Họ và tên: Chu Thắng

MSSV: 1050080242

Môn: Bảo mật mạng máy tính và hệ thống

Link youtube: https://youtu.be/tnC1zMz7UNw

Lab7

**Quét thăm dò mạng**

Bước 1: Truy cập máy ảo Kali

Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark: sudo wireshark

Chọn cạc mạng để bắt gói tin: eth0

A screenshot of a computer

AI-generated content may be incorrect.

Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

nmap –sn 192.168.146.0/24

Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có thể thấy kết quả tương tự

như sau:

A screenshot of a computer

AI-generated content may be incorrect.

Bước 5: Dừng bắt gói tin trên Wireshark

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.

**Quét thăm dò dịch vụ**

Bước 1: Truy cập máy ảo Kali

Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

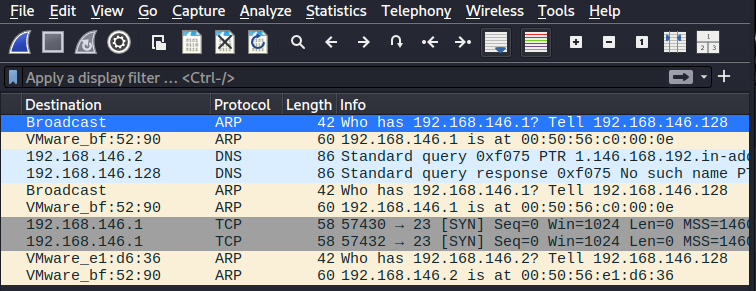
sudo nmap -p 23 192.168.146.1/24

Bước 4: Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.146.1 có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thểphán đoán rằng các máy này đang cung cấp dịch vụ Telnet.

A computer screen shot of a computer

AI-generated content may be incorrect.

Bước 5: Dừng bắt gói tin trên Wireshark



Tiếp tục quan sát lưu lượng mạng mà Wireshark phân tích, chúng ta thấy có các gói tin TCP

SYN được gửi tới cổng 23 của các máy đang hoạt động.



Trong bộ lọc gõ tcp

A screenshot of a computer

AI-generated content may be incorrect.

**Quét cổng dịch vụ**

Bước 1: Truy cập máy ảo Kali

Bước 2: Mở cửa sổ Terminal thứ 1 để khởi động Wireshark. Chọn cạc mạng để bắt gói tin.

Bước 3: Mở cửa sổ Terminal 2, sử dụng Nmap để quét mạng với lệnh sau:

nmap -sT 192.168.146.1

Bước 4: Sau khi nmap thực hiện xong quá trình quét mạng, ta có kết quả tương tự như dưới đây. Kết quả cho thấy các cổng dịch vụ 80, 135, 139, 445 trên máy mục tiêu 192.168.146.1 có trạng thái open.

A screen shot of a computer

AI-generated content may be incorrect.

Bước 5: Dừng bắt gói tin trên Wireshark

A screenshot of a computer

AI-generated content may be incorrect.

Từ bộ lọc gõ: tcp && ip.addr == 192.168.146.1

A screenshot of a computer

AI-generated content may be incorrect.

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 192.168.146.0/24 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? A screenshot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Kỹ thuật quét đã được sử dụng: arp

3.1.2. Kịch bản 2

Thực hiện lệnh quét nmap –sS –F 192.168.146.1. Dựa trênviệc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì?

A screenshot of a computer screen

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Kỹ thuật quét sử dụng: tcp syn

3.1.3. Kịch bản 3

Thực hiện lệnh quét nmap –sA –F 192.168.146.1. Dựa trên việc phân tích lưu lượng trên máy do thám, hãy cho biết kỹ thuật quét đã được sử dụng là gì?

A screen shot of a computer

AI-generated content may be incorrect.

A screenshot of a computer

AI-generated content may be incorrect.

Kỹ thuật quét sử dụng: tcp ack

3.2. Thu thập thông tin hệ thống

Sử dụng nmap để xác định nút mạng trong mạng 192.168.146.1 /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.

nmap -p 25,110,143 -sV 192.168.146.1

A screenshot of a computer

AI-generated content may be incorrect.