**BÁO CÁO BÀI THỰC HÀNH SỐ 7**

**PHÂN TÍCH MỘT SỐ KỸ THUẬT THĂM DÒ MẠNG**

**Họ và tên sinh viên: Nguyễn Phương Sinh**

**MSSV: 1050080155**

**3.1. Phân tích một số kỹ thuật quét cổng ứng dụng của nmap**

**3.1.1. Kịch bản 1**

Thực hiện lệnh quét nmap –sn Dia\_chi\_mang/Mat\_na trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là task1.pcap.

A screenshot of a computer

AI-generated content may be incorrect.

Kỹ thuật quét sử dụng trong nmap -sn là: Ping Scan (Host Discovery) – dùng các gói ICMP Echo Request, hoặc ARP Request (nếu trong cùng mạng LAN), để phát hiện host nào đang hoạt động.

**3.1.2. Kịch bản 2**

Thực hiện lệnh quét nmap –sS –F Địa\_chỉ\_IP\_máy\_mục\_tiêu trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là task2.pcap.

A screenshot of a computer

AI-generated content may be incorrect.

Lệnh nmap -sS thực hiện quét cổng bằng cách:

* Gửi gói TCP SYN đến cổng của máy mục tiêu
* Nếu cổng mở, máy mục tiêu phản hồi bằng SYN-ACK
* Sau đó, Nmap không gửi ACK tiếp theo, nên không hoàn tất bắt tay TCP
* Điều này giúp ẩn mình hơn và tránh ghi log

Kỹ thuật này được gọi là: Half-open scan hoặc Stealth Scan

**3.1.3. Kịch bản 3**

Thực hiện lệnh quét nmap –sA –F Địa\_chỉ\_IP\_máy\_mục\_tiêu trên máy do thám. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì? Lưu lại file lưu lượng trên máy do thám với tên là task3.pcap.

A screenshot of a computer

AI-generated content may be incorrect.

Trong kịch bản này, Nmap sử dụng kỹ thuật TCP ACK Scan (-sA) để xác định trạng thái lọc tường lửa đối với các cổng. Cụ thể, Nmap gửi gói ACK đến các cổng phổ biến. Dựa vào phản hồi RST hoặc không có phản hồi, công cụ phân biệt được giữa cổng filtered và unfiltered. Phân tích trên Wireshark cho thấy nhiều gói TCP ACK được gửi đến máy mục tiêu, với phản hồi RST từ những cổng không bị lọc.

**3.2. Thu thập thông tin hệ thống**

Sử dụng nmap để xác định nút mạng trong mạng 192.168.100.0 /24 cung cấp dịch vụ email. Sử dụng nmap để quét, thu thập thông tin về hệ điều hành và các dịch vụ trên nút mạng này. Sử dụng Wireshark để bắt lưu trên máy do thám. Hãy cho biết thông tin các dịch vụ đang được cung cấp trên máy mục tiêu. Lưu lại file lưu lượng trên máy do thám với tên là task4.pcap.

A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Qua quá trình quét mạng 192.168.100.0/24, máy có IP 192.168.100.10 được phát hiện đang mở các cổng liên quan đến dịch vụ email (SMTP – port 25). Quét sâu bằng nmap -A cho thấy máy này chạy hệ điều hành Linux và cung cấp các dịch vụ như:

* SMTP (email) – port 25
* SSH – port 22
* HTTP – port 80 File lưu lượng bắt được bằng Wireshark đã được lưu lại với tên task4.pcap.