**Bài luyện tập số 1**

**PHÂN TÍCH MỘT SỐ KỸ THUẬT TẤN CÔNG DO THÁM MẠNG**

**TỔNG QUAN**

**Mục tiêu**

Trong thực tế, tấn công thăm dò là một trong những bước đầu tiên kẻ tấn công thực hiện để xác định được các điểm mà chúng có khả năng khai thác để tấn công xâm nhập. Việc hiểu biết các kỹ thuật tấn công này giúp chúng ta phát hiện sớm các dấu hiệu cho thấy có khả năng hệ thống sẽ bị tấn công trong tương lai. Bài luyện tập này được thiết kế để hướng dẫn học viên sử dụng các công cụ do thám mạng cũng như biết cách phân tích đặc điểm một số kỹ thuật do thám.

**Yêu cầu**

* Sử dụng công cụ Nmap để thực hiện tấn công do thám mạng
* Sử dụng công cụ Wireshark để phân tích lưu lượng tấn công, từ đó xác định được đặc điểm của những kỹ thuật tấn công.

**Môi trường thực hành**

* Phần mềm ảo hóa: Virtualbox
* Các máy ảo đã triển khai trên Virtualbox như hướng dẫn:
* Máy ảo Server: máy chủ mục tiêu
* Máy ảo Attack: máy thực hiện do thám sử dụng công cụ nmap
* Máy ảo User: máy trạm người dùng

A close up of a logo

Description automatically generated

**Kết quả cần đạt**

* Danh sách các nút mạng đang hoạt động
* Danh sách các dịch vụ mà Server đang cung cấp

**NỘI DUNG LUYỆN TẬP**

**1. Giới thiệu công cụ Nmap**

**1.1 Giới thiệu chung**

Nmap là công cụ quét cổng mã nguồn mở hoạt động trên cả Windows/Linux/Mac. Các tính năng chính:

* Host discovery – Xác định các máy (host) trong mạng. Chẳng hạn thông qua việc host có phản hồi gói tin TCP hoặc ICMP
* Port scanning – Liệt kê các cổng mở của một host
* Version detection – Xác định các dịch vụ hoạt động trên host, theo port và phiên bản của dịch vụ đấy
* OS detection – Xác định phiên bản hệ điều hành của host hoặc thiết bị mạng
* Hỗ trợ khả năng viết Script tương tác với mục tiêu thông qua Nmap Scripting Engine (NSE) và ngôn ngữ Lua.

Cú pháp cơ bản của nmap như sau:

**nmap option hostname**

Trong đó **hostname** là địa chỉ mục tiêu cần quét. Địa chỉ này có thể là tên miền, địa chỉ IP của một nút mạng hoặc địa chỉ IP của một mạng. Một số tùy chọn **option** phổ biến như

* + -p port\_number | port\_range : chỉ định cổng dịch vụ sẽ quét. Tùy chọn này cho phép thiết lập tham số là 1 hoặc nhiều số hiệu cổng ứng dụng
  + -F: quét 100 cổng phổ biến
  + -O: tìm thông tin HĐH
  + -sV: tìm thông tin dịch vụ đang chạy và phiên bản
  + -A: tìm thông tin dịch vụ
  + --script: quét theo kịch bản định sẵn(http-title, http-headers, http-enum)

**1.2. Các kỹ thuật quét mạng của Nmap**

Để quét và phát hiện các nút mạng đang có kết nối và hoạt động trên mạng, ta sử dụng lệnh sau

**nmap -sn Địa chỉ mạng mục tiêu**

Nmap sử dụng một số kỹ thuật quét tùy thuộc mạng mục tiêu:

* ICMP Ping Scan: Nmap gửi lần lượt các gói tin ICMP Echo Request tới tất cả các địa chỉ IP. Nếu có gói tin ICMP Echo Reply trả lại có địa chỉ nguồn là một địa chỉ IP nào đó, chứng tỏ có nút mạng sử dụng địa chỉ IP đó đang hoạt động. Để sử dụng kỹ thuật này, lệnh trên cần thực hiện ở quyền root. Kỹ thuật này được sử dụng khi quét mạng mục tiêu là mạng ở xa, mà nút mạng thực thi Nmap không nằm trong mạng đó.
* ARP Ping Scan: Nmap gửi quảng bá lần lượt các gói tin ARP Request để tìm kiếm thông tin địa chỉ MAC của tất cả các địa chỉ IP. Nếu có gói tin ARP Response trả lại cho biết thông tin địa chỉ MAC của một nút nào đó, chứng tỏ nút đó đang hoạt động. Kỹ thuật này được sử dụng để quét mạng cục bộ mà nút mạng thực thi Nmap đang nằm trong đó.
* TCP SYN Ping: Nmap gửi lần lượt các gói tin TCP SYN tới cổng 80 và 443 của tất cả các địa chỉ IP trong mạng cần quét. Nếu có gói tin TCP ACK hoặc TCP RST trả về từ một địa chỉ IP nào đó, chứng tỏ có nút mạng sử dụng địa chỉ IP đó đang hoạt động. Kỹ thuật này được sử dụng khi quét mạng mục tiêu là mạng ở xa, mà nút mạng thực thi Nmap không nằm trong mạng đó.

**1.3. Các** **kỹ thuật quét cổng ứng dụng**

Mục đích của các kỹ thuật quét cổng ứng dụng là để phát hiện các dịch vụ mạng nào đang hoạt động trên máy trạm. Giả sử, quá trình quét cổng cho kết quả cổng 80 đang mở(Open), chứng tỏ trên nút mạng đó đang cung cấp dịch vụ Web. Nmap cung cấp rất nhiểu kỹ thuật quét cổng, trong đó phổ biến và hữu dụng nhất là 2 kỹ thuật sau:

* TCP SYN Scan: Nmap gửi lần lượt các gói tin TCP SYN tới các cổng cần quét. Nếu quá trình quét cổng nhận được bất kỳ gói tin TCP SYN/ACK trả lời từ một cổng nào đó, chứng tỏ cổng đó đang ở trạng thái Open. Câu lệnh thực thi kỹ thuật này là:

**nmap -sS** **Địa\_chỉ\_IP\_máy\_mục\_tiêu**

* TCP Connection Scan: tương tự như TCP SYN Scan. Điểm khác biệt nhỏ là Nmap sẽ gửi lại gói tin ACK để hoàn tất quá trình thiết lập liên kết. Sau đó, Nmap gửi lại ngay các gói tin RST để hủy liên kết này. Câu lệnh thực thi kỹ thuật này là:

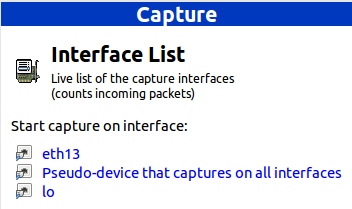
**nmap -sT** **Địa\_chỉ\_IP\_máy\_mục\_tiêu**

**2. Hướng dẫn thực hiện**

**2.1. Quét thăm dò mạng**

Trong phần này, chúng ta sẽ thực hiện kỹ thuật quét để phát hiện các nút đang hoạt động trên mạng.

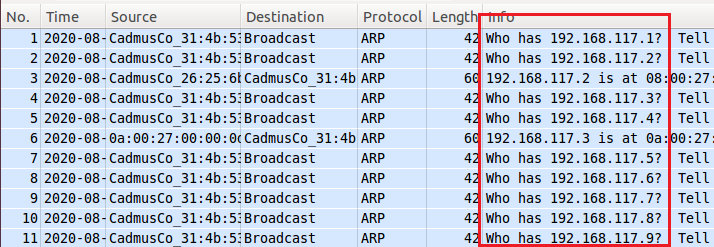
* Bước 1: [Attack] Bấm vào biểu tượng Ubuntu  ở góc trên màn hình và nhập Terminal. Chọn Terminal để mở cửa sổ dòng lệnh
* Bước 2: [Attack] Khởi động Wireshark bằng lệnh **sudo wireshark.** Bỏ qua cảnh báo nếu có.
* Bước 3: [Attack] Chọn cạc mạng eth13 trong danh sách cạc mạng.



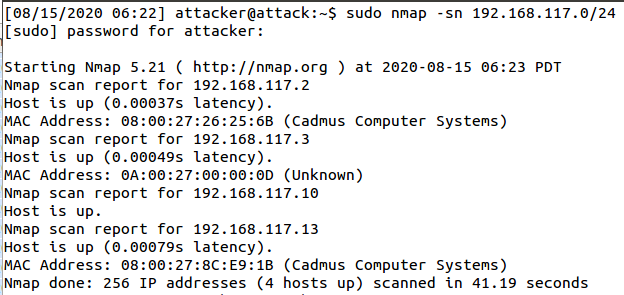
* Bước 4: [Attack] Mở cửa sổ dòng lệnh Terminal khác và thực hiện lệnh sau:

**sudo nmap -sn 192.168.117.0/24**

* Bước 5: [Attack] Trong khi câu lệnh trên được thực thi, 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 192.168.117.0/24

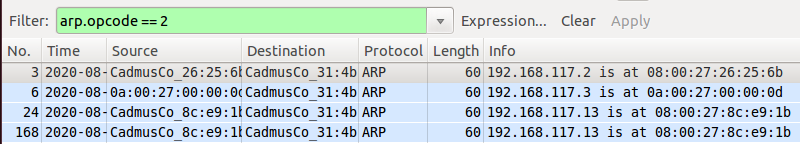


* Bước 6: [Attack] Khi câu lệnh quét mạng thực thi xong, chúng ta quan sát thấy danh sách địa chỉ IP của các nút mạng đang hoạt động tương tự hình minh họa sau:



Có thể thấy ngoài địa chỉ 192.168.117.10 là địa chỉ của máy tấn công thì còn 3 nút mạng nữa đang hoạt động có địa chỉ là 192.168.117.2, 192.168.117.3 và 192.168.117.13

* Bước 7: [Attack] 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.



***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.*

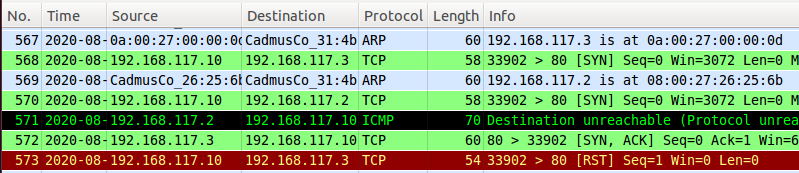
**2.2. Quét thăm dò dịch vụ trong mạng**

Trong phần này, chúng ta sẽ thực hiện kịch bản quét thăm dò để xác định các nút mạng đang cung cấp dịch vụ Web (số hiệu cổng ứng dụng là 80).

* Bước 1: [Attack] Trên cửa sổ Terminal, thực hiện lệnh sau:

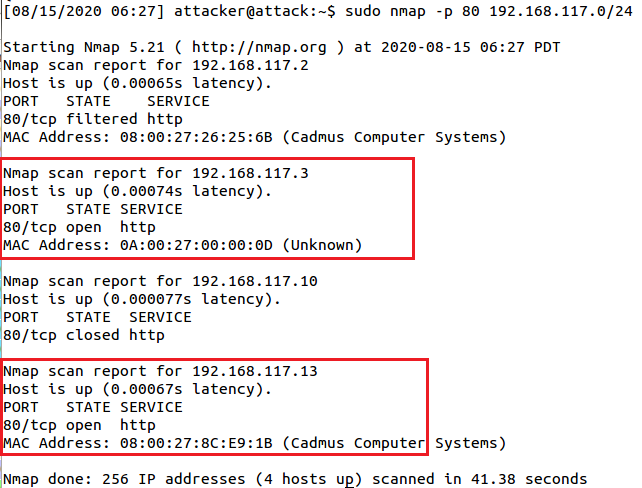
**sudo nmap -p 80 192.168.117.0/24**

* Bước 2: [Attack] Trong khi câu lệnh trên được thực thi, chúng ta quan sát màn hình phân tích lưu lượng trên Wireshark. Tương tự kịch bản trên, 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 192.168.117.0/24.
* Bước 3: [Attack] Tiếp tục quan sát lưu lượng mạng trên máy tấn công mà Wireshark đang phân tích, chúng ta thấy có các gói tin TCP SYN được gửi tới cổng 80 của các máy đang hoạt động.





* Bước 4: [Attack] Trên cửa sổ Command Prompt, chúng ta có thể thấy kết quả quét của Nmap cho biết máy có địa chỉ 192.168.117.3 và 192.168.117.13 đang có cổng 80 ở trạng thái **open**. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Web.



* Bước 5: [Attack] Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 80 của máy 192.168.117.3 và 192.168.117.13 về máy tấn công (nút mạng 192.168.117.2 gửi gói tin ICMP báo lỗi cho thấy cổng 80 trên nút mạng này không mở). Như vậy, điều này là phù hợp với kết quả của Nmap đã trả về.

***Kết quả****: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.*

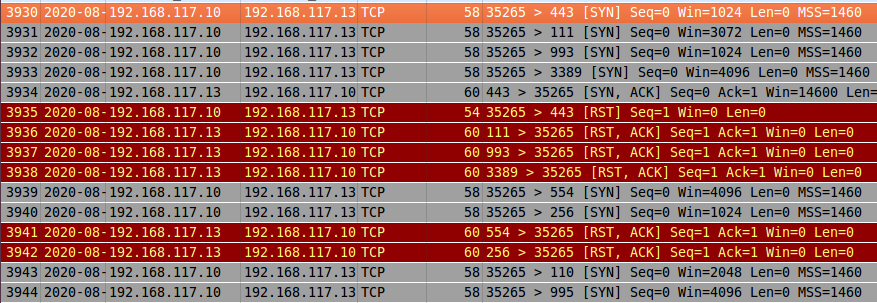
**2.3.** **Quét thăm dò dịch vụ của máy chủ**

Trong kịch bản này, chúng ta sẽ dùng Nmap để xác định máy chủ 192.168.117.13 ở phần trên còn cung cấp dịch vụ mạng nào khác ngoài dịch vụ Web.

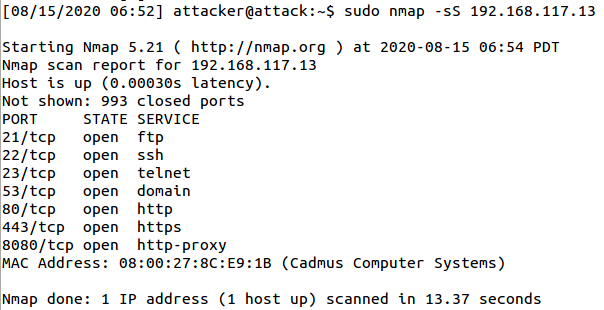
* Bước 1: [Attack] Trên cửa sổ Command Prompt của Windows, thực hiện lệnh sau:

**nmap -sS 192.168.117.13**

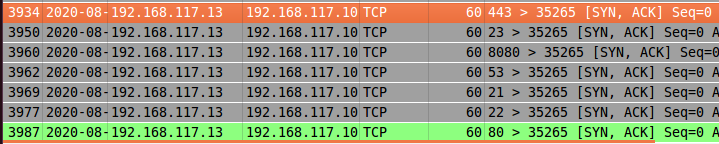
* Bước 2: [Attack] Quan sát lưu lượng trên cửa sổ của Wireshark, chúng ta thấy có rất nhiều gói tin TCP SYN gửi đi từ máy tấn công tới các cổng dịch vụ khác nhau của máy mục tiêu



* Bước 3: [Attack] Quan sát kết quả của Nmap, chúng ta thấy danh sách các cổng dịch vụ có trạng thái **open.** Điều này cho thấy có thể các dịch vụ đang được cung cấp trên máy chủ gồm là FTP, SSH, Telnet, DNS và Web.



* Bước 4[Attack]: Trên cửa sổ của Wireshark, sử dụng giá trị **tcp.flags == 0x012** để lọc, ta có thể thấy có các gói tin TCP ACK/SYN được gửi từ máy chủ mục tiêu. Các cổng dịch vụ gửi gói tin này là 21, 22, 23, 53, 80, 443, 8080 tương ứng với kết quả mà Nmap đã trả về.



***Kết quả****: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật TCP SYN Scan để phát hiện các dịch vụ đang được cung cấp trên máy chủ mục tiêu.*

**Kết luận**

Các bạn đã thực hiện một số kịch bản tấn công do thám bằng công cụ Nmap để thu thập thông tin của hệ thống. Bên cạnh đó, chúng ta cũng đã xác định được đặc điểm của các kỹ thuật do thám đã sử dụng trong kịch bản tấn công. Sau khi thực hiện bài này, các bạn đã tích lũy thêm kỹ năng để thực hiện bài tập lớn Assignment 1.