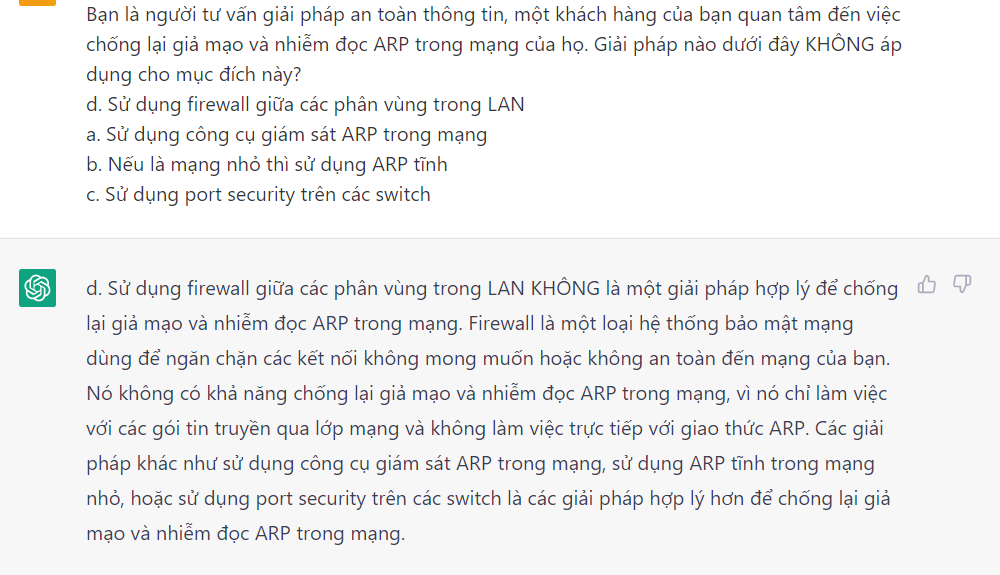
Bạn là người tư vấn giải pháp an toàn thông tin, một khách hàng của bạn quan tâm đến việc chống lại giả mạo và nhiễm đọc ARP trong mạng của họ. Giải pháp nào dưới đây KHÔNG áp dụng cho mục đích này?

Graphical user interface, text

Description automatically generated

D  


Tại sao các nhà phát triển phầm mềm đính kèm theo các giá trị băm bằng hàm MD5 của các gói cập nhật cho phần mềm cùng với các gói đó để các khách hàng của họ có thể download từ Internet?

(Khách hàng có thể xác thực tính toàn vẹn của gói cập nhật cho phần mềm sau khi download về)

Text

Description automatically generated

Một kiểu tấn công DoS sử dụng cơ chế bắt tay ba bước (three-way handshake) của TCP là? (SYN Flood)

Graphical user interface, text

Description automatically generated

Công cụ nào dưới đây có thể dùng để xác định các kết nối mạng đang có trên máy tính? (Netstat)

Graphical user interface, text

Description automatically generated

Một quản trị mạng mới thay thế hub bằng switch. Khi sử dụng phần mềm Sniffer bắt các gói tin trên mạng, người quản trị thấy được dữ liệu trao đổi giữa máy tính của anh ta và máy chủ, nhưng không thấy được các trao đổi giữa những máy khác nhau trong mạng với máy chủ. Coi như switch hoạt động tốt, điều gì đó đã tạo ra hiện tượng trên. (a)

Graphical user interface, text, application, email

Description automatically generated

Khái niệm bảo mật nào khuyến khích quản trị viên cài đặt tường lửa, chương trình quét phần mềm đọc hại (malware scanner) và IDS trên các host? (Endpoint security)

Graphical user interface, text

Description automatically generated

Email Server nên được đặt ở vùng mạng nào? **(d. DMZ)**

Graphical user interface, text, application

Description automatically generated

Máy chủ web của một công ty được cấu hình những dịch vụ sau: HTTP, SSI, FTP, SMTP. Máy chủ này được đặt trong vùng DMZ. Đâu là những cổng cần phải mở trên tường lửa để cho phép các máy trạm có thể sử dụng dịch vụ trên máy này? (80, 20, 21, 25, 443)

Text

Description automatically generated

Loại malware nào sau đây có thể ẩn các tiến trình và các tập tin trên hệ thống? **(Rookit)**

Graphical user interface, text

Description automatically generated

Kiểu tấn công nào sau đây không phải kiểu tấn công từ chối dịch vụ? a. MITM

Graphical user interface, text, application

Description automatically generated

Muốn thay thế telnet với một giao thức an toàn hơn để quản lý các thiệt bị mạng, ta cần sử dụng giao thức nào sau đây? **(SSH)**

Graphical user interface, text

Description automatically generated

Phát biểu nào sau đây không đúng về vùng DMZ? **(c)**

Graphical user interface, text, application

Description automatically generated

Thuật toán nào dưới đây không phải là một thuật toán mã hoá khối? **(RC4)**

Graphical user interface, text, application

Description automatically generated

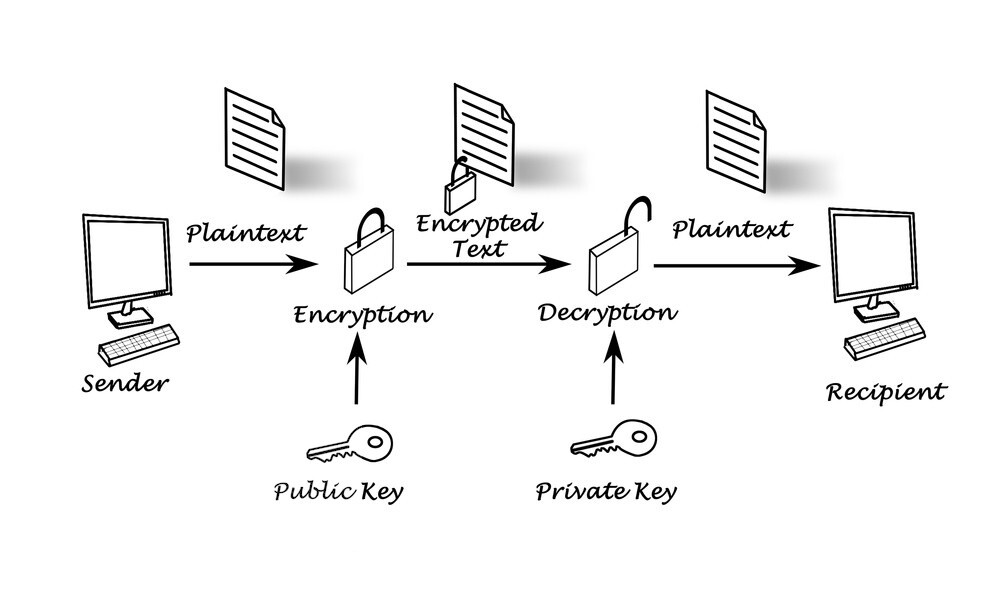
Mã hóa khối: AES, DES, 3DES

Mã hóa dòng: RC4

Trong mật mã khoá công khai (PKI), để xác nhận mình là người gửi thông tin, người gửi sẽ sử dụng khoá nào? **(Public key)**

Graphical user interface, text

Description automatically generated



Mặc dù báo cáo quét lỗ hổng cho thấy không có lỗ hổng nào được phát hiện, nhưng một cuộc kiểm tra thâm nhập tiếp theo cho thấy có các lỗ hổng trên mạng. Thuật ngữ nào sau đây mô tả cho trường hợp này? **(c. False negative)**

Graphical user interface, application

Description automatically generated with medium confidence

Giao thức nào sau đây thuộc mã khoá công khai? **(RSA)**

Graphical user interface

Description automatically generated

Kiểu tấn công nào sau đây không phải khai thác các lỗ hổng của ứng dụng Web? **(Social Engineering)**

Graphical user interface, text, application

Description automatically generated

Quản trị viên bảo mật thiết lập một AP mới nhưng nhận ra quá nhiều người bên ngoài có thế kết nối AP đó và truy cập trái phép. Các cách nào sau đây sẽ là cách TỐT NHẤT để giảm thiểu vấn đề này?

(Disable SSID broadcast + MAC filtering)

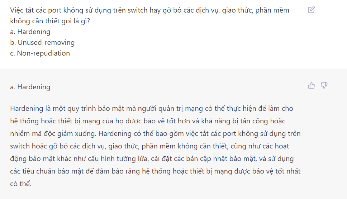
Text

Description automatically generated

Việc tắt các port không sử dụng trên switch hay gỡ bỏ các dịch vụ, giao thức, phần mềm không cần thiết gọi là gì? (Hardening)

Graphical user interface, application

Description automatically generated



Hệ thống IDS/IPS phát hiện xâm nhập dựa vào các kỹ thuật nào sau đây? **(A, B)**

Graphical user interface, text, application

Description automatically generated