, một quản trị viên bảo mật, đã quan sát thấy nhiều lần cố gắng đột nhập vào mạng. Cách nào sau đây được thiết kế để ngăn chặn sự xâm nhập vào mạng?

Chọn một:

- a. HIDS
- b. NIPS
- c. NEST
- d. HÔNG

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: NIPS

Câu hỏi 60

Không trả lời

Đạt điểm 1,00

Một thanh công cụ tin tức và thời tiết đã được cài đặt một cách tình cờ vào một trình duyệt web. Thanh công cụ theo dõi các hoạt động trực tuyến của người dùng và gửi chúng đến một máy chủ ghi nhật ký trung tâm. Cuộc tấn công nào sau đây đã diễn ra?

Chọn một:

- a. Cookie flash
- b. Man-in-the-browser
- c. Chiếm quyền điều khiển phiên
- d. Tiện ích bổ sung độc hại
- Là. Thực thi mã từ xa

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Tiện ích bổ sung độc hại

Câu hỏi 61

Không trả lời

Đạt điểm 1,00

Kỹ sư an ninh mạng vừa triển khai một IDS trên mạng, nhưng Giám đốc kỹ thuật (CTO) lo ngại rằng thiết bị này chỉ có thể phát hiện những điểm bất thường đã biết. Loại IDS nào sau đây đã được triển khai?

Chọn một:

- a. IDS dựa trên bất thường
- b. IDS dựa trên hành vi
- c. IDS dựa trên chữ ký
- d. Heuristic IDS

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: IDS Dựa trên Chữ ký

Câu hỏi 62

Không trả lời

Đạt điểm 1,00

Pete, quản trị viên hệ thống, đã chặn người dùng truy cập các trang web mạng xã hội. Ngoài việc bảo vệ thông tin của công ty khỏi vô tình bị rò rỉ, điều này cung cấp lợi ích bảo mật bổ sung nào?

Chọn một:

- a. Không cạnh tranh với sự hiện diện xã hội chính thức của công ty
- b. Bảo vệ chống lại phần mềm độc hại do quảng cáo biểu ngữ giới thiệu
- c. Tăng năng suất của người dùng dựa trên ít phiền nhiễu hơn
- d. Loại bỏ rủi ro do chia sẻ tệp P2P trái phép

Câu trả lời của bạn là không chính xác.

Câu trả lời đúng là: Bảo vệ chống lại phần mềm độc hại do quảng cáo biểu ngữ giới thiệu

◄ Chương 8 - Bảo mật cơ sở dữ liệu LAB

Chuyển tới...

Video: Bảo mật cơ sở dữ liệu ►