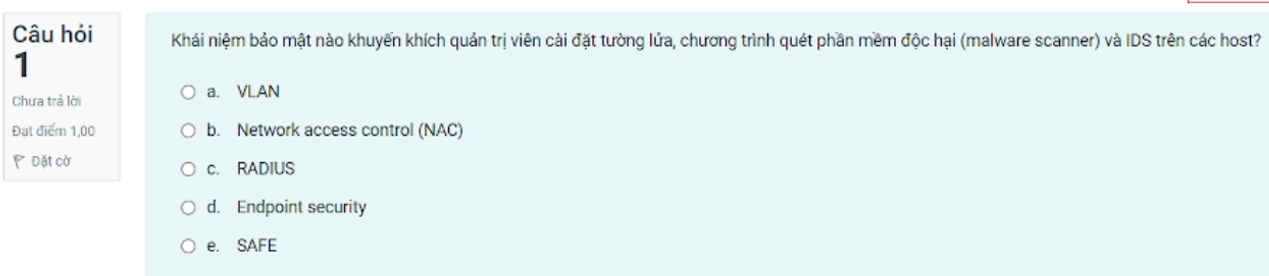
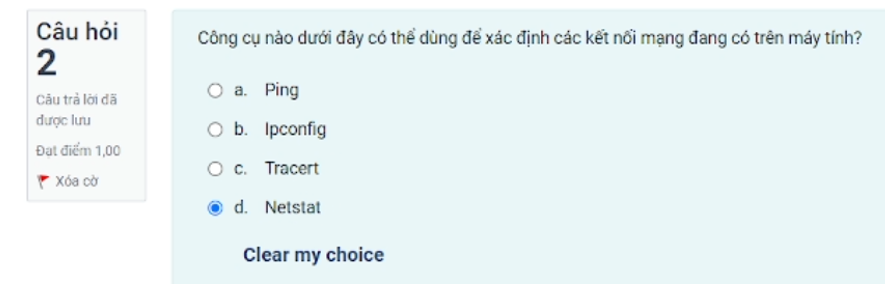
1. Khái niệm bảo mật nào khuyến khích quản trị viên đặt tường lửa, chương trình quét phần mềm độc hại và IDS trên các host?

B. Network access control(NAC)



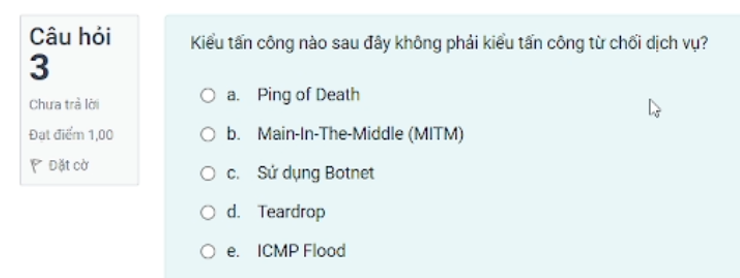
2. Công cụ nào dưới đây có thể dùng để xác định các kết nối mạng đang có trên máy tính?

D. Netstat



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

B. Main-In-The-Middle



4. Kiểu tấn công nào sau đây **không** phải khai thác các lỗ hổng của ứng dụng Web?

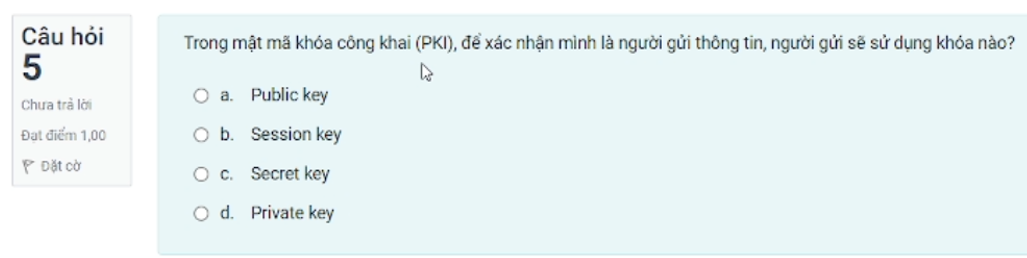
C. Social Engineering



5. Trong mật mã khóa công khai (PKI), để xác nhận mình là người gửi thông tin, người gửi sẽ sử dụng khóa nào?

A. Public key(Chưa chắc)

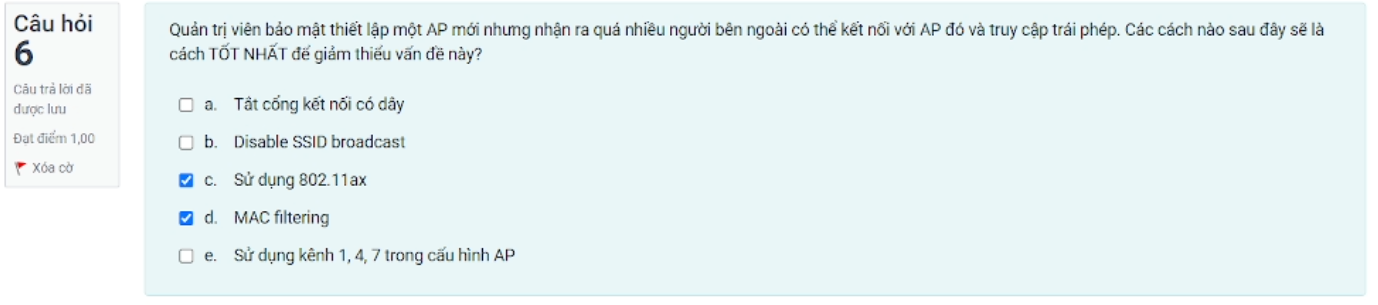
C. Secret key



6. Quản trị viên bảo mật thiết lập một AP mới

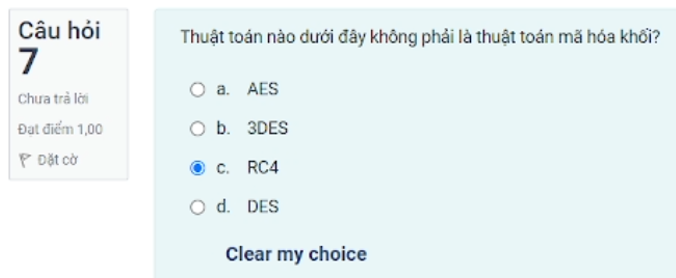
B. Disable SSID broadcast

D. MAC filtering



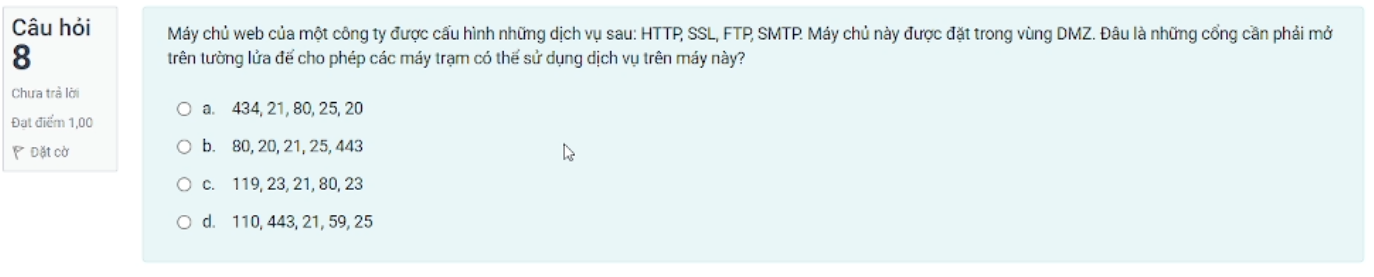
7. Thuật toán nào dưới đây **không phải** là thuật toán mã hóa khối?

C. RC4



8. Máy chủ web của một công ty được cấu hình nhữ dịch vụ sau:

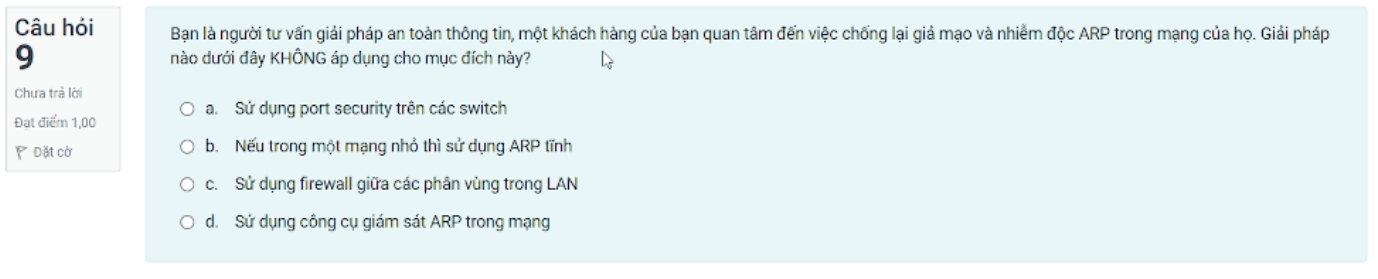
B. 80, 20, 21, 25, 443(Câu hỏi thiếu https)



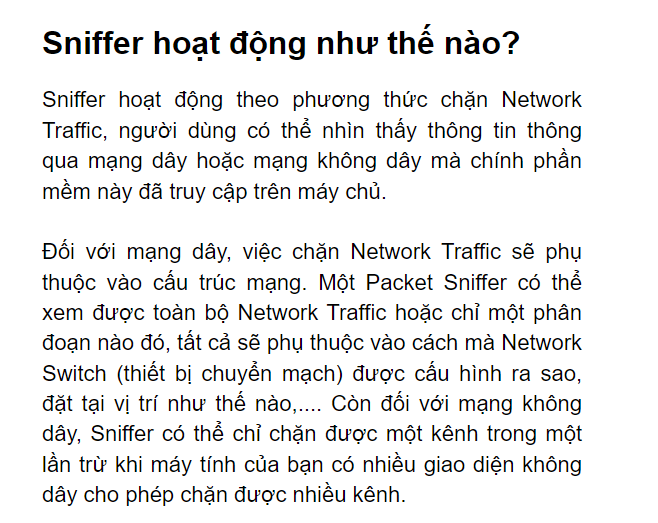
9. Bạn là người tư vấn giải pháp an toàn thông tin, một khách hàng của bạn

. Giải pháp nào dưới đây **KHÔNG** áp dụng cho mục đích này?

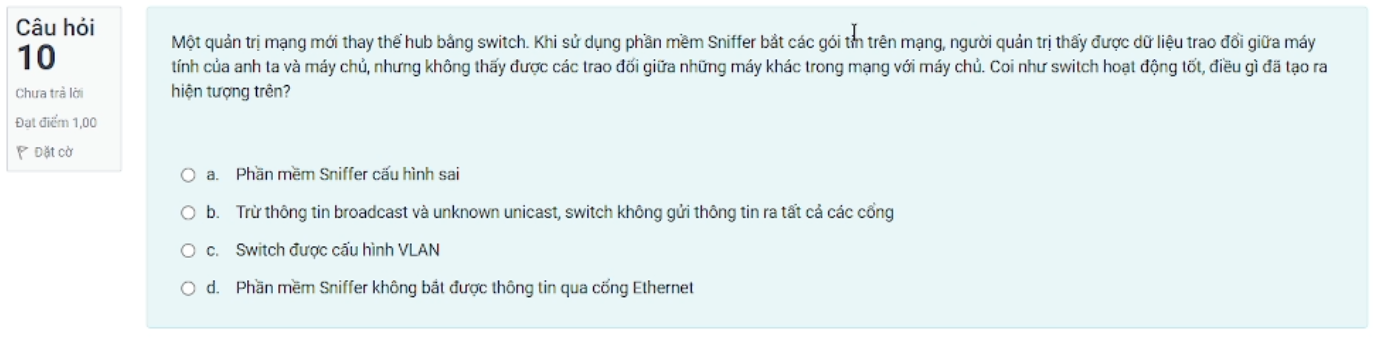
A. Sử dụng port security trên các switch



10. Một quản trị mạng mới thay thế hub bằng switch. Khi sử dụng phần mềm Sniffer

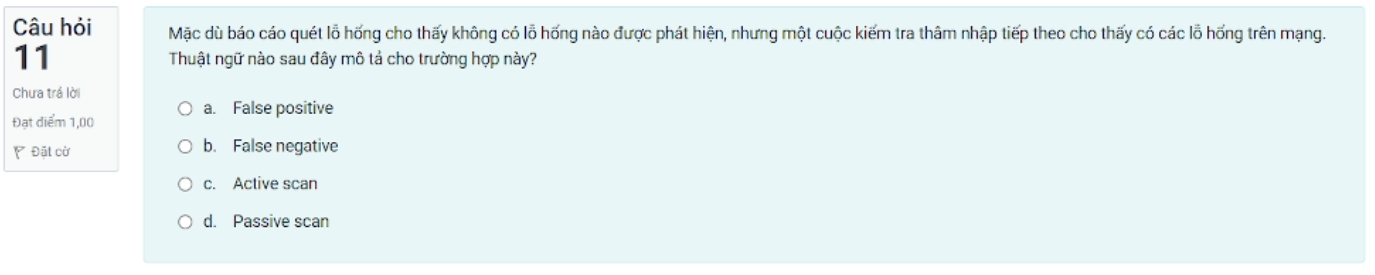


C. Switch được cấu hình VLAN



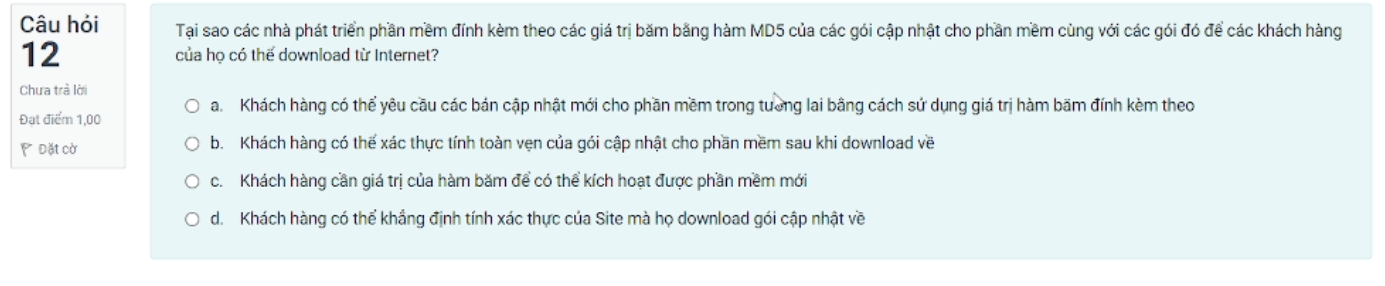
11. Mặc dù báo cáo quét lỗ hổng cho thấy không có lỗ hổng nào được phát hiện, nhưng một cuộc kiểm tra thâm nhập tiếp theo cho thấy có các lỗ hổng trên mạng

B. False negative



12. Tại sao các nhà phát triển phần mềm đính kèm theo các giá trị băm bằng hàm MD5 của các gói cập nhật cho phần mềm

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



13. Phát biểu nào **không đúng** về DMZ?

B. Chứa các server chỉ phục vụ cho người dùng bên trong

https://viblo.asia/p/tang-cuong-bao-ve-cho-he-thong-mang-noi-bo-su-dung-dmz-EoDGQOElkbV



14. Email Server **nên** được đặt ở vùng mạng nào?

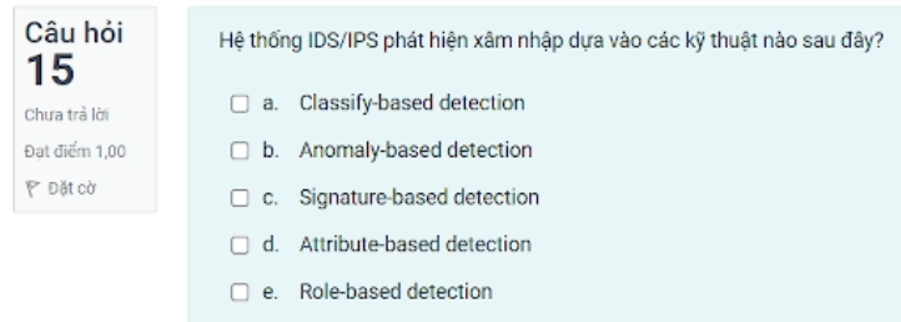
A. DMZ



15. Hệ thống IDS/IPS phát hiện xâm nhập dựa vào các kỹ thuật nào sau đây?

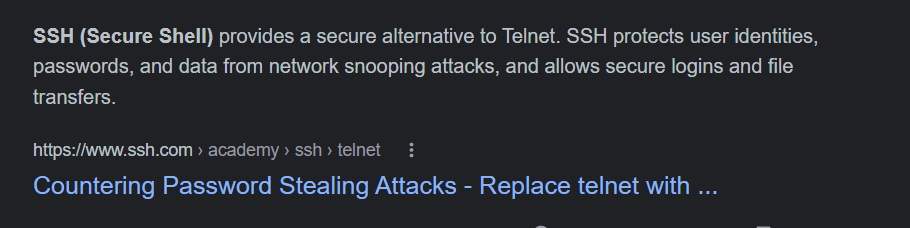
B. Anomaly based

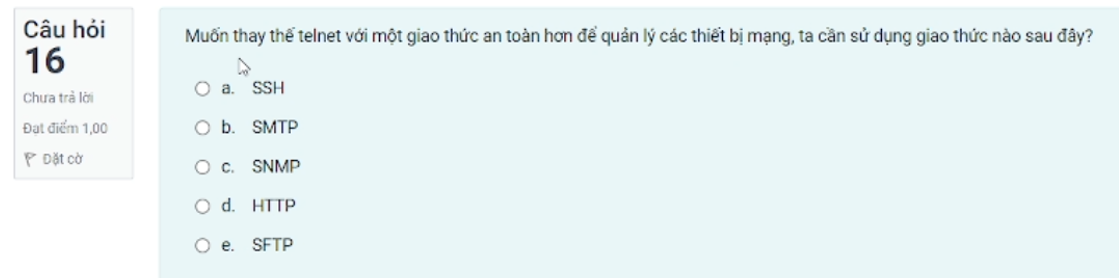
C. Signature based



16. Muốn thay thế telnet với một giao thức an toàn hơn đề quản lý các thiết bị mạng, ta cần sử dụng giao thức nào sau đây?

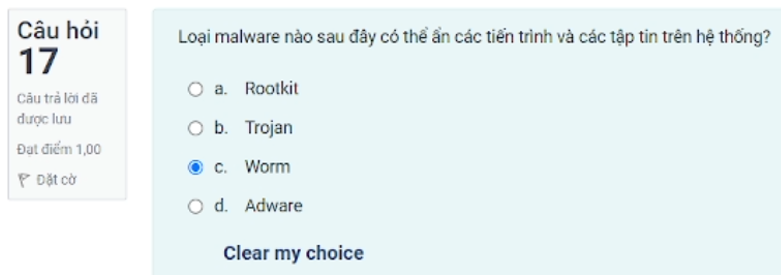
A. SSH





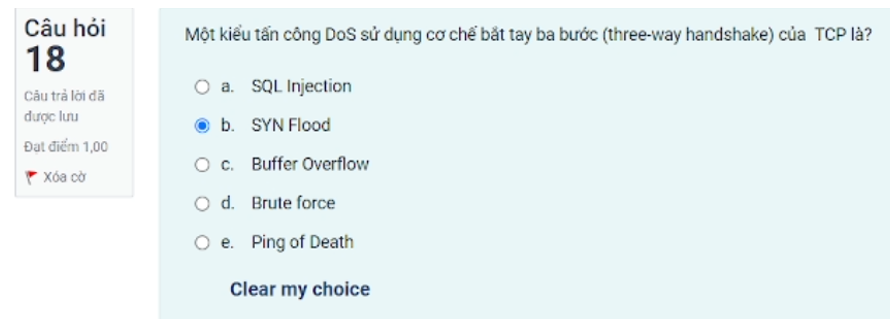
17. Loại malware nào sau đây có thể ấn các tiến trình và các tập tin trên hệ thống?

A. Rootkit



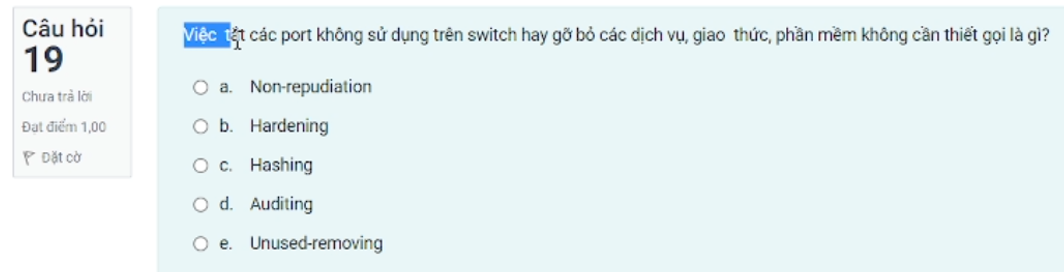
18. Một kiểu tấn công DoS sử dụng cơ chế bắt tay ba bước (three-way handshake) của TCP là?

B. SYN Flood



19. Việt tắt các port không sử dụng trên switch hay gỡ bỏ các dịch vụ, giao thức, phần mềm không cần thiết gọi là?

B. Hardening



20. Giao thức nào sau đây thuộc mã khóa công khai?

D. RSA

