CÂU HỎI TRẮC NGHIỆM
ĐỀ THI GIỮA KỲ NĂM 2024-2025
MÔN: GIAO THỨC MẠNG

Câu 1. Endpoints (thiết bị đầu cuối) đặc biệt dễ bị tấn công liên quan đến phần mềm độc hại qua email hoặc duyệt web, ví dụ như:

A. Trojan.. **B**. DDoS.. **C**. Phishing.. **D**. Malware..

Câu 2. Các tấn công mà endpoints thường phải đối mặt bao gồm:

A. Malware và phần mềm chống virus..

B. DDoS và các cuộc tấn công từ bên ngoài..

C. Vi phạm dữ liệu và phần mềm độc hại..

D. Hệ thống ngăn chặn xâm nhập và bảo mật phần cứng..

Câu 3. Hệ thống bảo mật nào thường được sử dụng trên thiết bị đầu cuối để bảo vệ chống lại các phần mềm độc hại?

A. Hệ thống bảo vệ mạng.. **B**. Phần mềm chống virus/anti-malware..

C. Tường lửa mạng.. **D**. Mã hóa dữ liệu..

Câu 4. AAA kiểm soát những gì trong mạng?

A. Ai có quyền truy cập vào mạng.. **B**. Các dữ liệu nhạy cảm của mạng..

C. Phần cứng trong mạng.. **D**. Lưu lượng mạng giữa các thiết bị..

Câu 5. AAA xác định điều gì sau khi người dùng được xác thực?

A. Các dịch vụ mà họ có quyền truy cập.. **B**. Các dữ liệu mà họ có thể chỉnh sửa..

C. Mức độ bảo mật của mạng.. **D**. Địa chỉ IP của thiết bị kết nối..

Câu 6. Các thiết bị đầu cuối được bảo vệ tốt nhất bởi sự kết hợp của:

A. NAC, tường lửa và hệ thống phát hiện xâm nhập..

B. Phần mềm AMP, ESA và WSA..

C. Các thiết bị bảo mật của mạng..

D. Bảo mật email và dữ liệu..

Câu 7. VLAN hopping là gì?

A. Một cuộc tấn công làm cho lưu lượng từ một VLAN có thể được nhìn thấy bởi một VLAN khác mà không cần router..

B. Một cuộc tấn công phá hủy toàn bộ mạng LAN..

C. Một tấn công vào máy chủ DNS..

D. Một phương thức bảo vệ mạng..

Câu 8. Để ngăn chặn tấn công VLAN hopping, quản trị viên mạng nên làm gì?

A. Kích hoạt auto trunking trên tất cả các cổng..

B. Tắt tính năng trunking trên tất cả các cổng truy cập..

C. Cải thiện khả năng kết nối của router..

D. Đảm bảo các VLAN có thể kết nối tự do..

Câu 9. Để bảo vệ chống lại các tấn công giả mạo DHCP, quản trị viên mạng nên sử dụng gì?

A. DHCP snooping.. **B**. Phân bổ dải địa chỉ IP tĩnh..

C. Cập nhật phần mềm thường xuyên.. **D**. Cấu hình lại VLAN..

Câu 10. Cách giảm thiểu việc khai thác CDP là gì?

A. Giới hạn việc sử dụng CDP trên thiết bị hoặc cổng..

B. Kích hoạt CDP trên tất cả các cổng..

C. Vô hiệu hóa tất cả các giao thức liên kết..

D. Tắt DHCP trên mạng nội bộ..

Câu 11. Tiêu chuẩn IEEE 802.1X là gì?
A. Một giao thức bảo mật dữ liệu..
B. Một giao thức kiểm soát truy cập và xác thực dựa trên cổng..
C. Một giao thức truyền tải dữ liệu..
D. Một giao thức phát hiện mạng..

Câu 12. IEEE 802.1X giúp làm gì?
A. Hạn chế các trạm làm việc kết nối với mạng LAN..
B. Kiểm tra tính bảo mật của các cổng switch..
C. Giới hạn các cổng mạng công cộng..
D. Hạn chế các trạm làm việc kết nối với LAN qua các cổng switch công khai..

Câu 13. Nếu Lớp 2 bị xâm phạm, điều gì sẽ xảy ra?
A. Chỉ các lớp trên Lớp 2 bị ảnh hưởng..
B. Lớp 2 sẽ không bị ảnh hưởng gì..
C. Tất cả các lớp trên Lớp 2 cũng bị ảnh hưởng..
D. Chỉ Lớp 1 bị ảnh hưởng..

Câu 14. Bước đầu tiên trong việc giảm thiểu các cuộc tấn công vào cơ sở hạ tầng Lớp 2 là gì?
A. Cập nhật phần mềm bảo mật..
B. Hiểu cách thức hoạt động của Lớp 2 và các giải pháp Lớp 2..
C. Kích hoạt bảo mật trên tất cả các cổng..
D. Tăng cường bảo mật mạng nội bộ..

Câu 15. Giải pháp nào giúp bảo vệ Lớp 2 khỏi các tấn công?
A. Port Security, DHCP Snooping, DAI, IPSG..
B. Port Security, DHCP Snooping, DAI, IPSG..
C. Cải thiện bảo mật Lớp 3..
D. Cấu hình thêm các mạng phụ..

Câu 16. Các tấn công tràn địa chỉ MAC nhắm vào gì?
A. Bộ định tuyến..
B. Switch bằng cách giả mạo các địa chỉ MAC..
C. Phần mềm chống virus..
D. Tường lửa mạng..

Câu 17. VLAN hopping cho phép gì?
A. Cho phép một VLAN nhìn thấy lưu lượng của VLAN khác mà không cần router..
B. Một cuộc tấn công phá hủy toàn bộ mạng LAN..
C. Một tấn công vào máy chủ DNS..
D. Một phương thức bảo vệ mạng..

Câu 18. Để ngăn chặn tấn công VLAN hopping, quản trị viên mạng nên làm gì?
A. Kích hoạt tính năng auto trunking trên tất cả các cổng..
B. Tắt tính năng trunking trên tất cả các cổng truy cập..
C. Sử dụng VLAN gốc..
D. Cải thiện khả năng kết nối giữa các VLAN..

Câu 19. Để bảo vệ chống lại các tấn công giả mạo DHCP, mạng nên làm gì?
A. Triển khai DHCP snooping..
B. Phân bổ dải địa chỉ IP tĩnh..
C. Cập nhật phần mềm thường xuyên..
D. Cấu hình lại các cổng VLAN..

Câu 20. Cách giảm thiểu việc khai thác CDP là gì?
A. Kích hoạt CDP trên tất cả các cổng..
B. Giới hạn việc sử dụng CDP trên thiết bị hoặc cổng..
C. Tăng cường bảo mật trên mỗi VLAN..
D. Sử dụng tường lửa mạng..

Câu 21. Các tấn công tràn địa chỉ MAC nhắm vào gì?
A. Bộ định tuyến..
B. Switch bằng cách giả mạo các địa chỉ MAC..
C. Phần mềm chống virus..
D. Tường lửa mạng..

Câu 22. Tấn công VLAN hopping cho phép gì?
A. Cho phép lưu lượng từ một VLAN được nhìn thấy bởi một VLAN khác mà không cần router..
B. Cho phép kết nối giữa các VLAN mà không cần cổng trunk..
C. Cho phép một VLAN nhìn thấy tất cả VLAN khác trong mạng..
D. Cải thiện bảo mật giữa các VLAN..

Câu 23. Một tấn công VLAN double-tagging là gì?
A. Một cuộc tấn công phá hủy toàn bộ mạng LAN..
B. Một cuộc tấn công mà tác nhân đe dọa kết nối với một cổng trong cùng VLAN với VLAN gốc của cổng trunk..
C. Một cuộc tấn công trên Lớp 3 để phá hủy cấu trúc mạng..
D. Một cuộc tấn công vào máy chủ DNS..

Câu 24. Khi nào tấn công VLAN hopping có thể xảy ra?
A. Khi một VLAN đang bị xâm phạm..
B. Khi có sự kết nối giữa các VLAN thông qua router..
C. Khi một VLAN không được bảo mật đúng cách..
D. Khi một VLAN có tính bảo mật cao và hạn chế kết nối giữa các VLAN khác..

Câu 25. Công cụ nào có thể được sử dụng để ngăn chặn tấn công VLAN hopping?
A. Trunking auto trên các cổng..
B. Tắt tính năng trunking trên tất cả các cổng truy cập..
C. Tăng cường bảo mật router..
D. Đảm bảo các VLAN có thể kết nối tự do..

Câu 26. Các tấn công giả mạo địa chỉ MAC có thể bị ngăn chặn bằng cách nào?
A. Cấu hình các VLAN để không chia sẻ địa chỉ MAC..
B. Triển khai IPSG (IP Source Guard)..
C. Cập nhật phần mềm bảo mật..
D. Sử dụng các thiết bị bảo mật như firewall..

Câu 27. Tấn công VLAN double-tagging hoạt động như thế nào?
A. Nó gửi thông tin giả mạo đến một VLAN không được phép kết nối..
B. Nó đánh lừa switch để cho phép một cổng trong VLAN nhìn thấy VLAN khác..
C. Nó chặn các cổng mạng công cộng..
D. Nó sử dụng địa chỉ MAC để định tuyến lưu lượng trên toàn bộ VLAN..

Câu 28. Mục tiêu chính của tấn công VLAN hopping là gì?
A. Làm gián đoạn các dịch vụ trong một VLAN..
B. Cho phép một VLAN nhìn thấy lưu lượng của VLAN khác mà không cần router..
C. Xâm nhập vào các thiết bị bảo mật của mạng..
D. Làm chậm tốc độ mạng giữa các VLAN..

Câu 29. Các tấn công tràn địa chỉ MAC có thể được ngăn chặn bằng cách nào?
A. Sử dụng thiết bị ngăn chặn tấn công mạng..
B. Triển khai Port Security trên các cổng switch..
C. Tăng cường các lớp bảo mật mạng..
D. Triển khai VLAN riêng biệt cho các dịch vụ mạng..

Câu 30. Một tấn công VLAN double-tagging có thể được ngăn chặn bằng cách nào?
A. Kích hoạt tính năng auto trunking trên tất cả các cổng..
B. Giới hạn sử dụng VLAN trên các cổng switch..
C. Cấu hình VLAN gốc cho các cổng trunk..
D. Chỉ sử dụng các cổng không có tính năng trunking..

Câu 31. Các tấn công VLAN hopping và VLAN double-tagging có thể được ngăn chặn bằng cách nào?
A. Kích hoạt tính năng trunking tự động trên tất cả các cổng..
B. Triển khai các hướng dẫn bảo mật trunk..
C. Sử dụng các cổng mạng mở rộng..
D. Cải thiện bảo mật trên Lớp 3 của mạng..

Câu 32. Cách nào giúp bảo vệ VLAN khỏi các tấn công double-tagging?
A. Sử dụng bảo mật phần mềm..
B. Tắt tính năng trunking trên tất cả các cổng truy cập..
C. Đảm bảo VLAN gốc chỉ được sử dụng cho các liên kết trunk..
D. Tăng cường khả năng bảo mật cho Lớp 3..

Câu 33. Điều gì cần làm để giảm thiểu tấn công VLAN hopping?
A. Kích hoạt tính năng trunking tự động trên tất cả các cổng..
B. Tắt tính năng trunking trên các cổng truy cập..
C. Tăng cường bảo mật router..
D. Đảm bảo các VLAN có thể kết nối tự do..

Câu 34. Các tấn công DHCP nào có thể được giảm thiểu bằng DHCP snooping?
A. DHCP starvation và DHCP spoofing..
B. DHCP starvation và DHCP spoofing..
C. DHCP flooding và DHCP discovery..
D. DHCP discovery và DHCP offering..

Câu 35. DHCP starvation là gì?
A. Một cuộc tấn công chiếm dụng tất cả các địa chỉ IP..
B. Một cuộc tấn công sử dụng IP giả mạo để gây xung đột địa chỉ..
C. Một cuộc tấn công gây cạn kiệt các địa chỉ IP có sẵn..
D. Một cuộc tấn công làm chậm quá trình cấp phát DHCP..

Câu 36. Cách giảm thiểu DHCP spoofing là gì?
A. Triển khai DHCP snooping..
B. Triển khai DHCP snooping..
C. Cấu hình firewall mạng..
D. Cải thiện hệ thống bảo mật phần cứng..

Câu 37. Các tấn công DHCP starvation và DHCP spoofing có thể giảm thiểu bằng cách nào?
A. Cấu hình router bảo mật..
B. Triển khai DHCP snooping..
C. Giới hạn băng thông mạng..
D. Cấu hình lại các cổng VLAN..

Câu 38. VLAN double-tagging xảy ra khi nào?
A. Khi một VLAN bị xâm nhập và không bảo mật..
B. Khi tác nhân đe dọa kết nối với một cổng trong cùng VLAN với VLAN gốc của cổng trunk..
C. Khi VLAN không được cấu hình đúng..
D. Khi một VLAN không có cổng trunk..

Câu 39. Câu nào dưới đây là một trong những phương pháp để giảm thiểu tấn công VLAN hopping?
A. Tăng cường bảo mật mạng nội bộ..
B. Đảm bảo VLAN gốc chỉ sử dụng cho các liên kết trunk..
C. Tạo thêm VLAN..
D. Cấu hình phần mềm firewall trên các thiết bị..

Câu 40. Tấn công DHCP spoofing là gì?
A. Tấn công giả mạo máy chủ DHCP để cung cấp thông tin sai cho các client..
B. Tấn công chặn lưu lượng giữa các cổng..
C. Tấn công giả mạo máy chủ DHCP để cung cấp thông tin sai cho các client..
D. Tấn công vào bộ định tuyến..

Câu 41. Tấn công ARP là gì?
A. Tấn công vào địa chỉ MAC của các cổng mạng..
B. Tấn công giả mạo địa chỉ MAC gửi đến switch để cập nhật bảng MAC..
C. Tấn công vào địa chỉ IP của các máy chủ trong mạng..
D. Tấn công vào cổng kết nối của router..

Câu 42. Khi một tấn công ARP xảy ra, switch làm gì?
A. Cập nhật bảng MAC của mình với địa chỉ MAC giả..
B. Chặn tất cả lưu lượng từ các cổng bị tấn công..
C. Cập nhật bảng MAC với địa chỉ MAC của tác nhân đe dọa..
D. Cập nhật tất cả các thông tin trên hệ thống..

Câu 43. Các tấn công ARP poisoning và ARP spoofing có thể được giảm thiểu bằng cách nào?
A. Cài đặt tường lửa mạnh..
B. Triển khai Dynamic ARP Inspection (DAI)..
C. Tăng cường bảo mật Lớp 3..
D. Sử dụng các cổng không phải trunk..

Câu 44. Tấn công giả mạo địa chỉ IP xảy ra khi nào?
A. Khi tác nhân thay đổi địa chỉ IP của host trong mạng..
B. Khi tác nhân giả mạo địa chỉ IP hợp lệ để chiếm đoạt địa chỉ..
C. Khi người dùng sử dụng IP ngẫu nhiên trong mạng..
D. Khi một máy chủ DNS bị tấn công..

Câu 45. Tấn công giả mạo địa chỉ MAC xảy ra khi nào?
A. Khi tác nhân thay đổi địa chỉ MAC của host trong mạng..
B. Khi một địa chỉ MAC bị xâm nhập vào hệ thống..
C. Khi tác nhân giả mạo địa chỉ MAC của host khác để đánh lừa switch..
D. Khi một host thay đổi địa chỉ IP của mình..

Câu 46. Giải pháp nào giúp giảm thiểu các tấn công giả mạo địa chỉ MAC?
A. Cấu hình cổng switch không bảo mật..
B. Cấu hình firewall để ngăn chặn lưu lượng không hợp lệ..
C. Triển khai IP Source Guard (IPSG)..
D. Sử dụng phần mềm chống virus mạnh..

Câu 47. Khi nào tấn công giả mạo địa chỉ MAC có thể xảy ra?
A. Khi host thay đổi địa chỉ IP của mình..
B. Khi một host giả mạo địa chỉ MAC của host khác..
C. Khi một host giả mạo địa chỉ MAC của một host mục tiêu..
D. Khi kết nối giữa các cổng switch bị gián đoạn..

Câu 48. Công cụ nào có thể giảm thiểu các tấn công ARP spoofing?

A. Sử dụng phần mềm diệt virus..

B. Triển khai Dynamic ARP Inspection (DAI)..

C. Tắt các tính năng trunking..

D. Cấu hình máy chủ DHCP..

Câu 49. Tấn công ARP spoofing có thể gây ra hậu quả gì?

A. Làm gián đoạn toàn bộ mạng..

B. Chặn tất cả lưu lượng giữa các cổng mạng..

C. Làm giả mạo địa chỉ MAC và IP trên mạng, gây xung đột địa chỉ..

D. Làm thay đổi các cài đặt DNS trong mạng..

Câu 50. Câu nào dưới đây là đúng khi nói về tấn công giả mạo địa chỉ IP?

A. Tấn công giả mạo IP chỉ xảy ra trên các mạng IPv6..

B. Tấn công giả mạo IP chỉ làm gián đoạn mạng trong thời gian ngắn..

C. Tấn công giả mạo IP có thể chiếm đoạt địa chỉ IP hợp lệ của thiết bị..

D. Tấn công giả mạo IP không ảnh hưởng đến việc cấp phát DHCP..