**Nmap Live Host Discovery**

**Giới thiệu:**

Khi chúng ta muốn nhắm đến mạng, chúng ta muốn tìm 1 công cụ hiệu quả để giúp chúng ta xử lí các công việc lặp đi lặp lại, trả lời những câu hỏi sau:

* Hệ thống nào đang mở?
* Những dịch vụ nào đang chạy trên hệ thống đó?

Công cụ chúng ta sẽ dùng là Nmap.

Room này giải thích các bước mà Nmap thực hiện để khám phá những hệ thống đang trực tuyến trước khi scan cổng.

Chúng ta sẽ đi qua những cách tiếp cận khác nhau mà Nmap dùng để khám phá các máy chủ đang hoạt động.

1. ARP scan

2. ICMP scan

3. TCP/UDP ping scan: Loại scan này gửi gói tin đến cổng TCP và UDP để xác định máy chủ đang hoạt động

Nmap được tạo ra bởi Gordon Lyon (Fyodor), 1 chuyên gia bảo mật mạng và lập trình viên mã nguồn mở. Nó được phát hành năm 1997. Nmap là 1 công cụ để ánh xạ mạng, xác định máy chủ đang mở và khám phá những dịch vụ đang chạy. Công cụ viết kịch bản của Nmap có thể mở rộng thêm chức năng, từ việc theo dấu dịch vụ đến khám phá các lỗ hổng. Một lần quét Nmap thường trải qua các bước sau:



**Những mạng con:**

Phân đoạn mạng là một nhóm máy tính được kết nối bằng phương tiện chung.

Phương tiện đó có thể là Ethernet switch hoặc điểm truy cập Wifi. Trong 1 mạng IP, 1 mạng con tương đương với 1 hay nhiều phân đoạn mạng kết nối với nhau và được cấu hình dùng chung 1 router. Phân đoạn mạng đề cập đến 1 kết nối vật lý, trong khi mạng con đề cập đến 1 kết nối logic.

Trong sơ đồ mạng sau, chúng ta có 4 phân đoạn mạng hoặc những mạng con. Nhìn chung, hệ thống của bạn sẽ được kết nối đến 1 trong những phân đoạn mạng/mạng con. Một mạng con có địa chỉ IP riêng và được kết nối đến 1 mạng lưới rộng lớn hơn qua router. Có thể có tường lửa thực thi những chính sách bảo mật dựa trên mỗi mạng.



Hình trên cho thấy hai loại mạng con:

* Những mạng con với /16, có nghĩa là subnet mask (địa chỉ IP) có thể được viết là 255.255.0.0. Mạng con này có thể có khoảng 65 nghìn máy chủ.
* Những mạng con với /24, chỉ ra subnet mask có thể được viết là 255.255.255.0. Mạng con này có thể có khoảng 250 máy chủ.

Vì là 1 phần của active recon, chúng ta muốn khám phá thêm thông tin về nhóm các máy chủ hoặc 1 mạng con. Nếu bạn được kết nối chung mạng con, bạn sẽ mong đợi máy quét dựa vào các truy vấn ARP để khám phá máy chủ đang chạy. Một truy vấn ARP mục đích là lấy địa chỉ phần cứng (MAC) để mà giao tiếp qua lớp đường dẫn; tuy vậy chúng ta có thể dùng nó để chỉ ra máy chủ đang trực tuyến.

Nếu bạn đang ở mạng A, bạn có thể dùng ARP để khám phá các thiết bị trong mạng con đó (10.1.100.0/24). Giả sử bạn được kết nối với 1 mạng con khác với mạng con của một hệ thống mình nhắm đến. Trong trường hợp đó, tất cả những gói tin được tạo ra bởi máy quét của bạn sẽ được định tuyến qua cổng mặc định (router cha) để đi đến những hệ thống trên mạng con khác. Tuy nhiên những truy vấn ARP sẽ không được định tuyến và do đó không thể chạm được các định tuyến con. ARP là 1 giao thức lớp đường dẫn (lớp 2 trong OSI) và những gói tin ARP bị giới hạn trong mạng con của chúng.

**Liệt kê các mục tiêu:**

Chúng ta đã đề cập những kĩ thuật khác nhau chúng ta có thể dùng để quét ở Task 1. Trước khi chúng ta giải thích từng chi tiết và đưa nó vào mục tiêu trực tiếp, chúng ta cần xác định những mục tiêu chúng ta muốn quét.

* Danh sách: MACHINE\_IP scanme.nmap.org example.com sẽ scan 3 địa chỉ IP
* Phạm vi: 10.11.12.15-20 sẽ scan 6 địa chỉ IP: 10.11.12.15, 10.11.12.16,… và 10.11.12.20
* Mạng con: MACHINE\_IP/30 sẽ scan 4 địa chỉ IP

Bạn cũng có thể cung cấp 1 tập tin chứa danh sách các đối tượng

nmap -iL list\_of\_hosts.txt

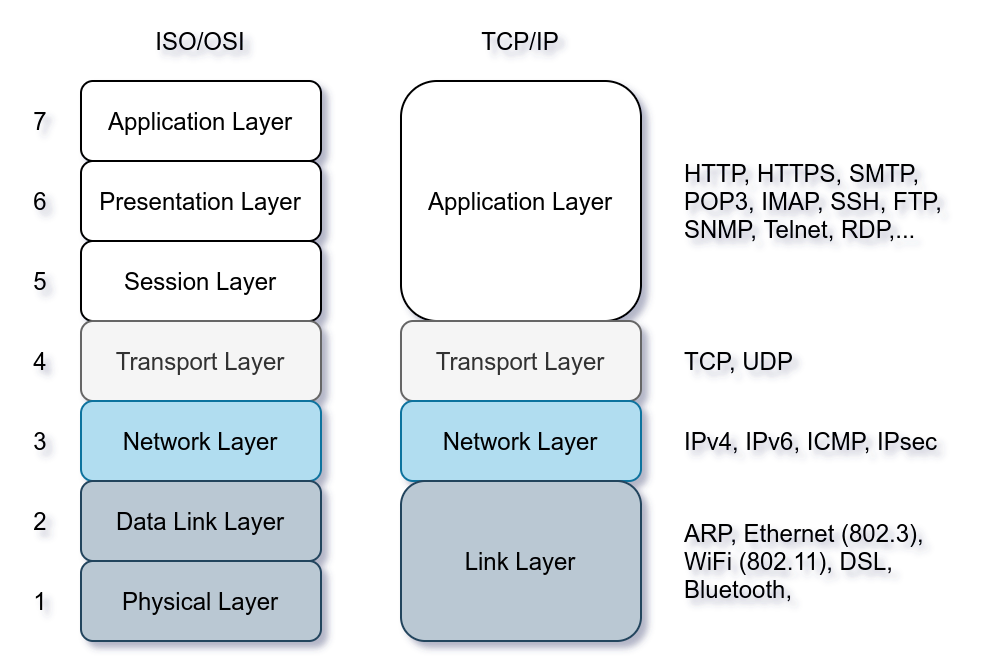
Nếu bạn muốn kiểm tra danh sách những máy chủ Nmap sẽ scan, bạn có thể sử dụng nmap -sL TARGETS.

Tuy nhiên Nmap sẽ cố gắng phân giải DNS ngược trên tất cả những đối tượng để nhận được các tên của chúng. Những cái tên này có thể chứa rất nhiều thông tin đối với kiểm thử viên (nếu bạn không muốn Nmap gửi đến máy chủ DNS, bạn có thể thêm -n)

**Khám phá những máy chủ đang hoạt động**

Cùng xem lại những lớp TCP/IP trong hình bên dưới. Chúng ta sẽ tận dụng những giao thức để khám phá những máy chủ đang hoạt động. Bắt đầu từ dưới lên trên, chúng ta có thể dùng

* ARP từ lớp đường dẫn
* ICMP từ lớp mạng
* TCP từ lớp vận chuyển
* UDP từ lớp vận chuyển



ARP có 1 mục đích: gửi frame đến phân đoạn mạng và yêu cầu máy tính có địa chỉ IP cụ thể phản hồi bằng việc cung cấp địa chỉ MAC của nó.

ICMP có rất nhiều loại. ICMP ping dùng Type 8 (Echo) và Type 0 (Echo Reply)

Nếu bạn muốn ping 1 hệ thống trong cùng mạng con, truy vấn ARP phải đi trước ICMP echo.

Mặc dù TCP và UDP là những lớp vận chuyển, nhưng với mục đích quét mạng, máy quét có thể gửi 1 gói tin đặc biệt đến những cổng TCP/UDP phổ biến để kiểm tra xem đối tượng có phản hồi không. Phương pháp này rất hiệu quả, đặc biệt khi ICMP echo bị chặn.

**Nmap Host Discovery Using ARP**

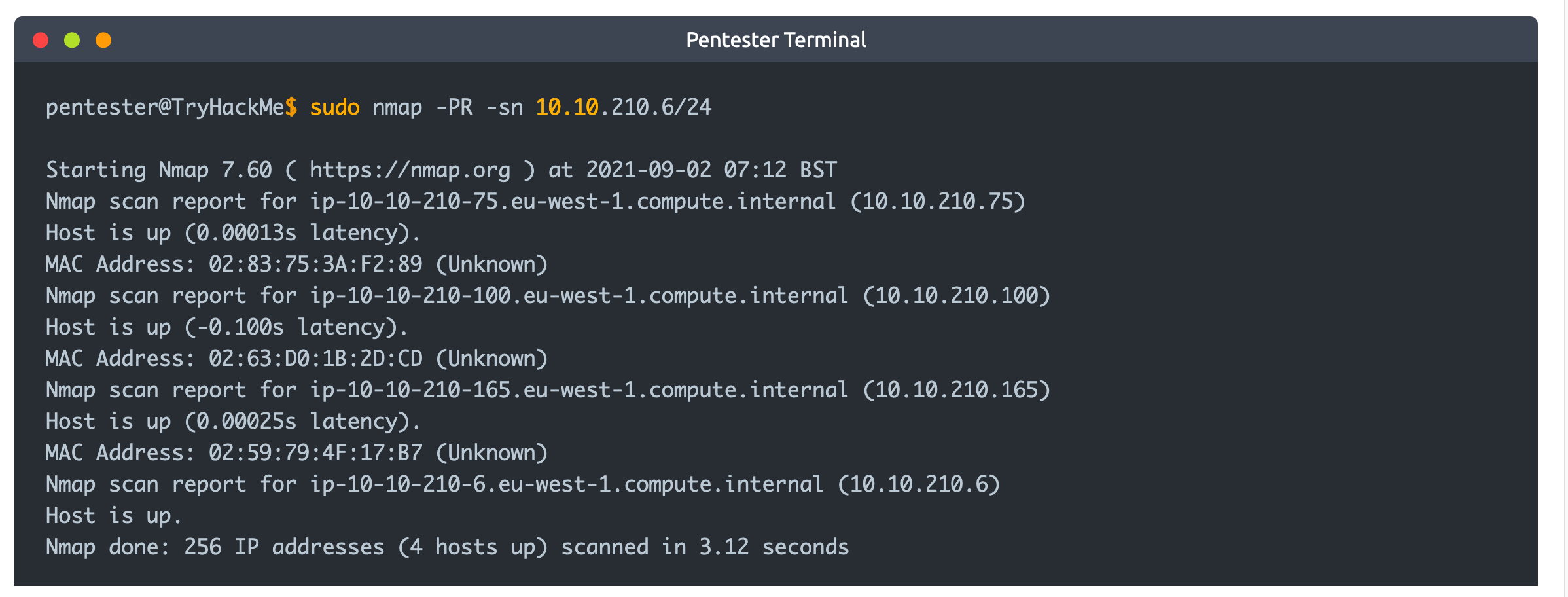
Làm thế nào bạn biết máy chủ đó đang chạy? Để tránh mất nhiều thời gian để quét cổng 1 máy chủ ngoại tuyến và địa chỉ IP không được sử dụng. Có rất nhiều cách để khám phá những máy chủ trực tuyến.

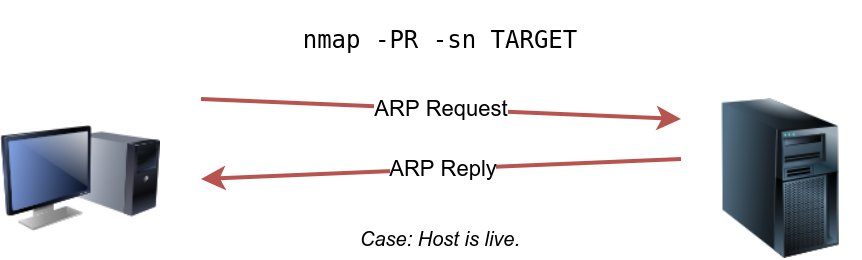
Khi không có những lựa chọn để khám phá máy chủ đang chạy, Nmap sẽ làm theo những cách sau:

* Khi 1 người dùng đặc quyền cố gắng quét những đối tượng trên 1 mạng cục bộ (Ethernet), Nmap sử dụng những yêu cầu ARP.
* Khi 1 người có đặc quyền cố gắng quét những đối tượng nằm ngoài mạng cục bộ, Nmap sử dụng những yêu cầu ICMP echo, TCP ACK đến cổng 80, TCP SYN đến cổng 443 và yêu cầu ICMP timestamp.
* Khi 1 người không có đặc quyền cố gắng quét những đối tượng nằm ngoài mạng cục bộ, Nmap sử dụng Three-way handshake bằng việc gửi những gói tin SYN đến cổng 80 và 443

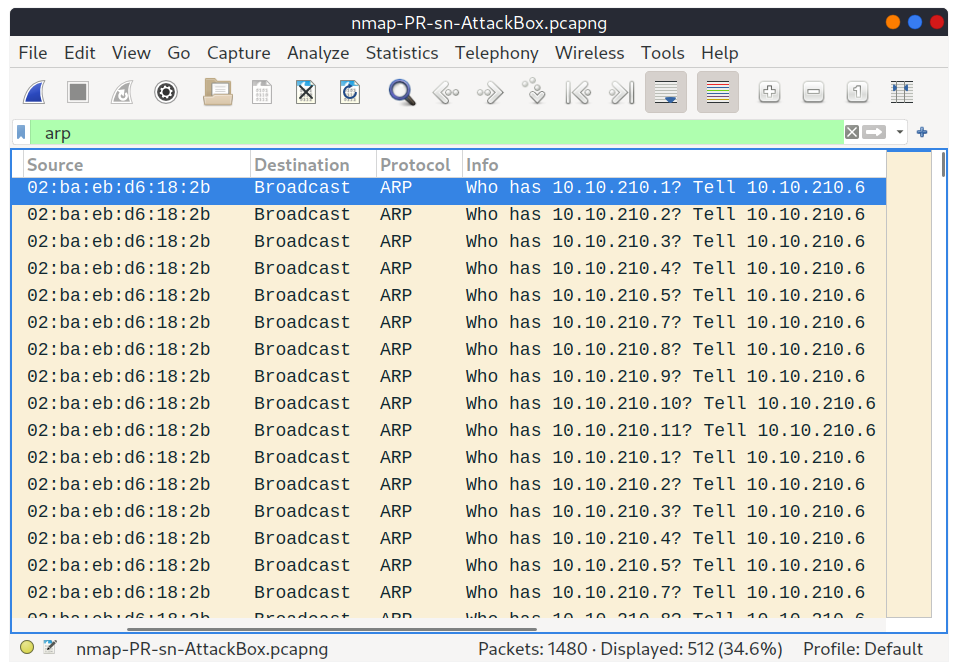
Nmap mặc định dùng ping quét để tìm máy chủ đang chạy sau đó chỉ quét các máy chủ trực tiếp. Nếu bạn muốn dùng Nmap để khám phá những máy chủ trực tuyến mà không có quét cổng, bạn có thể dùng nmap -sn TARGETS

ARP scan chỉ khả thi nếu bạn đang ở chung mạng con. Trên Ethernet (802.3) và Wifi (802.11), bạn cần biết địa chỉ MAC của bất cứ hệ thống nào trước khi bạn có thể giao tiếp với chúng. Địa chỉ MAC rất cần thiết với header link-layer; header chứa địa chỉ MAC nguồn và đích. Để có địa chỉ MAC, hệ điều hành gửi 1 câu truy vấn ARP. Máy chủ phản hồi ARP đang mở. Câu truy vấn ARP chỉ hoạt động nếu đối tượng ở chung mạng con với bạn (cùng Ethernet/Wifi). Bạn sẽ thấy nhiều truy vấn ARP được tạo ra trong quá trình quét Nmap của mạng cục bộ. Nếu bạn muốn Nmap chỉ thực hiện scan Arp mà không quét cổng, bạn có thể dùng nmap -PR -sn TARGETS. Ví dụ dưới cho thấy Nmap sử dụng Arp để khám phá máy chủ mà không có quét cổng. Chúng ta chạy nmap -PR -sn MACHINE\_IP/24 để khám phá tất cả hệ thống trực tiếp trong cùng mạng con với mục tiêu của chúng ta.





Nếu chúng ta nhìn những gói tin được tạo ra bởi công cụ như tcpdump hay Wireshark, chúng ta sẽ thấy lưu lượng mạng tương tự như hình bên dưới. Wireshark hiển thị địa chỉ MAC nguồn, đích, giao thức, và truy vấn liên quan đến mỗi yêu cầu ARP. Địa chỉ nguồn là địa chỉ MAC của AttackBox, trong khi điểm đến là địa chỉ broadcast vì chúng ta không biết địa chỉ MAC của đối tượng. Tuy vậy, chúng ta nhìn thấy địa chỉ IP của đối tượng, xuất hiện trong cột Info. Trong hình minh họa, chúng ta có thể thấy chúng ta đang yêu cầu những địa chỉ MAC của tất cả địa chỉ IP trong mạng con, bắt đầu với 10.10.210.1. Máy chủ với địa chỉ IP chúng ta yêu cầu sẽ gửi ARP phản hồi với địa chỉ MAC của chúng và nhờ đó, chúng ta biết nó đang trực tuyến.



Nhắc đến quét ARP, chúng ta nên đề cập đến công cụ arp-scan; nó cung cấp rất nhiều lựa chon để tùy chỉnh quá trình quét của bạn. Một lựa chọn rất phổ biến là arp-scan –localnet hoặc đơn giản hơn arp-scan -l. Lệnh này sẽ gửi những truy vấn ARP đến tất cả địa chỉ IP hợp lệ trên mạng cục bộ của mạng. Hơn nữa nếu hệ thống của bạn có nhiều hơn 1 giao diện và bạn thích khám phá 1 máy chủ trực tiếp trong số chúng, bạn có thể dùng -I. Ví dụ, sudo arp-scan -I eth0 -l sẽ gửi những câu truy vấn ARP đối với những địa chỉ IP hợp lệ trên giao diện eth0.

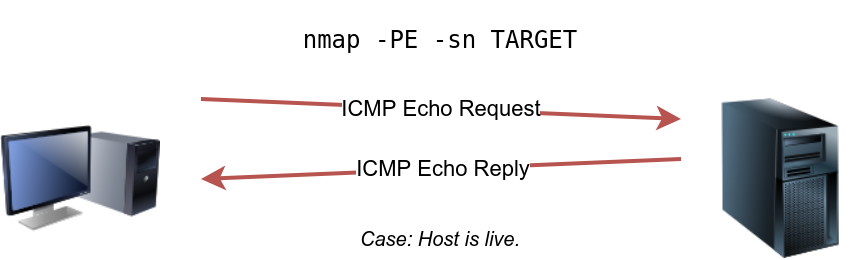
**Nmap Host Discovery Using ICMP**

Chúng ta có thể ping mọi địa chỉ IP trên mạng mục tiêu bằng cách gửi những yêu cầu (ICMP type 8/echo) và nhận phản hồi (ICMP type 0).

Rất nhiều tường lửa chặn ICMP echo; phiên bản mới của Ms Windows được cấu hình chặn những yêu cầu ICMP mặc định. Nhớ là câu truy vấn ARP sẽ đi trước yêu cầu ICMP nếu mục tiêu của bạn trong cùng mạng con.

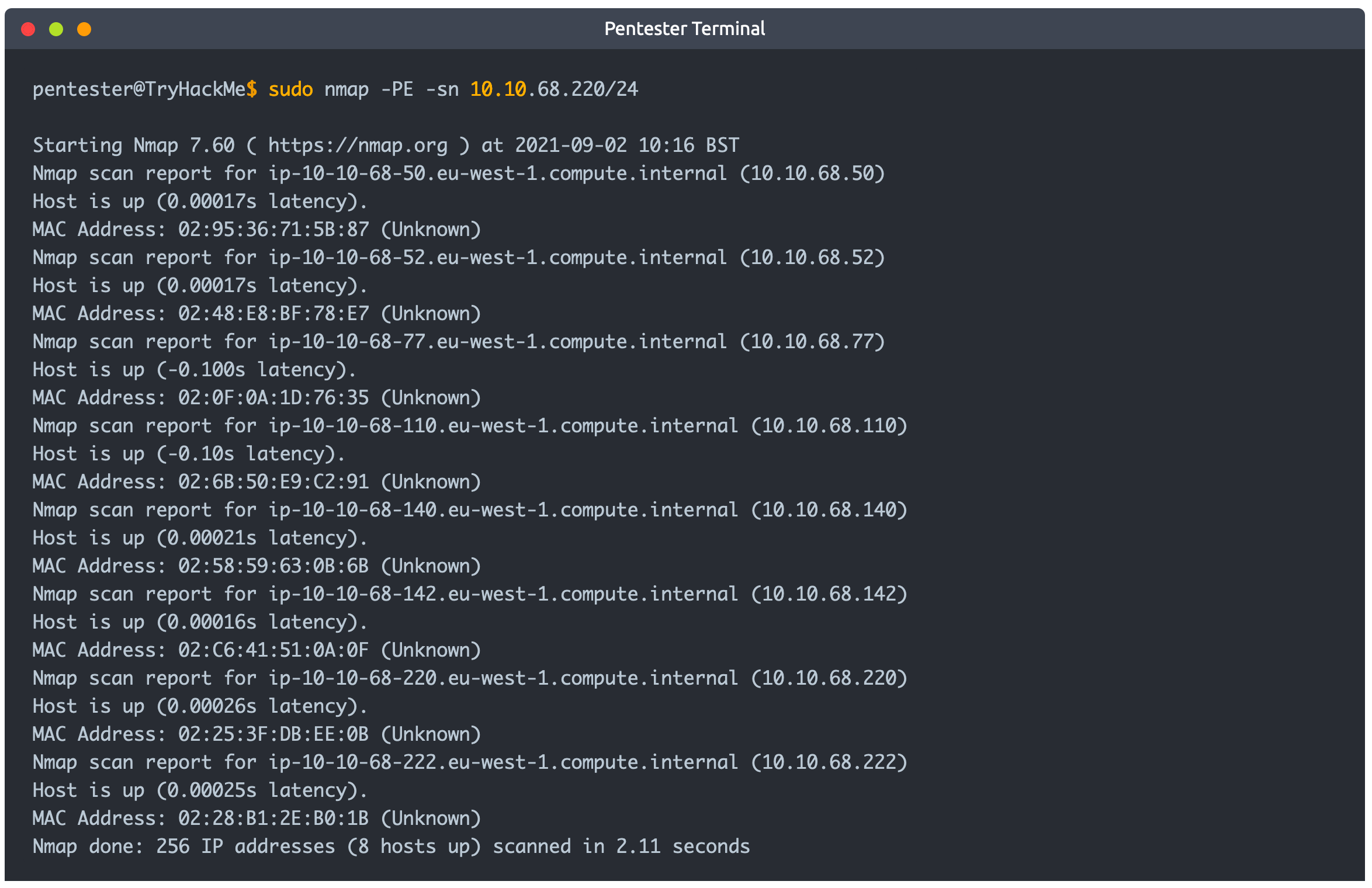
Để sử dụng ICMP echo khám phá máy chủ đang hoạt động, thêm -PE (nhớ thêm

-sn nếu bạn không muốn Nmap quét cổng).



Ở ví dụ dưới, chúng ta quét mạng con của mục tiêu bằng việc dùng câu lệnh

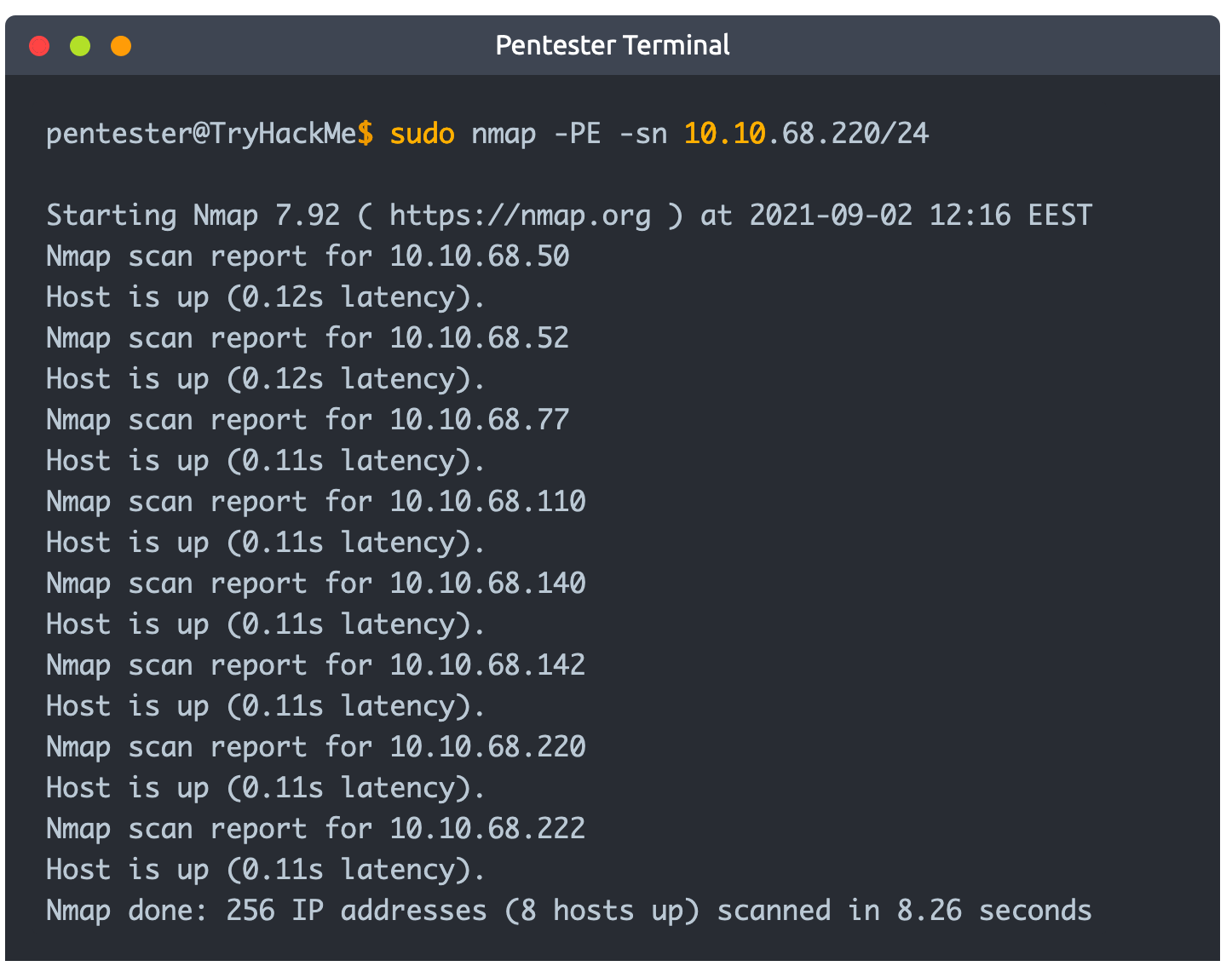
nmap -PE -sn MACHINE\_IP/24 . Nó sẽ gửi gói tin ICMP cho mỗi địa chỉ IP trên mạng con. Chúng ta thấy máy chủ đang chạy; Tuy nhiên, nên nhớ rằng rất nhiều tường lửa chặn ICMP.



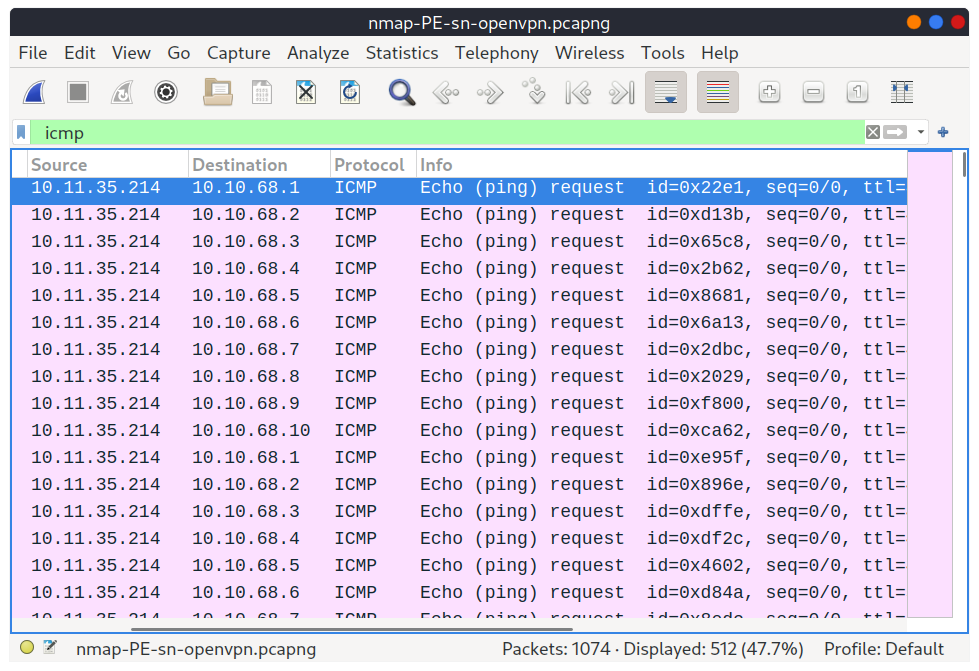
Đầu ra cho thấy 8 máy chủ đang chạy; hơn nữa, nó hiển thị địa chỉ MAC. Nhìn chung, chúng ta không nhận được địa chỉ MAC của mục tiêu nếu chúng không ở cùng 1 mạng con

Đầu ra ở trên cũng chỉ ra rằng Nmap không cần gửi những gói tin ICMP vì nó đã xác nhận rằng các máy chủ đang hoạt động dựa trên những phản hồi ARP mà nó nhận được

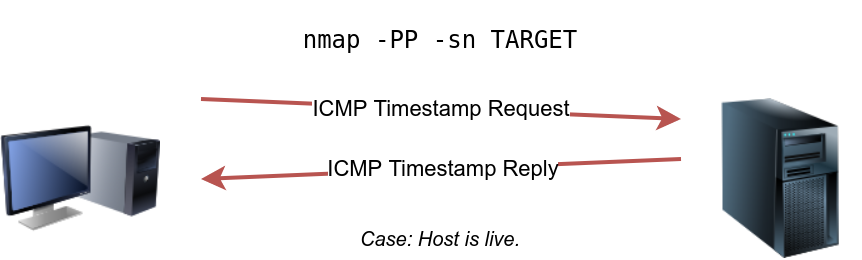
Chúng ta sẽ quét 1 lần nữa; Tuy nhiên, lần này, chúng ta sẽ quết 1 hệ thống ở mạng con khác. Kết quả tương tự nhưng không có địa chỉ mac



Nhìn những gói tin mạng bằng việc dùng Wireshark, chúng ta có 1 địa chỉ ip nguồn trên 1 mạng con khác với mạng con đích, gửi ICMP echo đến tất cả địa chỉ IP trong mạng mục tiêu.



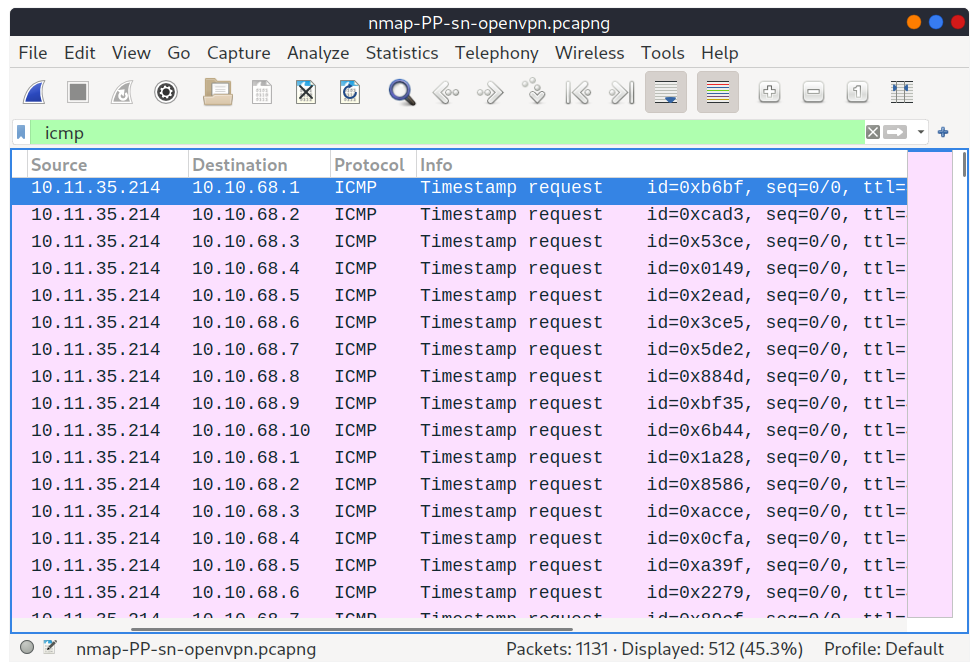
Vì những yêu cầu ICMP thường bị chặn, bạn cũng có thể xem xét ICMP Timestamp hoặc những yêu cầu ICMP Address Mask để kiểm tra xem hệ thống có trực tuyến không. Nmap sử dụng yêu cầu timestamp (ICMP type 13) và kiểm tra xem nó có nhận được phản hồi timestamp (ICMP type 14). Việc thêm -PP yêu cầu Nmap sử dụng ICMP timestamp



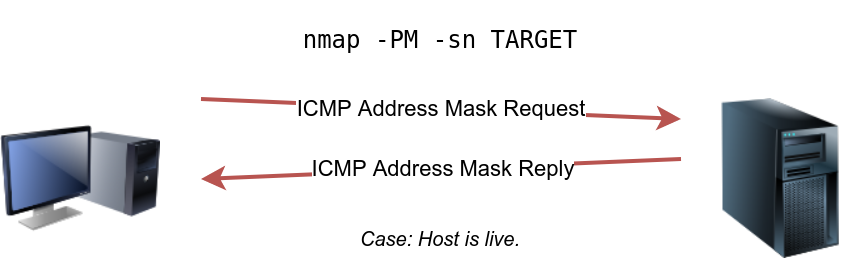
Chúng ta chạy nmap -PP -sn MACHINE\_IP/24 để khám phá những máy tính đang trực tuyến trên mạng con



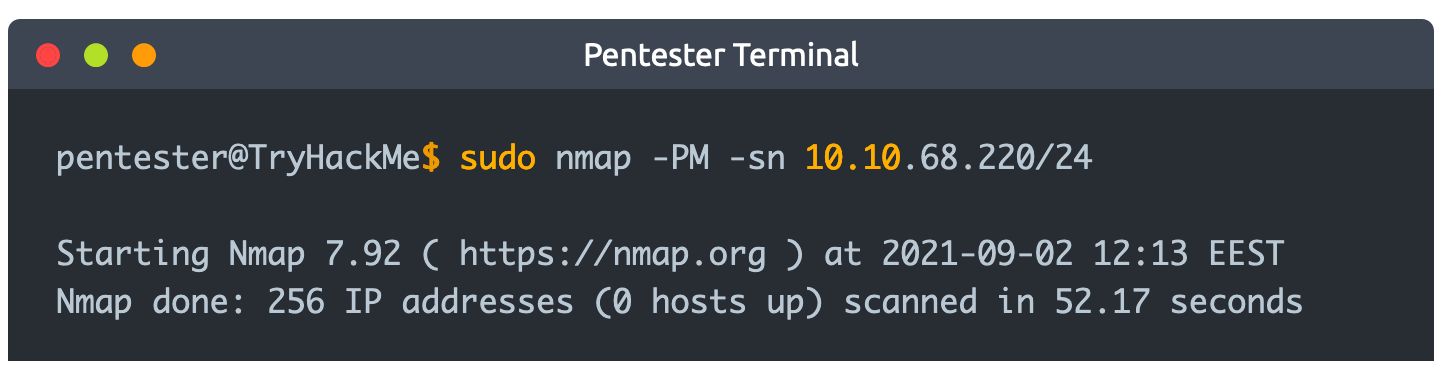
Bạn có thể xem những gói tin gửi đi bằng Wireshark.



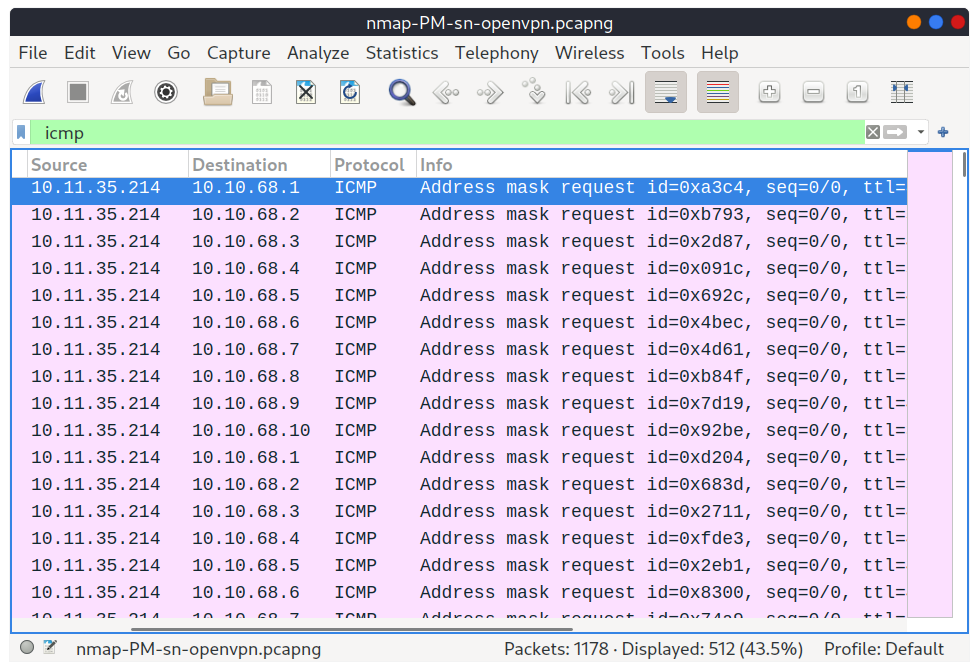
Tương tự, Nmap dùng những câu truy vấn address mask (ICMP type 17) và kiểm tra phản hồi address mask (ICMP type 18).



Để khám phá máy chủ đang chạy bằng việc dùng ICMP address mask, chúng ta chạy lệnh sau: nmap -PM -sn MACHINE\_IP/24. Những lần quét trước có ít nhất 8 máy chủ đang chạy nhưng lần quét này không có máy chủ nào chạy. Đó là vì hệ thống hoặc tường lửa trên route đang chặn những gói tin ICMP loại này.



Mặc dù, chúng ta không nhận được bất cứ phản hồi nào và không thể tìm ra máy chủ nào đang chạy. Điều đáng lưu ý là lần quét này nó gửi ICMP address mask đến mỗi địa chỉ IP 2 lần.

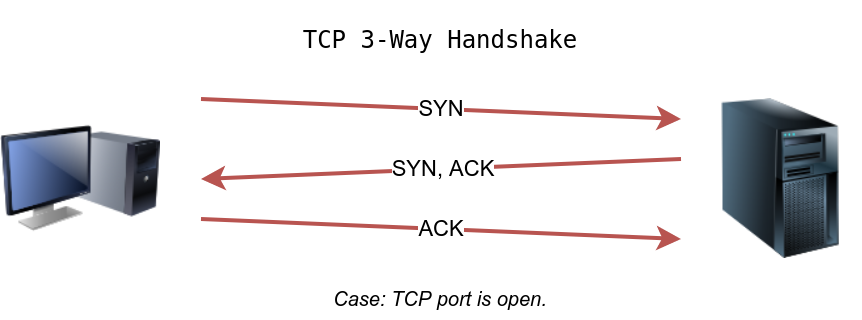


**Nmap Host Discovery Using TCP and UDP**

**TCP SYN Ping**

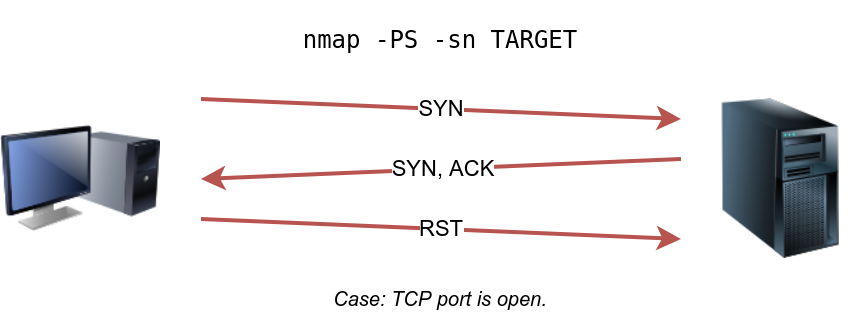
Chúng ta có thể gửi 1 gói tin với trạng thái SYN đến cổng TCP, mặc định là 80 và đợi phản hồi. Một cổng mở sẽ phản hồi với trạng thái SYN/ACK; một cổng đóng sẽ dẫn đến RST (Reset). Trong trường hợp này, chúng ta chỉ kiểm tra xem có nhận được bất cứ phản hồi nào để suy luận xem máy chủ có hoạt động không.

Hình dưới là cách TCP 3-way handshake hoạt động:

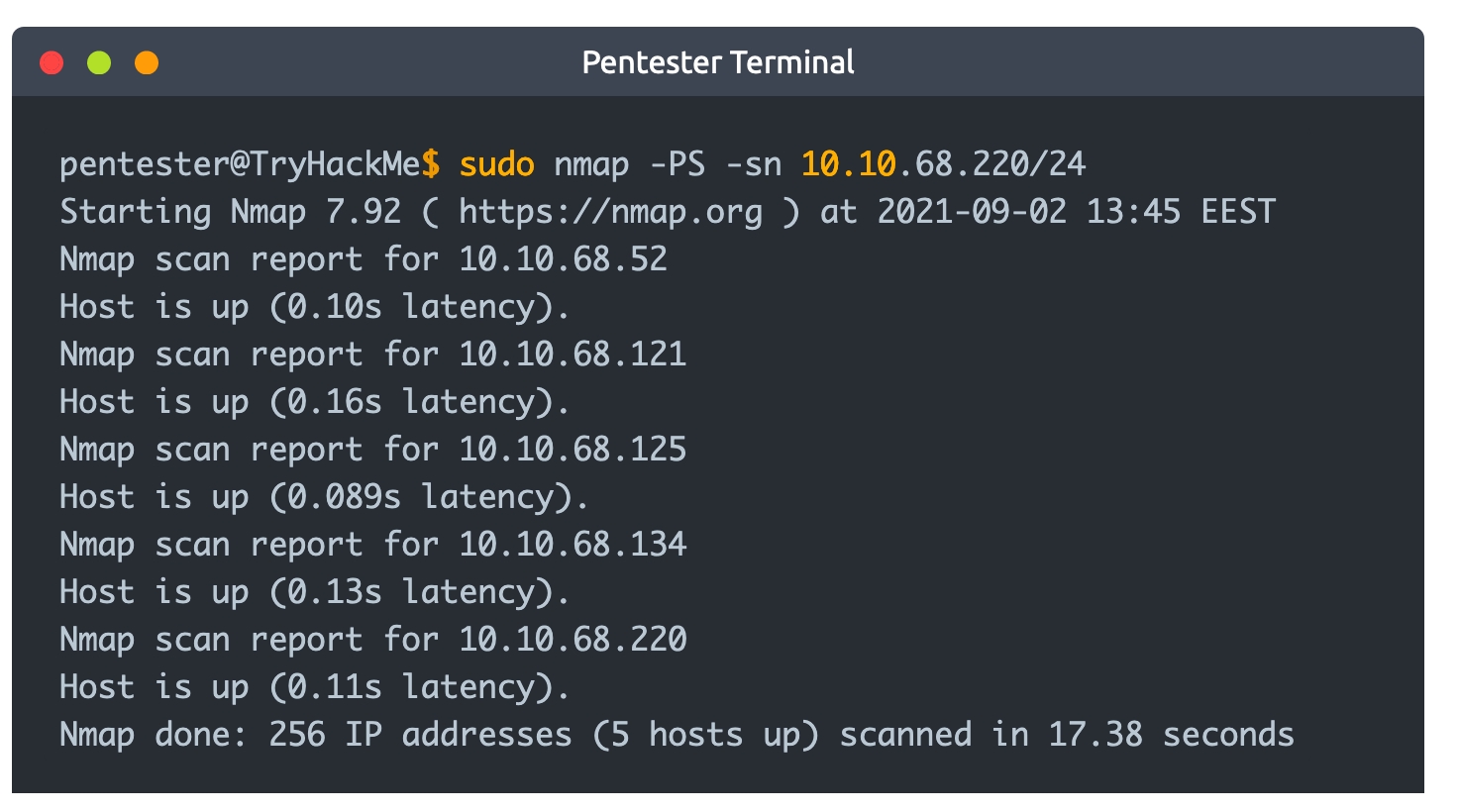


Nếu bạn muốn Nmap dùng TCP Syn ping, bạn có thể dùng -PS cùng với số cổng trong phạm vi, danh sách. Ví dụ, -PS21 sẽ nhắm đến cổng 21, trong khi -PS21-25 sẽ nhắm đến cổng 21,22,…,25. Cuối cùng, -PS80,443,8080 sẽ nhắm đến cổng 80, 443, 8080.

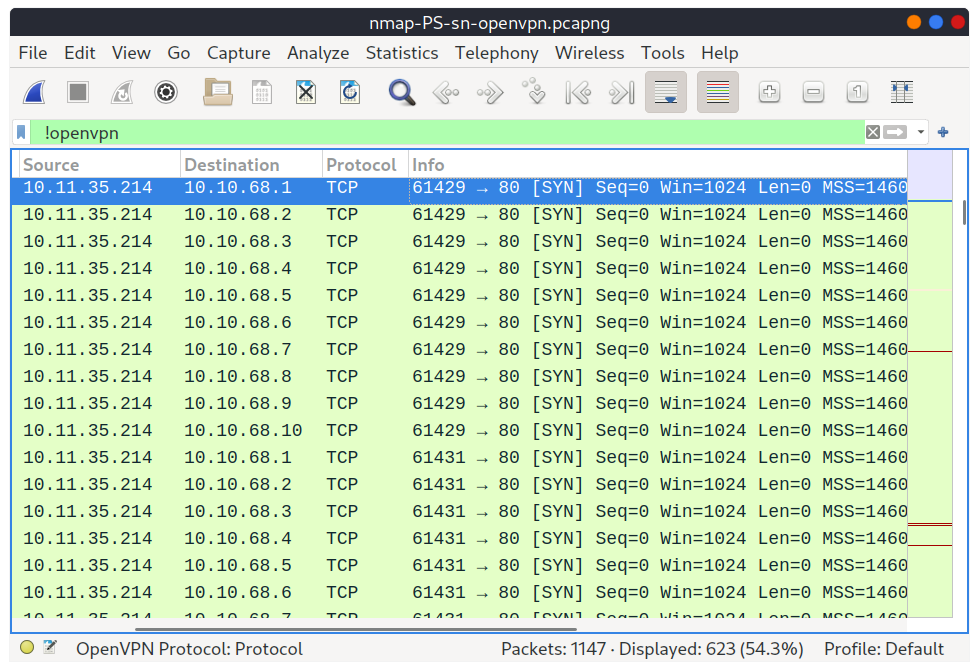
Những người dùng có đặc quyền (root và sudoers) có thể gửi những gói tin TCP SYN và không cần hoàn thành TCP 3-way handshake thậm chí cổng đang mở.



Chúng ta sẽ chạy nmap -PS -sn MACHINE\_IP/24 để quét mạng con.



Vì chúng ta không chỉ định cổng TCP, Nmap đã sử dụng những cổng phổ biến; trong trường hợp này là TCP 80. Bất cứ dịch vụ nào đang nghe ở cổng 80 sẽ phản hồi chỉ ra rằng máy chủ đang hoạt động.

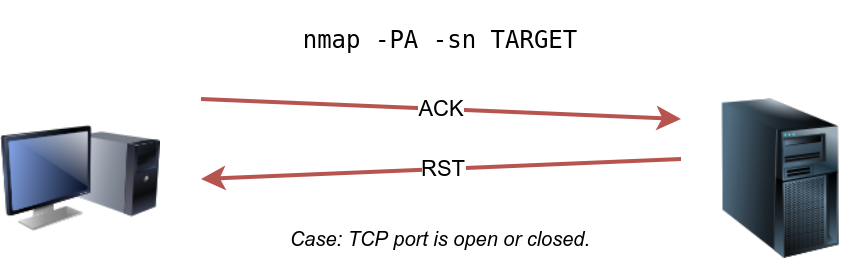


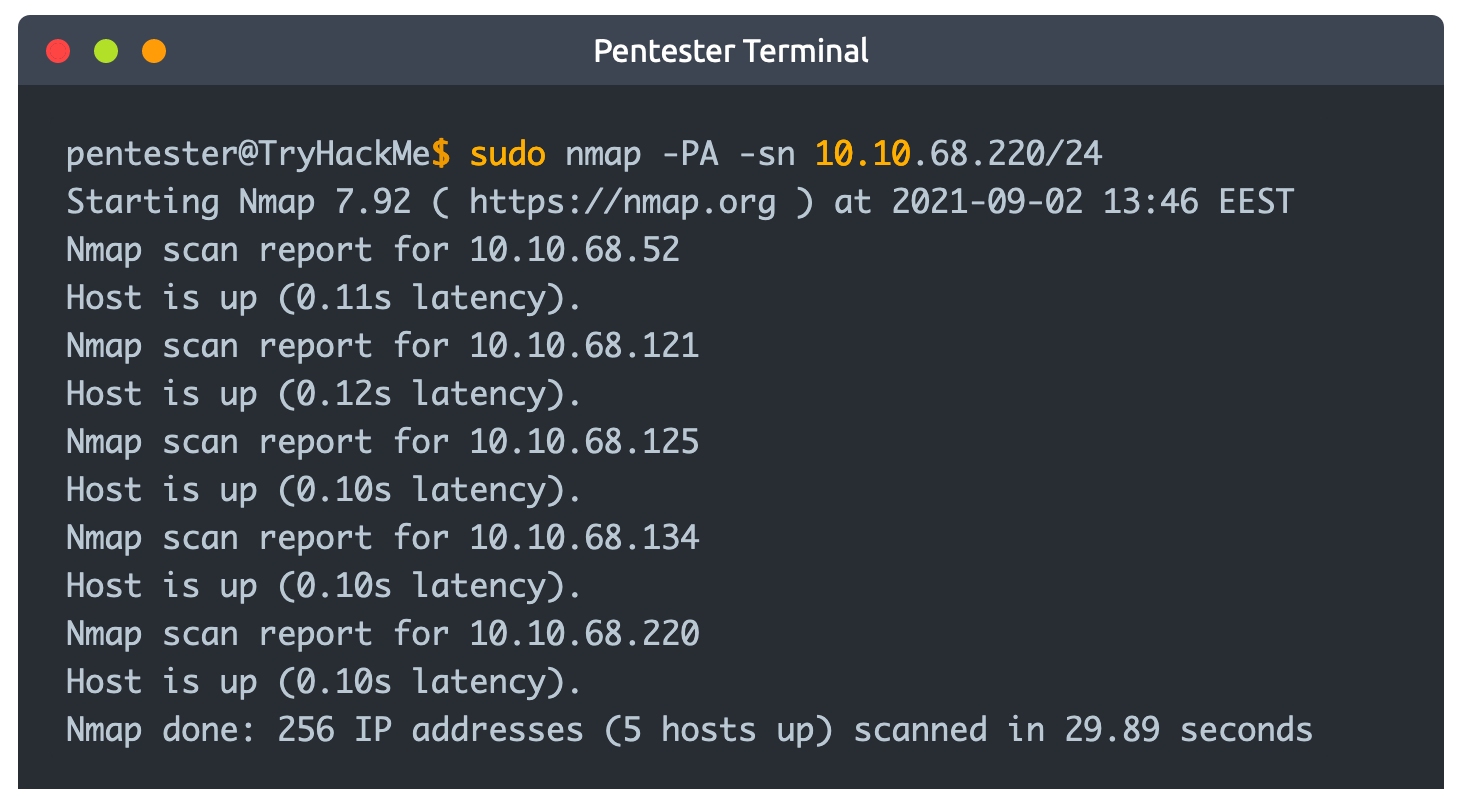
**TCP ACK ping:**

Nó gửi 1 gói tin với trạng thái ACK. Bạn bắt buộc phải chạy Nmap với tư cách là người dùng có đặc quyền để làm được điều này.

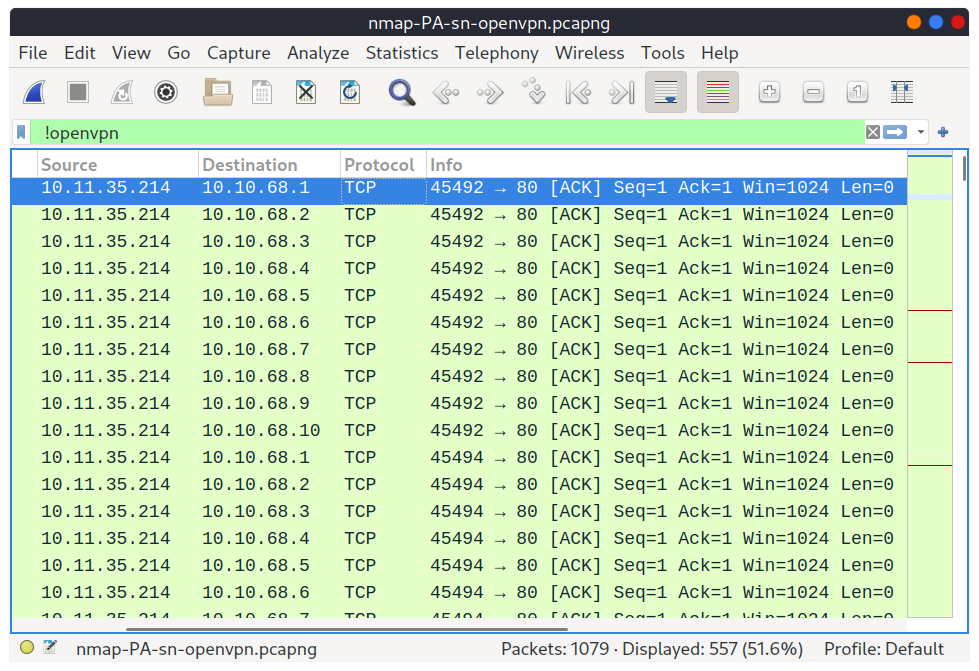
Mặc định dùng cổng 80. Cách dùng tương tự như SYN ping: -PA

Hình dưới cho thấy bất cứ gói tin TCP với trạng thái ACK sẽ nhận lại được 1 gói tin TCP với trạng thái RST. Đối tượng phản hồi với trạng thái RST vì gói tin TCP ACK không phải là 1 phần của bất kỳ kết nối nào đang diễn ra.



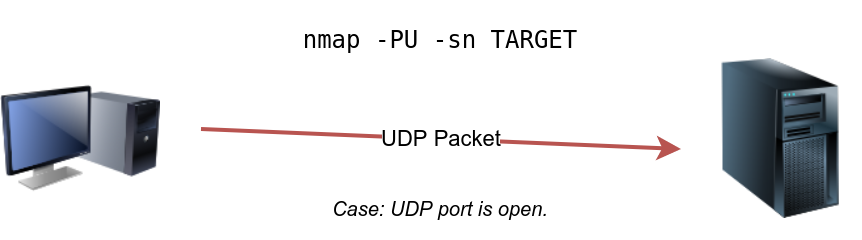


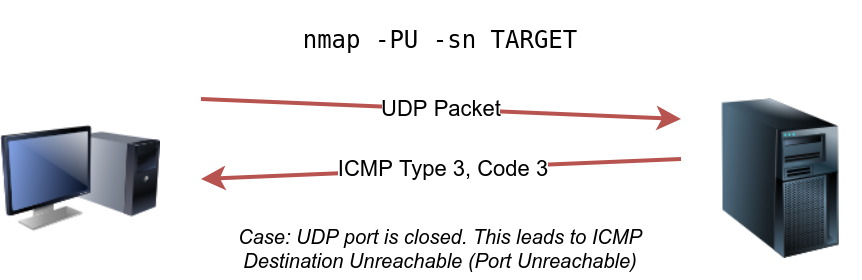
Nếu chúng ta xem lưu lượng mạng ở Wireshark, chúng ta sẽ khám phá rất nhiều gói tin với trạng thái ACK và gửi đến cổng 80 của hệ thống nhắm đến. Nmap gửi mỗi gói tin hai lần. Những hệ thống không phản hồi thì đang ngoại tuyến hoặc không thể truy cập.

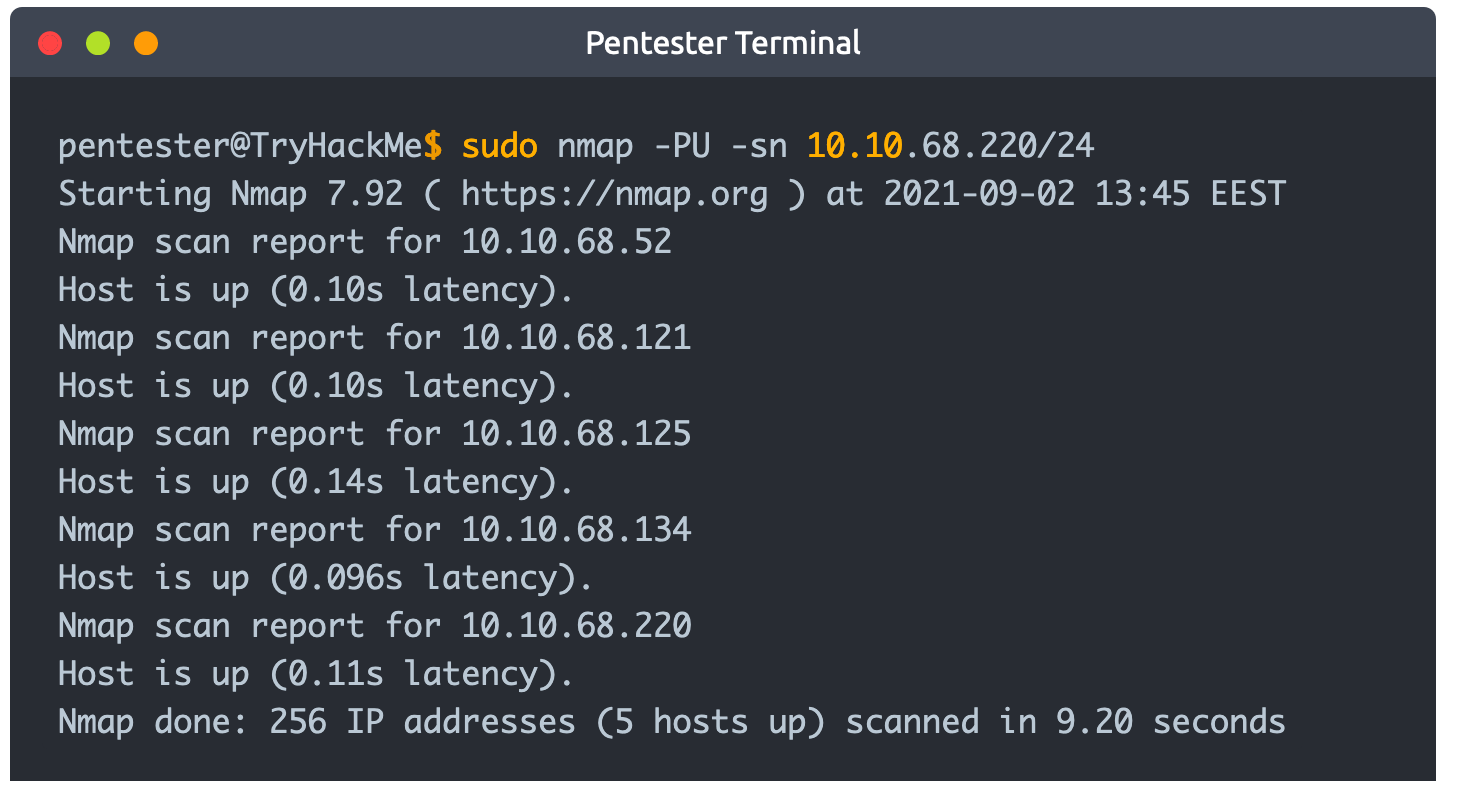


**UDP Ping**

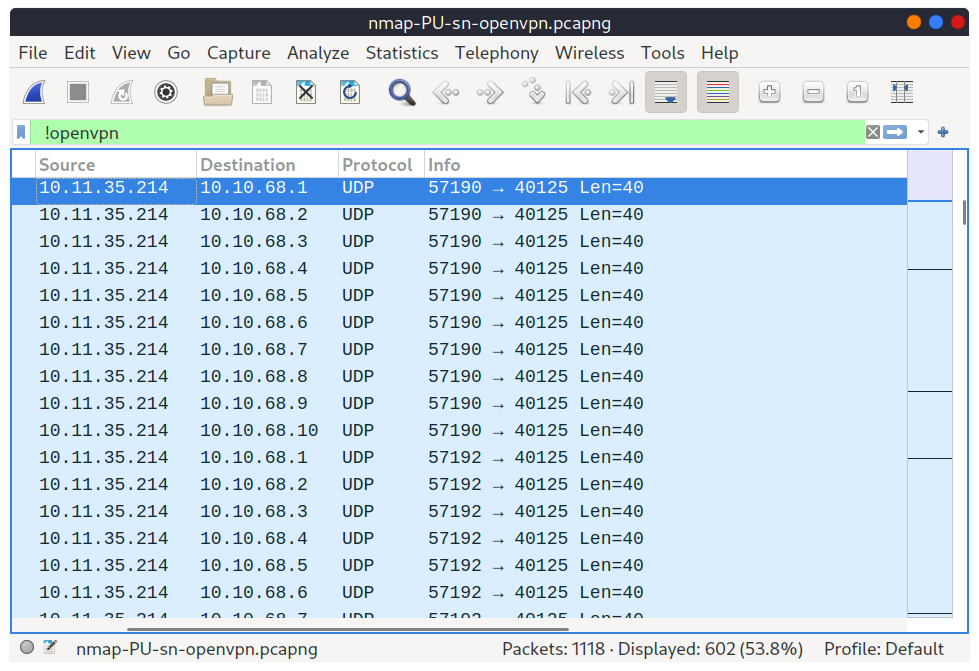
Cuối cùng, chúng ta có thể dùng UDP để khám phá máy chủ đang chạy. Ngược lại với TCP SYN ping, việc gửi 1 gói tin UDP đến 1 cổng đang mở không mong nhận được phản hồi. Tuy nhiên, nếu chúng ta gửi 1 gói tin UDP đến 1 cổng UDP đã đóng, chúng ta sẽ nhận được gói tin không thể truy cập cổng ICMP; Điều này chỉ ra rằng đối tượng đang hoạt động.







Chúng ta để ý thấy Nmap gửi những gói tin UDP đến những cổng UDP khả năng cao đã đóng



**Sử dụng tra cứu DNS ngược:**

Hành vi mặc định của Nmap là tra cứu DNS ngược. Vì tên những máy chủ có thể tiết lộ rất nhiều, nó là 1 bước rất quan trọng. Tuy nhiên, nếu bạn không muốn gửi bất cứ truy vấn DNS nào, bạn có thể dùng -n để bỏ qua.

Mặc định, Nmap sẽ tìm kiếm những máy chủ trực tuyến; Tuy nhiên, bạn có thể dùng -R để truy vấn đến máy chủ DNS cho những máy chủ ngoại tuyến. Nếu bạn muốn sử dụng máy chủ DNS đặc biệt, bạn có thể thêm –dns-servers DNS\_SERVER.

**Kết luận:**

Bạn đã học về cách ARP, ICMP, TCP và UDP có thể phát hiện những máy chủ đang trực tuyến. Dưới đây là bảng tóm tắt về những lệnh cho Nmap:

| **Scan Type** | **Example Command** |
| --- | --- |
| ARP Scan | sudo nmap -PR -sn MACHINE\_IP/24 |
| ICMP Echo Scan | sudo nmap -PE -sn MACHINE\_IP/24 |
| ICMP Timestamp Scan | sudo nmap -PP -sn MACHINE\_IP/24 |
| ICMP Address Mask Scan | sudo nmap -PM -sn MACHINE\_IP/24 |
| TCP SYN Ping Scan | sudo nmap -PS22,80,443 -sn MACHINE\_IP/30 |
| TCP ACK Ping Scan | sudo nmap -PA22,80,443 -sn MACHINE\_IP/30 |
| UDP Ping Scan | sudo nmap -PU53,161,162 -sn MACHINE\_IP/30 |

Nhớ thêm -sn nếu bạn chỉ thích khám phá máy chủ mà không quét các cổng.

| **Option** | **Purpose** |
| --- | --- |
| -n | no DNS lookup |
| -R | reverse-DNS lookup for all hosts |
| -sn | host discovery only |