BÁO CÁO BÀI THỰC HÀNH SỐ 7

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

***Họ và tên sinh viên: Hoàng Hải Đăng***

***MSSV: 1050080258***

**KẾT QUẢ THỰC HÀNH**

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

Bước 1: Truy cập máy ảo

Bước 2: Ở terminal thứ nhất khởi động wireshark bằng lệnh $sudo wireshark

A screen shot of a computer

AI-generated content may be incorrect.

Sau khi nhập lệnh thì sẽ hiện ra wireshark

A screenshot of a computer

AI-generated content may be incorrect.

Bước 3: Ở terminal 2 sử dụng nmap để quét mạng với lệnh sau

Namp -sn 192.168.23.1/24

A screenshot of a computer

AI-generated content may be incorrect.

Bước 4: Sau khi quét mạng sẽ có kết quả như sau:

A screenshot of a computer screen

AI-generated content may be incorrect.

Có thể thấy ngoài địa chỉ 192.168.23.135 là địa chỉ của máy tấn công thì còn 2 nút mạng nữa đang hoạt động có địa chỉ là, 192.168.23.2 và 192.168.23.254

Bước 5: Dừng bắt những tập tin

**Phân tích lưu lượng**

Chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Có thể thấy rằng máy tấn

công đang gửi đi một loạt các gói tin ARP Request để tìm kiếm địa chỉ MAC của các máy tính trong mạng 192.168.23.1/24

A screenshot of a computer

AI-generated content may be incorrect.

- Trên cửa sổ của Wireshark, sử dụng giá trị **arp.opcode == 2** cho bộ lọc, chúng ta có thể thấy các gói tin ARP Reply được gửi lại từ các nút mạng đang hoạt động đã quan sát thấy ở trong kết quả quét mạng bằng công cụ nmap.

A screenshot of a computer

AI-generated content may be incorrect.

**Kết quả**: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan để phát hiện các nút mạng đang hoạt động trong mạng.

Lưu file lưu lượng trên máy do thám với tên là task1.pcap.

A screenshot of a computer

AI-generated content may be incorrect.

* 1. **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.

Bước 1: Truy cập máy ảo

Bước 2: Ở terminal 1 khởi động wireshark

Bước 3: Ở terminal 2 quét mạng máy mục tiêu với lệnh

nmap –sS –F 192.168.23.254

A screenshot of a computer

AI-generated content may be incorrect.

Bước 4: Sau khi chạy sẽ có kết quả như sau

A computer screen shot of a computer

AI-generated content may be incorrect.

Bước 5: Dừng bắt gói tin

A screenshot of a computer

AI-generated content may be incorrect.

* 1. **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.

Bước 1: Truy cập máy ảo

Bước 2: Ở terminal 1 khởi động wireshark

Bước 3: Ở terminal 2 quét mạng máy mục tiêu với lệnh

nmap –sA –F 192.168.23.254

A black background with white spots

AI-generated content may be incorrect.

Bước 4: Kết quả sau khi chạy

A computer screen shot of a computer program

AI-generated content may be incorrect.

Bước 5 dùng bắt gói tin

A screenshot of a computer

AI-generated content may be incorrect.

* 1. 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 cungcấp trên máy mục tiêu. Lưu lại file lưu lượng trên máy do thám với tên là task4.pcap.

Bước 1: Mở máy ảo

Bước 2: Ở terminal thứ nhất truy cập wireshark

Bước 3: Ở terminal thứ 2 nhập lệnh truy cập dịch vụ email

Sudo nmap -p 25 192.168.100.0/24

A screenshot of a computer

AI-generated content may be incorrect.

Bước 4:

A screenshot of a computer

AI-generated content may be incorrect.