BÀI THỰC HÀNH SỐ 1

PHÂN TÍCH CÁC KỸ THUẬT DO THÁM HỆ THỐNG

Mục đích:

Do thám và thu thập thông tin hệ thống là giai đoạn đầu tiên khi tin tặc muốn tấn công vào hệ thống. Do đó, việc phân tích các kỹ thuật do thám cho phép người quản trị có sự hiểu biết và nhận diện được tình trạng hệ thống bị thăm dò, từ đó có thể đưa ra các phương án đề phòng, sẵn sàng phản ứng với các giai đoạn tiếp theo. Mặt khác, quản trị viên cũng cần sử dụng thành thạo các kỹ thuật này để phục vụ cho các tác vụ kiểm thử xâm nhập, phát hiện lỗ hổng và đánh giá rủi ro cho hệ thống.

Môi trường thực hành:

- Hệ điều hành: Kali Linux hoặc Ubuntu
- Các công cụ: Nmap, Wireshark

Các công việc cần chuẩn bị:

- Đọc tài liệu thực hành và thực hiện các nội dung luyện tập tại nhà để làm quen với công cụ
- Tìm hiểu cách thức thu thập thông tin hệ thống của nmap:
  https://nmap.org/book/vscan-technique.html
- Tìm hiểu về CVE List:

  https://www.cvedetails.com/

  https://cve.mitre.org/cve

1. Giới thiệu công cụ nmap

Nmap là công cụ quét thăm dò mạng 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.

Ngoài ra Nmap cung cấp nhiều khả năng khác như tìm DNS, kiểu thiết bị, và địa chỉ MAC.
Trên hệ điều hành Kali Linux, nmap đã được cài đặt sẵn.
Đối với hệ điều hành Ubuntu, nmap có thể được cài đặt bằng câu lệnh sau

```
$sudo apt-get install nmap
```

Cú pháp cơ bản của nmap như sau:

```
$nmap option hostname
```

Trong đó các tùy chọn option có thể là

- -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)
- -p ***port_number***: : chỉ định cổng dịch vụ sẽ quét là ***port_number***
- -p ***start end***: chỉ định cổng dịch vụ sẽ quét từ ***start*** đến ***end***
- -F: quét 100 cổng phổ biến

Tham khảo thêm các lệnh quét của Nmap ở địa chỉ sau:

- https://highon.coffee/blog/nmap-cheat-sheet/
- https://hackertarget.com/nmap-cheatsheet-a-quick-reference-guide/
- https://www.tecmint.com/nmap-command-examples/

1.1. Các kỹ thuật quét mạng của Nmap

Để quét và phát hiện các nút mạng đang có kết nối và hoạt động trên mạng, Nmap sử dụng 2 kỹ thuật quét:

- 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
- 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
- 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.

1.2. 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 các kỹ thuật quét cổng 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
- 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.
- TCP Null Scan: Nmap gửi lần lượt các gói tin TCP có giá trị Flags trong tiêu đề là NULL tới các cổng cần quét. Nếu nhận được gói tin TCP RST trả lại từ bất kỳ cổng nào, chứng tỏ công đó

đang ở trạng thái đóng (Close). Tuy nhiên, hiện tại hầu hết các hệ điều hành đã ngăn chặn được kỹ thuật quét cổng này.

- TCP FIN Scan: Nmap gửi lần lượt các gói tin TCP có giá trị Flags trong tiêu đề là FIN tới các cổng cần quét. Nếu nhận được gói tin TCP RST trả lại từ bất kỳ cổng nào, chứng tỏ công đó đang ở trạng thái đóng (Close). Tuy nhiên, hiện tại hầu hết các hệ điều hành đã ngăn chặn được kỹ thuật quét cổng này.
- TCP Xmas Scan: Nmap gửi lần lượt các gói tin TCP có giá trị Flags trong tiêu đề là FIN, PSH, và URG tới các cổng cần quét. Nếu nhận được gói tin TCP RST trả lại từ bất kỳ cổng nào, chứng tỏ cổng đó đang ở trạng thái đóng (Close). Tuy nhiên, hiện tại hầu hết các hệ điều hành đã ngăn chặn được kỹ thuật quét cổng này.
- TCP ACK Scan: Kỹ thuật này được sử dụng để phát hiện trên mục tiêu có sử dụng firewall hay không. Nmap gửi lần lượt các gói tin TCP có giá trị Flags trong tiêu đề là ACK tới các cổng cần quét. Nếu nhận được gói tin TCP RST trả lại từ bất kỳ cổng nào, chứng tỏ mục tiêu có thể đã được bảo vệ bởi firewall.

1.3. Quét thu thập thông tin hệ thống

Nmap có khả năng xác định được các thông tin về hệ thống mục tiêu như phiên bản hệ điều hành hay phần mềm dịch vụ. Để thực hiện điều này, Nmap gửi các yêu cầu truy cập tới các cổng dịch vụ đang mở trên máy mục tiêu và thu thập thông tin từ thông điệp phản hồi. Thông tin này được so sánh với các bộ dấu hiêu đặc trưng mà Nmap đã có về những hệ điều hành và phần mềm phổ biến. Dựa trên dữ kiện so sánh, Nmap phán đoán được thông tin về phiên bản hệ điều hành và phần mềm dịch vụ.

Có 2 cách thức để thực hiện hoạt động quét và thu thập:

- Cách 1: **nmap -sV -O Địa_chỉ_máy_mục_tiêu**

- Cách 2: **nmap -A Địa_chỉ_máy_mục_tiêu**

2. Luyện tập tại nhà

Triển khai môi trường thực hành theo hướng dẫn.

2.1. Quét thăm dò mạng

- **Bước 1:** Truy cập máy ảo Attack
- **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 –sn 192.168.117.0/24

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

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-09-19 09:52 EDT
Nmap scan report for 192.168.117.2
Host is up (-0.20s latency).
MAC Address: 08:00:27:8B:B7:FB (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.117.3
Host is up (-0.13s latency).
MAC Address: 0A:00:27:00:00:0C (Unknown)
Nmap scan report for 192.168.117.13
Host is up (-0.18s latency).
MAC Address: 08:00:27:44:38:B0 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.117.10
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 5.97 seconds
```

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

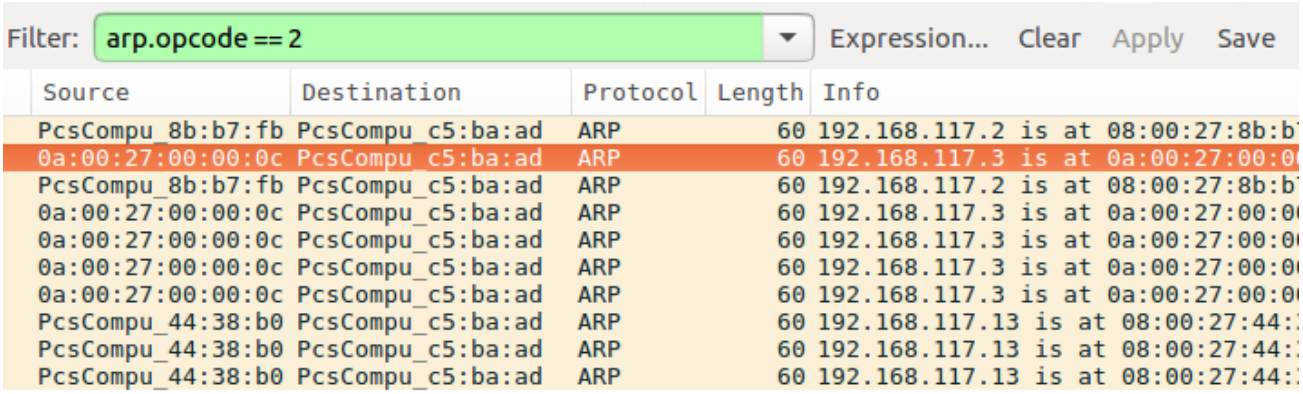
- **Bước 5:** Dừng bắt gói tin trên Wireshark

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 192.168.117.0/24

Source	Destination	Protocol	Length	Info
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.1? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.2? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.3? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.4? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.5? Tell
PcsCompu_8b:b7:fb	PcsCompu_c5:ba:ad	ARP	60	192.168.117.2 is at 08:00:27
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.6? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.7? Tell
0a:00:27:00:00:0c	PcsCompu_c5:ba:ad	ARP	60	192.168.117.3 is at 0a:00:27
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.8? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.9? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.11? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.1? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.2? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.3? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.4? Tell
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.5? Tell

- 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 phần này, chúng ta sẽ thực hiện kịch bản quét thăm dò để xác định các nút mạng đang cung cấp dịch vụ telnet (số hiệu cổng ứng dụng là 23).

- **Bước 1:** Truy cập máy ảo Attack
- **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 23 192.168.117.0/24

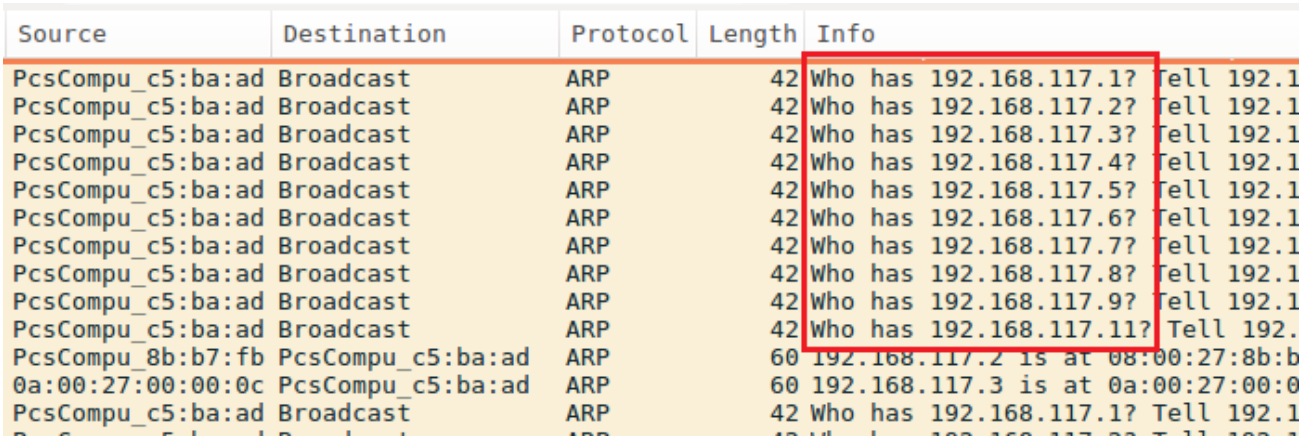
- **Bước 4:** Sau khi nmap thực hiện xong quá trình quét thăm dò, ta có thể thấy có các nút mạng 192.168.117.13 và 192.168.117.10 có trạng thái cổng dịch vụ 23 là open. Như vậy, ta có thể phán đoán rằng các máy này đang cung cấp dịch vụ Telnet.

```
Starting Nmap 7.01 ( https://nmap.org ) at 2020-09-19 05:48 EDT
Nmap scan report for 192.168.117.2
Host is up (-0.15s latency).
PORT    STATE    SERVICE
23/tcp filtered telnet
MAC Address: 08:00:27:8B:B7:FB (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.117.3
Host is up (-0.12s latency).
PORT    STATE  SERVICE
23/tcp closed telnet
MAC Address: 0A:00:27:00:00:0C (Unknown)

Nmap scan report for 192.168.117.13
Host is up (0.00091s latency).
PORT    STATE SERVICE
23/tcp open  telnet
MAC Address: 08:00:27:44:38:B0 (Oracle VirtualBox virtual NIC)

Nmap scan report for 192.168.117.10
Host is up (0.000052s latency).
PORT    STATE SERVICE
23/tcp open  telnet
```

- **Bước 5:** Dừng bắt gói tin trên Wireshark

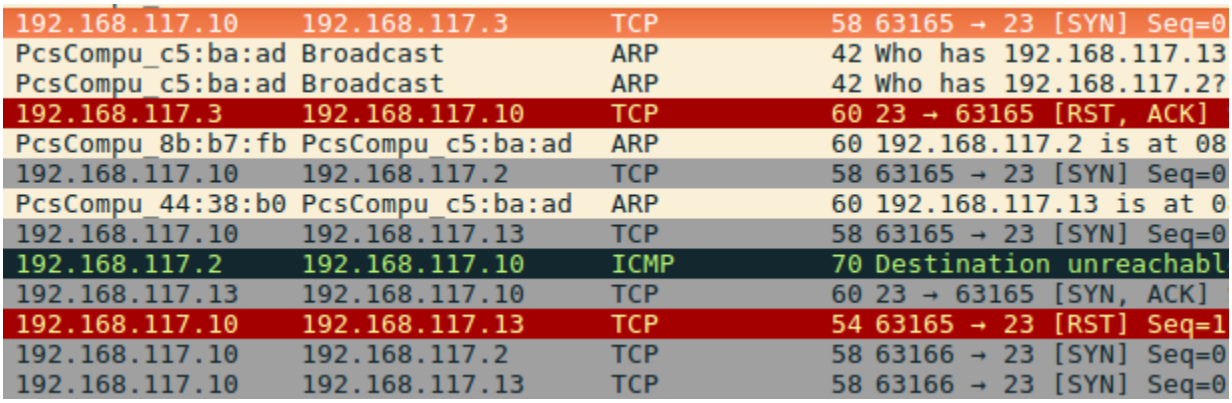
Phân tích lưu lượng:

- 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.



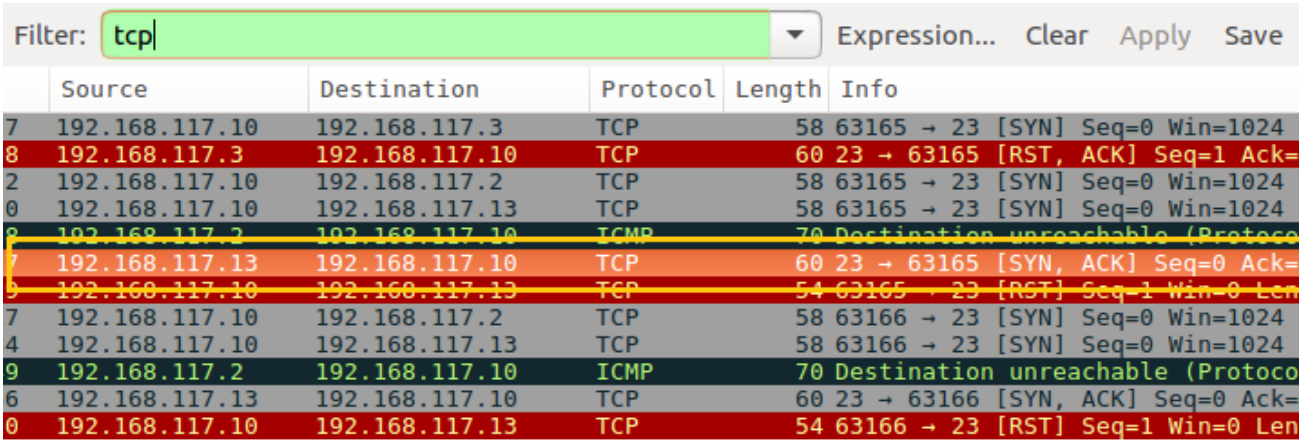
Source	Destination	Protocol	Length	Info
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.1? Tell 192.1
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.2? Tell 192.1
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.3? Tell 192.1
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.4? Tell 192.1
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.5? Tell 192.1
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.6? Tell 192.1
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.7? Tell 192.1
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.8? Tell 192.1
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.9? Tell 192.1
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.11? Tell 192.
PcsCompu_8b:b7:fb	PcsCompu_c5:ba:ad	ARP	60	192.168.117.2 is at 08:00:27:8b:b
0a:00:27:00:00:0c	PcsCompu_c5:ba:ad	ARP	60	192.168.117.3 is at 0a:00:27:00:0
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.1? Tell 192.1

- 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.



192.168.117.10	192.168.117.3	TCP	58 63165 → 23 [SYN] Seq=0
PcsCompu_c5:ba:ad	Broadcast	ARP	42 Who has 192.168.117.13
PcsCompu_c5:ba:ad	Broadcast	ARP	42 Who has 192.168.117.2?
192.168.117.3	192.168.117.10	TCP	60 23 → 63165 [RST, ACK]
PcsCompu_8b:b7:fb	PcsCompu_c5:ba:ad	ARP	60 192.168.117.2 is at 08
192.168.117.10	192.168.117.2	TCP	58 63165 → 23 [SYN] Seq=0
PcsCompu_44:38:b0	PcsCompu_c5:ba:ad	ARP	60 192.168.117.13 is at 0
192.168.117.10	192.168.117.13	TCP	58 63165 → 23 [SYN] Seq=0
192.168.117.2	192.168.117.10	ICMP	70 Destination unreachabl
192.168.117.13	192.168.117.10	TCP	60 23 → 63165 [SYN, ACK]
192.168.117.10	192.168.117.13	TCP	54 63165 → 23 [RST] Seq=1
192.168.117.10	192.168.117.2	TCP	58 63166 → 23 [SYN] Seq=0
192.168.117.10	192.168.117.13	TCP	58 63166 → 23 [SYN] Seq=0

- Nhập giá trị tcp vào bộ lọc. Trên kết quả phân tích lưu lượng của Wireshark chúng ta có thể thấy gói tin TCP SYN/ACK được gửi từ cổng 23 từ địa chỉ 192.168.117.13 về máy tấn công. Như vậy, điều này là phù hợp với kết quả của Nmap đã trả về (Địa chỉ 192.168.117.10 trong kết quả trả về là địa chỉ của chính máy tấn công vì máy này cũng cung cấp dịch vụ Telnet)



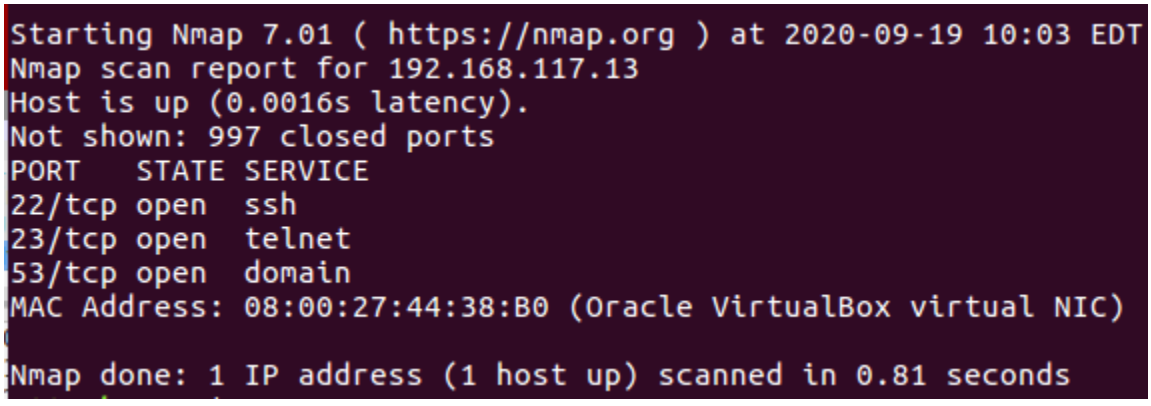
***Kết quả**: Như vậy, trong kịch bản vừa thực hiện, Nmap đã sử dụng kỹ thuật ARP Ping Scan và TCP SYN Scan để phát hiện các nút mạng cung cấp dịch vụ.*

2.3. Quét cổng dịch vụ

- **Bước 1:** Truy cập máy ảo Attack
- **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 192.168.117.13

- **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 22, 23, 53 trên máy mục tiêu 192.168.117.13 có trạng thái open. Ta có thể phán đoán máy này đang cung cấp các dịch vụ tương ứng là ssh, telnet và dns.

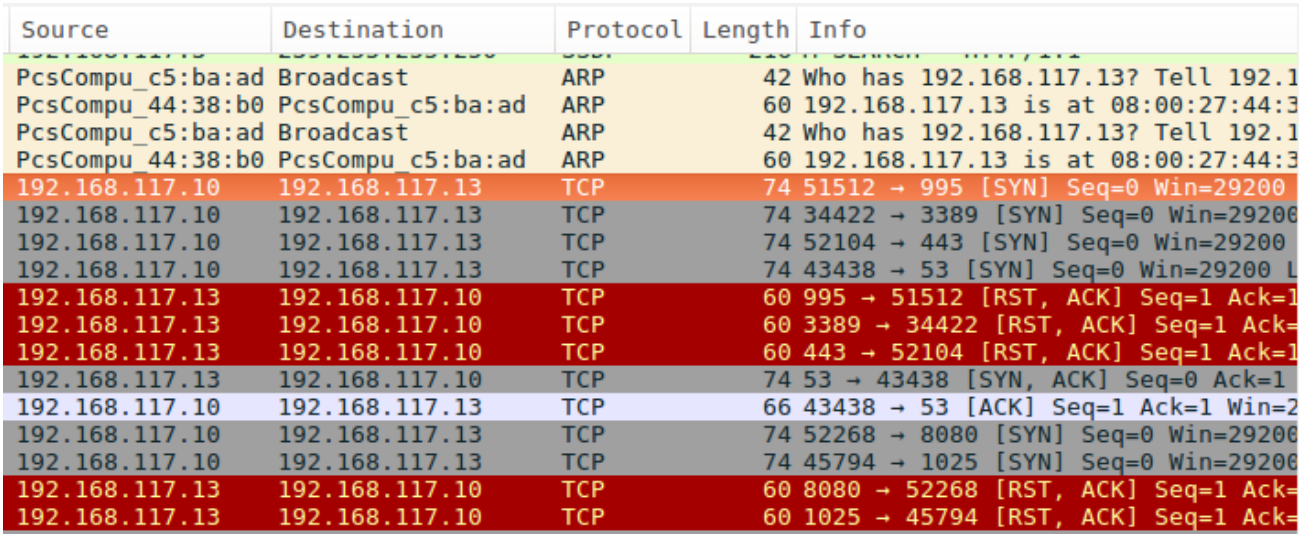


- **Bước 5:** Dừng bắt gói tin trên Wireshark

Phân tích lưu lượng:

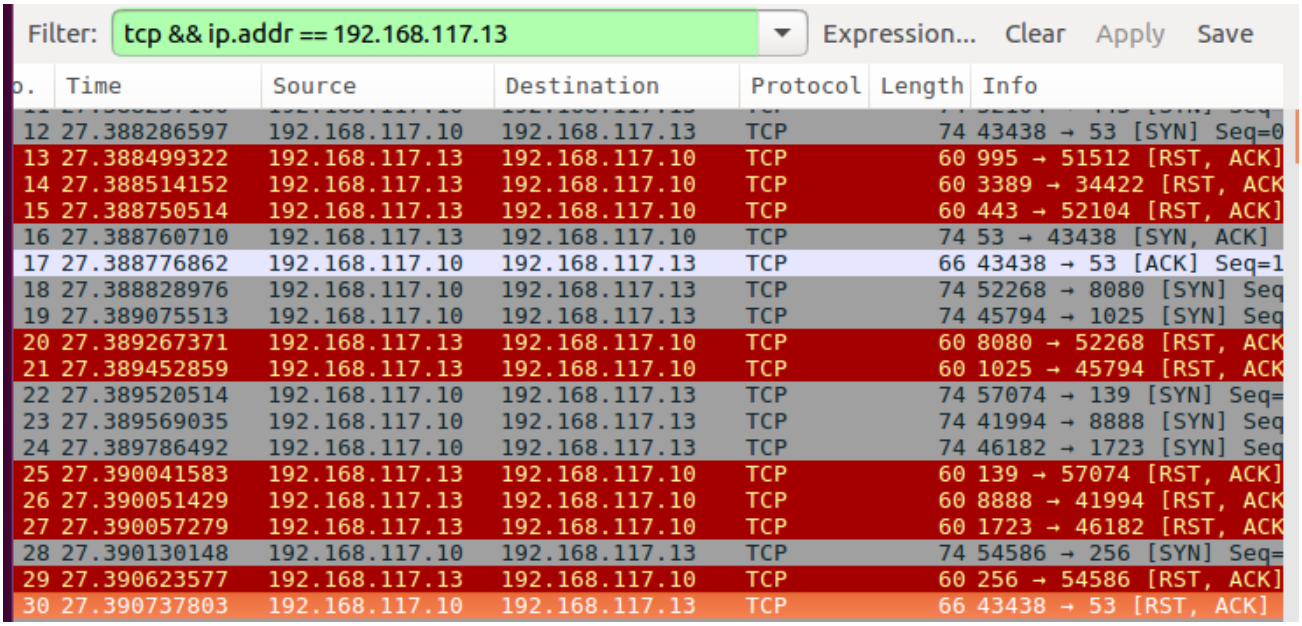
- Quan sát file lưu lượng ta thấy trước tiên máy tấn công gửi gói tin ARP Request để kiểm tra máy mục tiêu 192.168.117.13 có hoạt động hay không. Sau đó, ta thấy một lượng lớn các gói

tin TCP SYN được gửi từ máy tấn công (192.168.117.10) tới máy mục tiêu là 192.168.117.13. Các gói tin SYN này được gửi tới các cổng ứng dụng khác nhau.



Source	Destination	Protocol	Length	Info
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.13? Tell 192.1
PcsCompu_44:38:b0	PcsCompu_c5:ba:ad	ARP	60	192.168.117.13 is at 08:00:27:44:3
PcsCompu_c5:ba:ad	Broadcast	ARP	42	Who has 192.168.117.13? Tell 192.1
PcsCompu_44:38:b0	PcsCompu_c5:ba:ad	ARP	60	192.168.117.13 is at 08:00:27:44:3
192.168.117.10	192.168.117.13	TCP	74	51512 → 995 [SYN] Seq=0 Win=29200
192.168.117.10	192.168.117.13	TCP	74	34422 → 3389 [SYN] Seq=0 Win=29200
192.168.117.10	192.168.117.13	TCP	74	52104 → 443 [SYN] Seq=0 Win=29200
192.168.117.10	192.168.117.13	TCP	74	43438 → 53 [SYN] Seq=0 Win=29200 L
192.168.117.13	192.168.117.10	TCP	60	995 → 51512 [RST, ACK] Seq=1 Ack=1
192.168.117.13	192.168.117.10	TCP	60	3389 → 34422 [RST, ACK] Seq=1 Ack=
192.168.117.13	192.168.117.10	TCP	60	443 → 52104 [RST, ACK] Seq=1 Ack=1
192.168.117.13	192.168.117.10	TCP	74	53 → 43438 [SYN, ACK] Seq=0 Ack=1
192.168.117.10	192.168.117.13	TCP	66	43438 → 53 [ACK] Seq=1 Ack=1 Win=2
192.168.117.10	192.168.117.13	TCP	74	52268 → 8080 [SYN] Seq=0 Win=29200
192.168.117.10	192.168.117.13	TCP	74	45794 → 1025 [SYN] Seq=0 Win=29200
192.168.117.13	192.168.117.10	TCP	60	8080 → 52268 [RST, ACK] Seq=1 Ack=
192.168.117.13	192.168.117.10	TCP	60	1025 → 45794 [RST, ACK] Seq=1 Ack=

- Sử dụng giá trị **tcp && ip.addr == 192.168.117.13** ta lọc được các gói tin TCP. Có thể nhận thấy một liên kết tới cổng 53 đã được thiết lập (các gói tin 12, 16, 17 của quá trình bắt tay 3 bước) nhưng không có dữ liệu trao đổi. Thay vì vậy, máy tấn công gửi gói tin TCP RST(gói tin 30) để hủy kết nối này.



Filter: tcp && ip.addr == 192.168.117.13 Expression... Clear Apply Save

o.	Time	Source	Destination	Protocol	Length	Info
12	27.388286597	192.168.117.10	192.168.117.13	TCP	74	43438 → 53 [SYN] Seq=0
13	27.388499322	192.168.117.13	192.168.117.10	TCP	60	995 → 51512 [RST, ACK]
14	27.388514152	192.168.117.13	192.168.117.10	TCP	60	3389 → 34422 [RST, ACK
15	27.388750514	192.168.117.13	192.168.117.10	TCP	60	443 → 52104 [RST, ACK]
16	27.388760710	192.168.117.13	192.168.117.10	TCP	74	53 → 43438 [SYN, ACK]
17	27.388776862	192.168.117.10	192.168.117.13	TCP	66	43438 → 53 [ACK] Seq=1
18	27.388828976	192.168.117.10	192.168.117.13	TCP	74	52268 → 8080 [SYN] Seq
19	27.389075513	192.168.117.10	192.168.117.13	TCP	74	45794 → 1025 [SYN] Seq
20	27.389267371	192.168.117.13	192.168.117.10	TCP	60	8080 → 52268 [RST, ACK
21	27.389452859	192.168.117.13	192.168.117.10	TCP	60	1025 → 45794 [RST, ACK
22	27.389520514	192.168.117.10	192.168.117.13	TCP	74	57074 → 139 [SYN] Seq=
23	27.389569035	192.168.117.10	192.168.117.13	TCP	74	41994 → 8888 [SYN] Seq
24	27.389786492	192.168.117.10	192.168.117.13	TCP	74	46182 → 1723 [SYN] Seq
25	27.390041583	192.168.117.13	192.168.117.10	TCP	60	139 → 57074 [RST, ACK]
26	27.390051429	192.168.117.13	192.168.117.10	TCP	60	8888 → 41994 [RST, ACK
27	27.390057279	192.168.117.13	192.168.117.10	TCP	60	1723 → 46182 [RST, ACK
28	27.390130148	192.168.117.10	192.168.117.13	TCP	74	54586 → 256 [SYN] Seq=
29	27.390623577	192.168.117.13	192.168.117.10	TCP	60	256 → 54586 [RST, ACK]
30	27.390737803	192.168.117.10	192.168.117.13	TCP	66	43438 → 53 [RST, ACK]

Tiếp tục phân tích trên các cổng ứng dụng khác, ta thấy hiện tượng xảy ra tương tự với các cổng ứng dụng 22, 23. Điều này cho thấy máy do thám đã thực hiện hành vi quét cổng với kỹ thuật TCP Connection Scan

- Danh sách các cổng ứng dụng trên máy mục tiêu có thiết lập kết nối với máy do thám trùng khớp với kết quả trả về của lệnh quét nmap trên máy do thám.

3. Yêu cầu thực hành trên lớp

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**.

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**.

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**.

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.

3.3. Tìm kiếm thông tin về các lỗ hổng

Dựa vào kết quả quét ở phần 2, hãy lập báo cáo ngắn gọn về các lỗ hổng đã được công bố trên các phần mềm cung cấp dịch vụ. Thông tin về các lỗ hổng có thể tìm kiếm trên https://www.cvedetails.com/

Phần mềm dịch vụ (tên dịch vụ, tên phần mềm, phiên bản)	**Số CVE**	**Mô tả ngắn gọn về lỗ hổng**