Câu 2: Kẻ tấn công có thể sử dụng backdoor do rootkit tiết lộ để truy cập từ xa được không? Giải thích lý do tại sao và tại sao không

Trả lời:

Kẻ tấn công có thể sử dụng backdoor mà rootkit tiết lộ để truy cập từ xa bởi vì:

- Rootkit có khả cung cấp quyền root, khi kẻ tấn công sử dụng backdoor do rootkit tạo sẽ có quyền truy cập và kiểm soát toàn bộ hệ thống mà cần sự đồng ý hay nhận thức của người dùng

- Backdoor do rootkit tạo có thể được thiết lập như một cổng truy cập từ xa, cho phép kẻ tấn công kết nối và tương tác với hệ thống. Điều này giúp kẻ tấn công cài đặt các phần mềm độc hại khác hoặc truy cập một số dữ liệu.

- Rootkit thường có khả năng ản danh và xóa dấu vết hoạt động độc hại trên hệ thống, do đó gây khó khăn cho người dùng để phát hiện ra các hành động độc hại của kẻ tấn công

Tuy nhiên một số lưu ý có thể xảy ra như sau

- Kẻ tấn công cần phải khai thác được một số lỗ hổng phần mềm trên máy nạn nhân để có thể cài đặt được rootkit

- Các phần mềm giám sát và phát hiện được cài đặt và cấu hình an toàn, chính xác cao thì khả năng thành công của kẻ tấn công sẽ giảm.