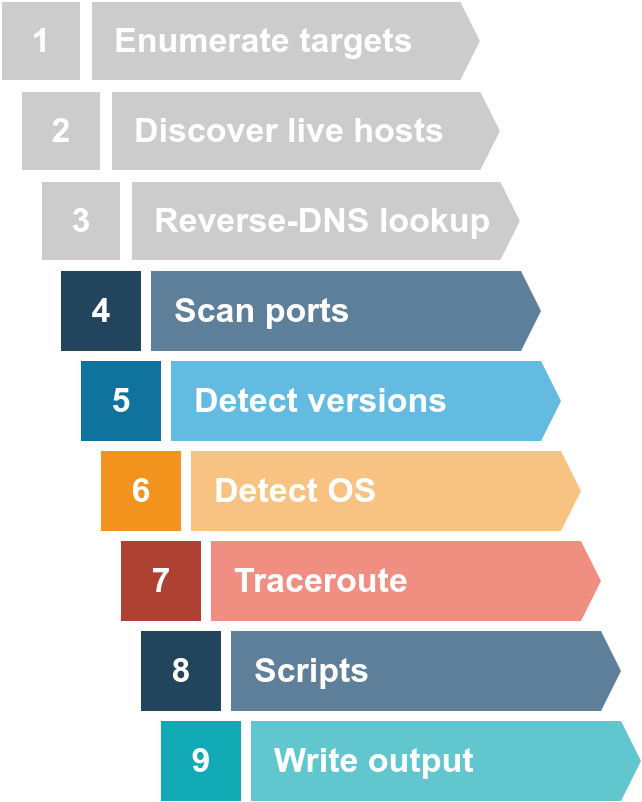
**Nmap Basic Port Scans**

Trong bài trước, chúng ta tập trung khám phá những hệ thống đang chạy. Cho đến nay, chúng ta đã đi qua ba bước quét của Nmap.

1. Liệt kê các đối tượng

2. Khám phá những máy chủ trực tuyến

3. Tra cứu DNS ngược



Bước tiếp theo sẽ kiểm tra những cổng đang mở và lắng nghe. Do đó, trong bài này và bài tiếp theo, chúng ta tập trung quét các cổng và những loại quét cổng khác nhau bằng nmap. Phòng này giải thích:

1. TCP connect port scan

2. TCP SYN port scan

3. UDP port scan

**Những cổng TCP và UDP**

Một địa chỉ IP chỉ định 1 máy chủ trên mạng, cổng TCP/UDP được dùng để xác định những dịch vụ mạng chạy trên máy chủ đó. 1 máy chủ cung cấp dịch vụ mạng và nó tuân theo 1 giao thức mạng cụ thể. Nó bao gồm việc cung cấp thời gian, phản hồi những câu truy vấn DNS và vận chuyển những trang web. 1 cổng được liên kết với 1 dịch vụ bằng số cổng. Ví dụ, máy chủ HTTP mặc định sẽ gắn với cổng TCP 80; nếu máy chủ HTTP hỗ trợ SSL/TLS, nó sẽ lắng nghe ở cổng TCP 443. Tuy vậy, nhà quản trị có thể chọn số cổng khác nếu cần thiết.

Chúng ta có thể phân loại cổng theo hai trạng thái:

1. Cổng đang mở chỉ ra rằng có một vài dịch vụ đang lắng nghe trên cổng đó.

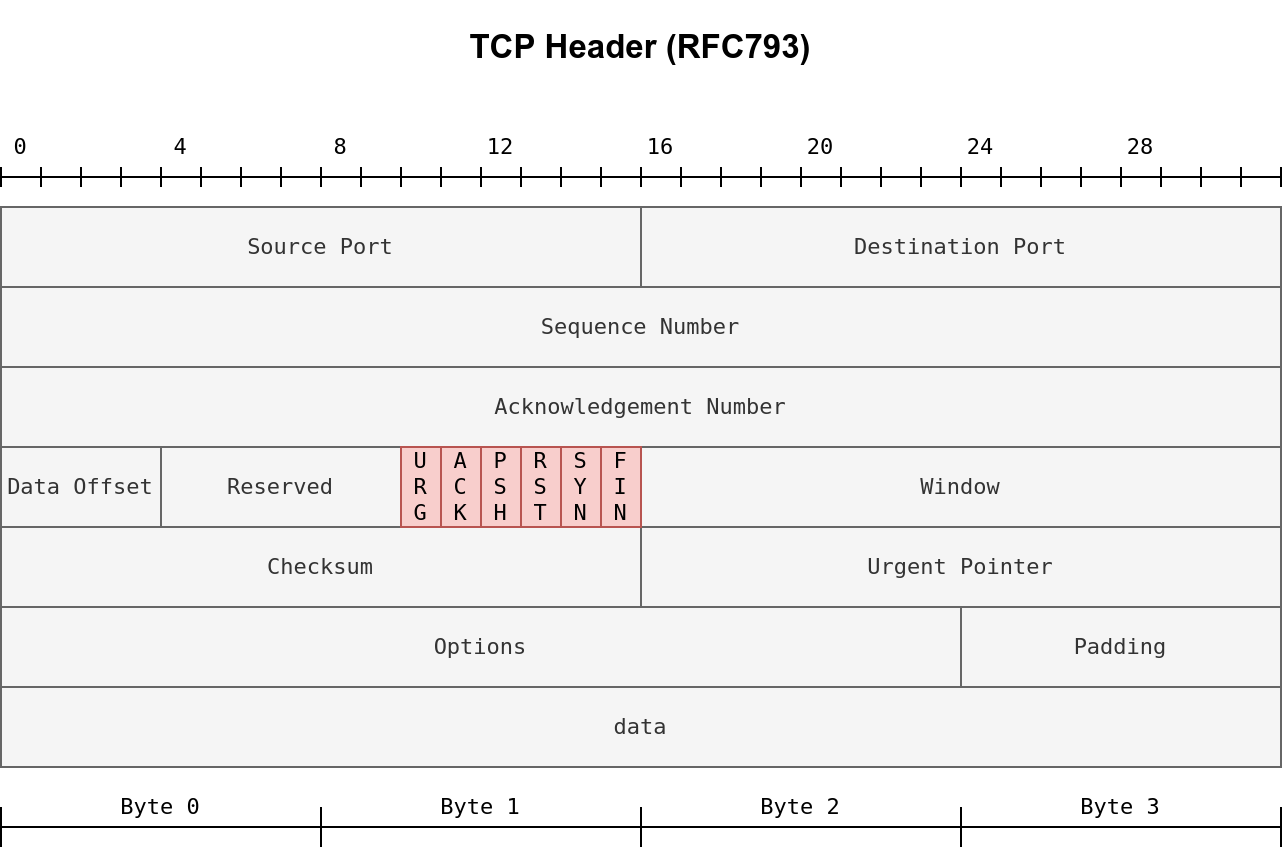
2. Cổng đang đóng

Tuy vậy, trong tình huống thực tế, chúng ta cần xem xét ảnh hưởng của tường lửa. Ví dụ, 1 cổng có thể mở nhưng tường lửa có thể chặn những gói tin. Do đó, Nmap xem xét 6 trạng thái sau:

1. Mở: chỉ ra rằng dịch vụ đang chạy trên cổng đó
2. Đóng: chỉ ra rằng không có dịch vụ nào đang lắng nghe mặc dù cổng đó có thể truy cập. Có thể truy cập, có nghĩa là nó có thể chạm và không bị chặn bởi tường lửa hoặc những chương trình/ứng dụng bảo mật khác.
3. Bị lọc: Nmap không thể xác định cổng đó đang mở hay đóng vì cổng không thể truy cập. Trạng thái này thường là vì tường lửa ngăn chặn Nmap chạm vào cổng đó. Những gói tin của Nmap có thể bị chặn khi chạm đến cổng đó; Ngoài ra, những phản hồi bị chặn chạm vào máy chủ của Nmap
4. Không bị lọc: Nmap không thể xác định cổng đó đang mở hay đóng mặc dù cổng có thể truy cập. Trạng thái này thường hay gặp khi quét ACK -sA
5. Mở|Bị lọc: Nmap không thể xác định cổng đó đang mở hay bị lọc
6. Đóng|Bị lọc: Nmap không thể quyết định cổng đó đang đóng hay bị lọc

**TCP Flags**

Nmap hỗ trợ rất nhiều loại quét cổng TCP. Để hiểu về sự khác nhau giữa chúng, chúng ta cần xem qua TCP header. TCP header là 24 bytes đầu tiên của phân đoạn TCP. Hình bên dưới thoạt đầu nhìn rất phức tạp nhưng lại rất dễ hiểu. Ở dòng đầu tiên, chúng ta có cổng TCP nguồn và cổng đích. Chúng ta có thể thấy số cổng được phân bổ 16 bits (2 bytes). Ở dòng thứ 2 và 3, chúng ta có số thứ tự và số xác nhận. Mỗi dòng chiếm 32 bits (4 bytes). Tổng cộng có 6 dòng tương ứng 24 bytes

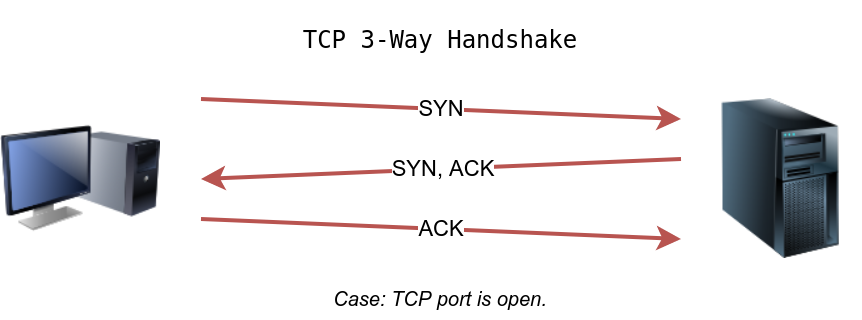


Đặc biệt chúng ta cần tập trung vào các trạng thái mà Nmap có thể thiết lập. Chúng ta đã đánh dấu nó bằng màu đỏ. Việc đặt 1 flag có nghĩa là đặt giá trị là 1. Từ trái sang phải, những flag của TCP header là:

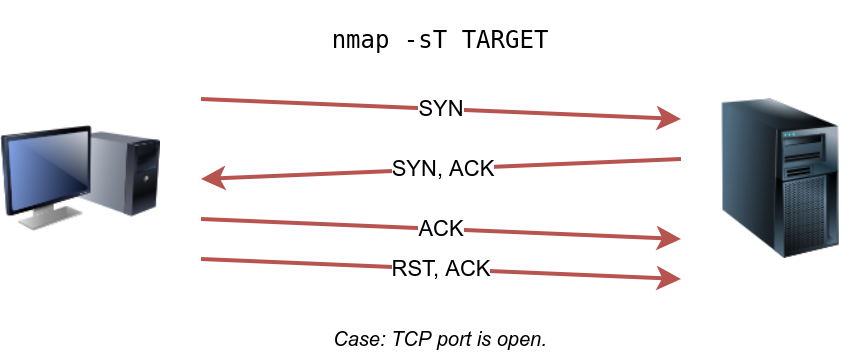
1. URG: cờ khẩn cấp chỉ ra rằng urgent pointer là quan trọng. Urgent pointer chỉ ra rằng dữ liệu sắp đến rất khẩn cấp và phân đoạn TCP với cờ URG được xử lí ngay lập tức mà không cần xem xét việc đợi các phân đoạn TCP đã gửi trước đó.
2. ACK: cờ xác nhận chỉ ra rằng số xác nhận là quan trọng. Nó được dùng để xác nhận việc nhận 1 phân đoạn TCP
3. PSH: cờ push yêu cầu TCP chuyển dữ liệu đến ứng dụng ngay lập tức
4. RST: cờ reset được dùng để đặt lại kết nối. 1 thiết bị khác như tường lửa có thể gửi nó để hủy kết nối TCP. Cờ này được dùng khi dữ liệu được gửi đến máy chủ và không có dịch vụ nào trả lời
5. SYN: cờ synchronize được dùng để khởi tạo TCP 3-way handshake và đổng bộ hóa số thứ tự với máy chủ khác. Số thứ tự nên được đặt ngẫu nhiên trong quá trình thiết lập kết nối TCP
6. FIN: Người gửi không có dữ liệu để gửi

**TCP Connect Scan**

TCP connect scan làm việc bằng cách hoàn tất TCP 3-way handshake. Trong quá trình thiết lập kết nối TCP, máy khách gửi 1 gói tin TCP với flag SYN và máy chủ phản hồi với flag SYN/ACK nếu cổng đang mở; Cuối cùng, máy khách hoàn tất 3-way handshake bằng việc gửi 1 ACK.

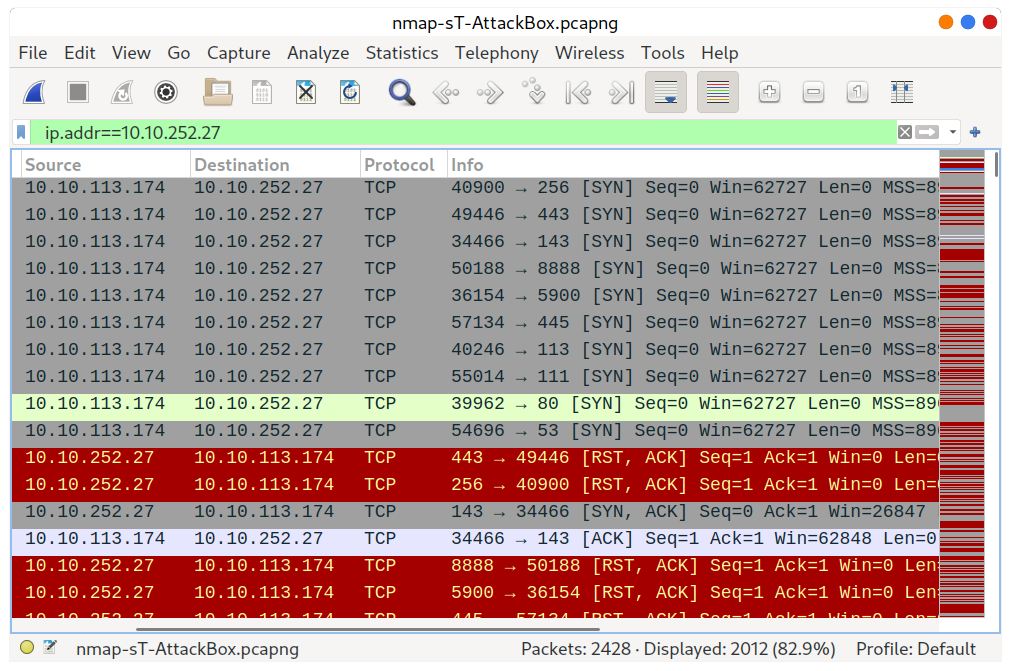


Chúng ta hứng thú xem cổng TCP nào đang mở, không thiết lập kết nối TCP. Do vậy kết nối bị ngắt ngay khi trạng thái của nó được xác nhận bằng cách gửi RST/ACK. Bạn có thể chạy TCP connect scan bằng -sT



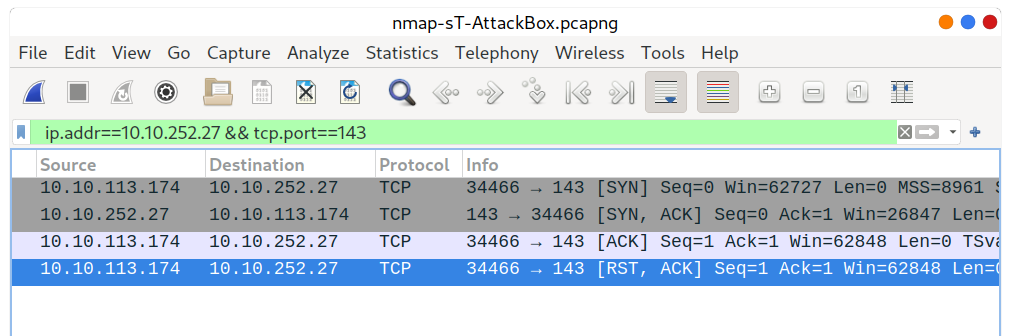
Điều đáng lưu ý là nếu bạn không phải là người dùng có đặc quyền, TCP connect scan là lựa chọn duy nhất có thể khám phá những cổng TCP đang mở.

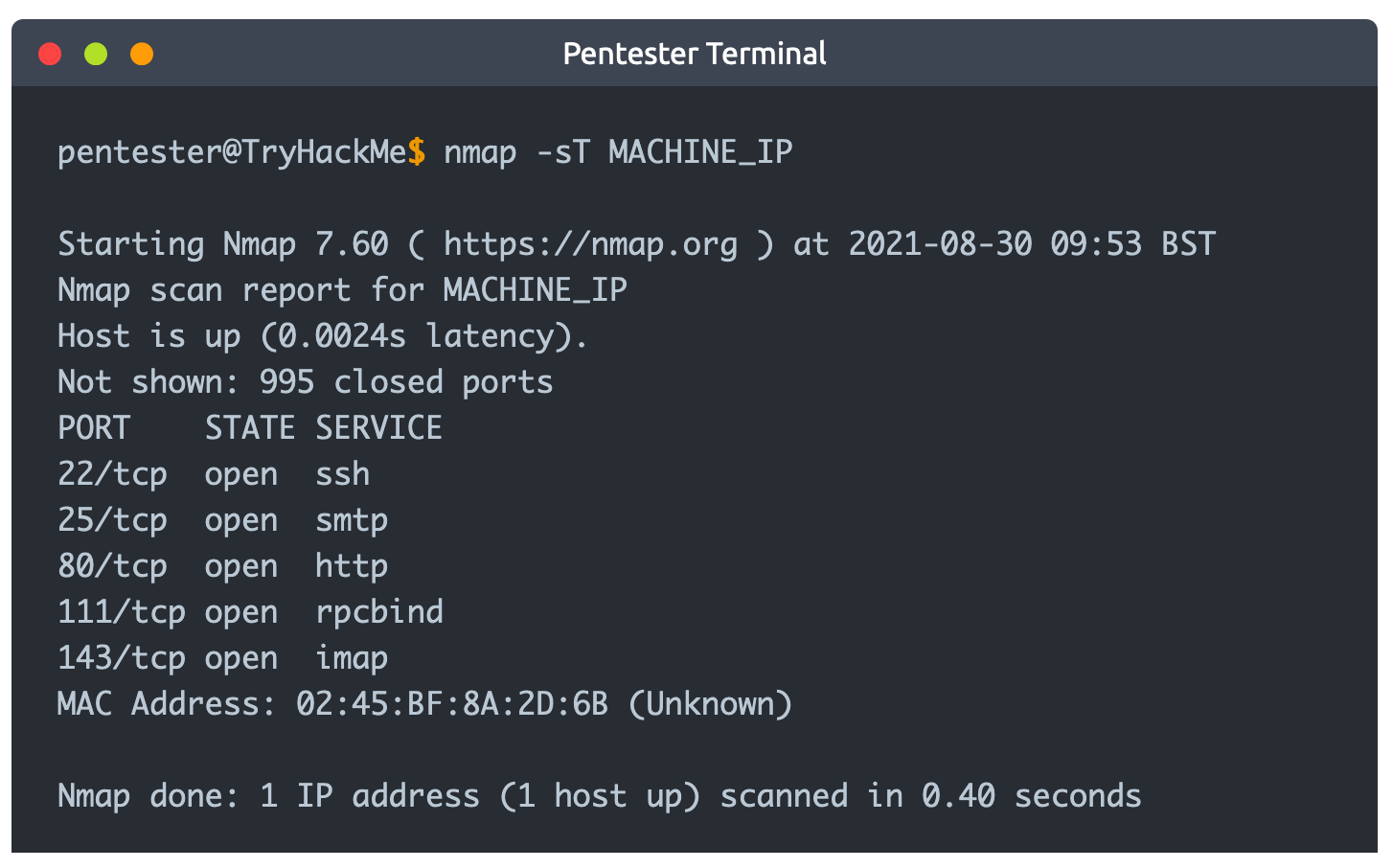
Trong wireshark, chúng ta thấy Nmap đang gửi những gói tin TCP với flag SYN đến rất nhiều cổng 256, 443, 143,… Mặc định, Nmap sẽ cố gắng kết nối với 1000 cổng phổ biến nhất. Cổng TCP đã đóng phản hồi 1 gói tin SYN với RST/ACK để chỉ ra rằng nó không mở. Điều này sẽ tương tự với những cổng đã đóng vì chúng ta cố gắng khởi tạo TCP 3-way handshake với chúng.



Chúng ta chú ý thấy cổng 143 đang mở vì vậy nó phản hồi SYN/ACK và Nmap hoàn tất 3-way handshake bằng cách gửi ACK.

Đây là tất cả những gói tin trao đổi giữa máy chủ Nmap và hệ thống đích ở cổng 143.



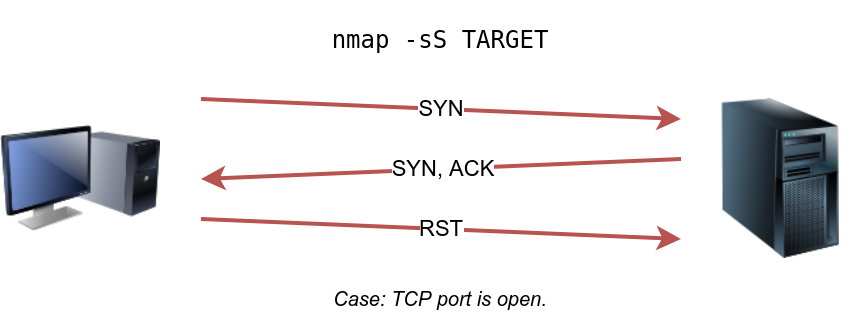


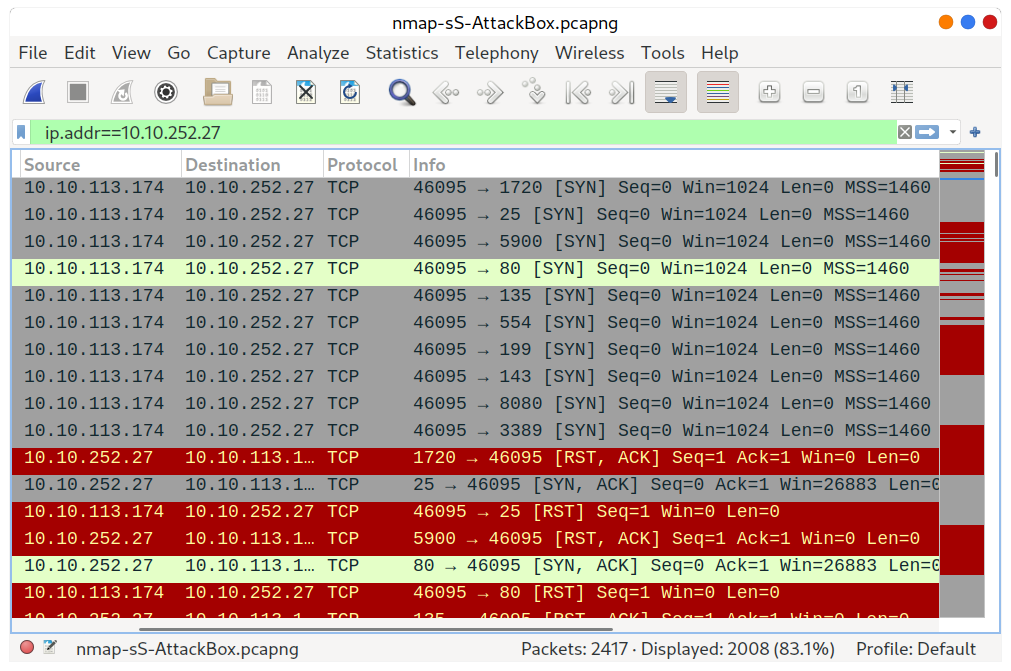
Chúng ta có thể dùng -F để bật chế độ nhanh và giảm số cổng quét từ 1000 đến 100 cổng phổ biến.

Điều đáng nói là -r cũng có thể thêm vào để quét các cổng theo thứ tự liên tiếp thay vì ngẫu nhiên.

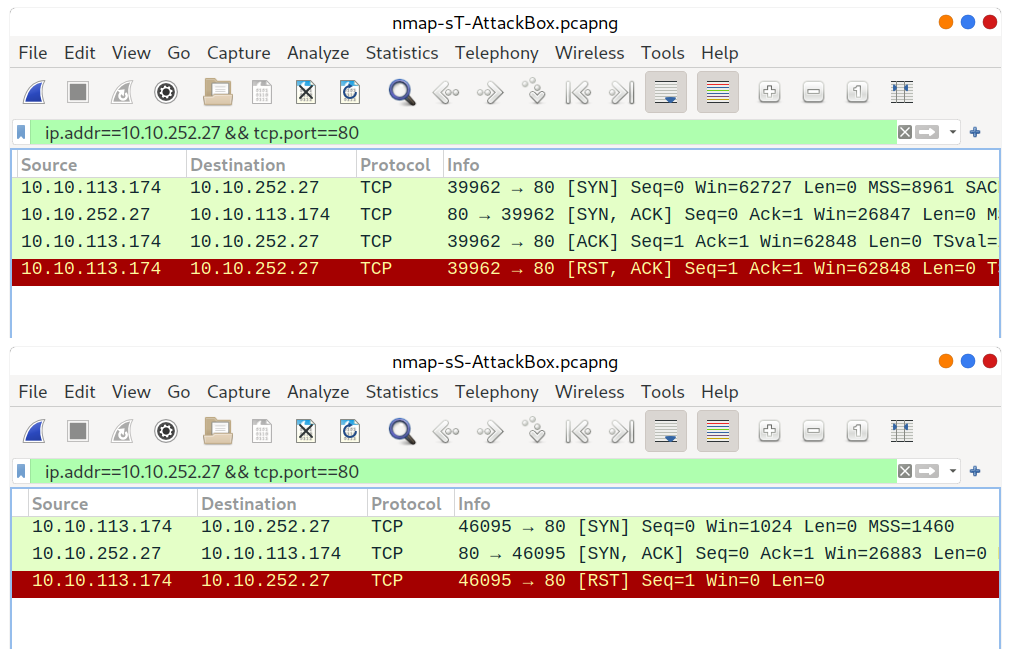
**TCP SYN scan**

Những người dùng không có đặc quyền chỉ có thể dùng connect scan. Tuy vậy, chế độ quét mặc định là SYN và nó yêu cầu người dùng có đặc quyền để chạy. SYN scan không cần hoàn tất TCP 3-way handshake; Thay vào đó, nó sẽ làm gãy kết nối khi nó nhận được phản hồi từ máy chủ. Vì chúng ta không thiết lập kết nối TCP, nó giảm khả năng việc quét bị ghi lại. Chúng ta có thể chọn loại quét này bằng việc dùng -sS. Hình dưới cho thấy cách quét TCP SYN hoạt động mà không hoàn tất 3-way handshake.

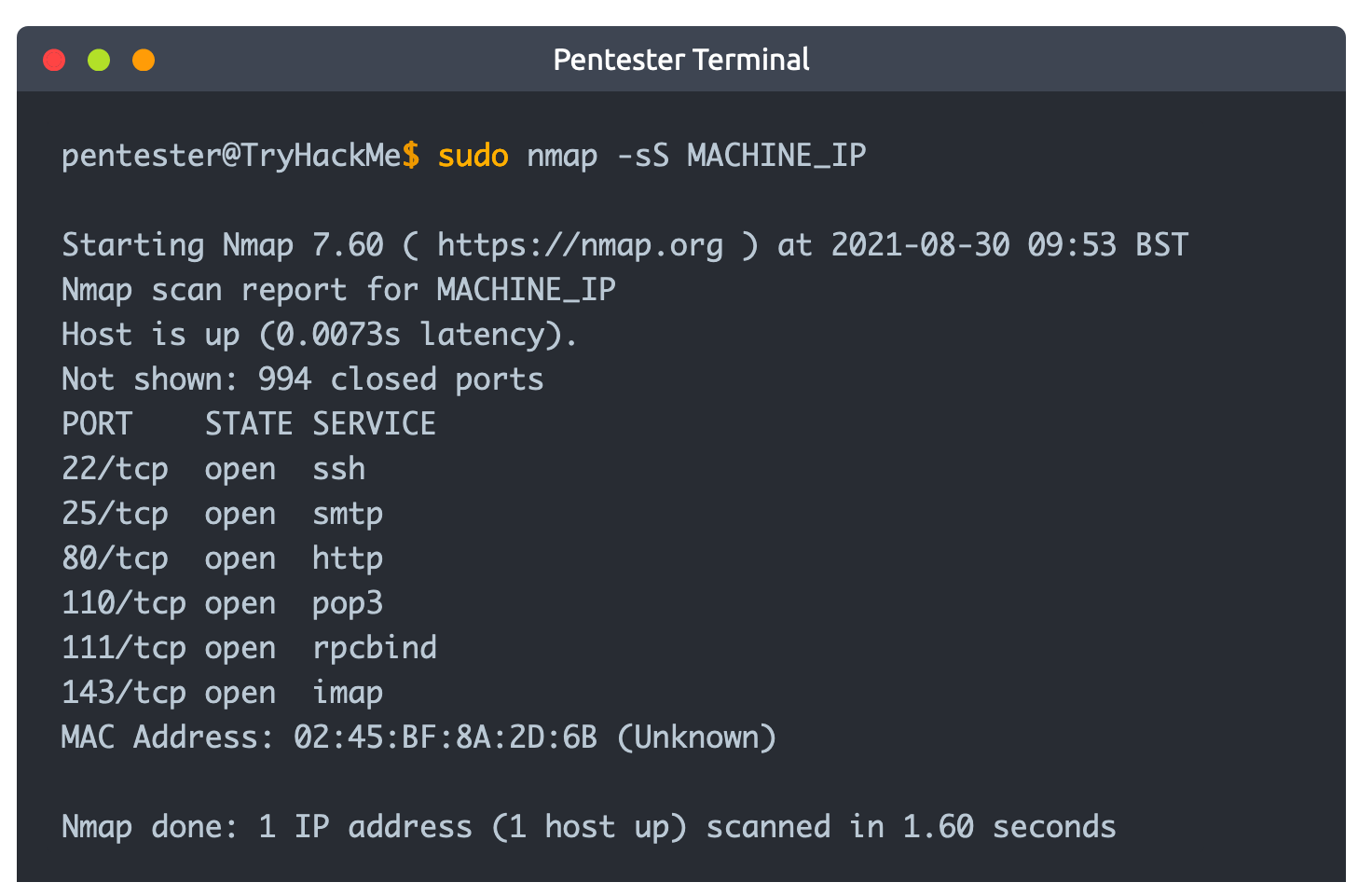




Sự khác nhau giữa hai loại quét:

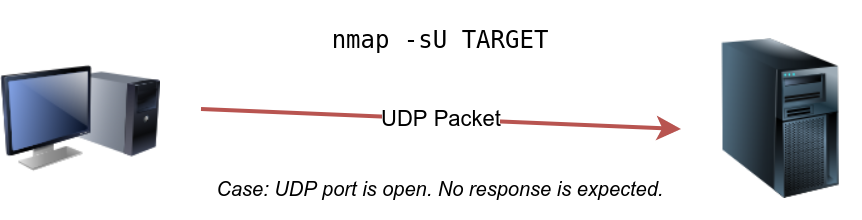


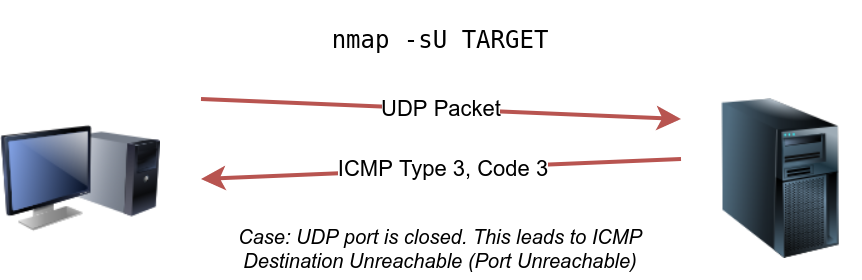
TCP SYN scan là chế độ quét mặc định khi chạy nmap với tư cách là người dùng có đặc quyền và nó là 1 lựa chọn đáng tin cậy. Nó khám phá những cổng đang mở nhanh hơn vì không phải thiết lập kết nối TCP



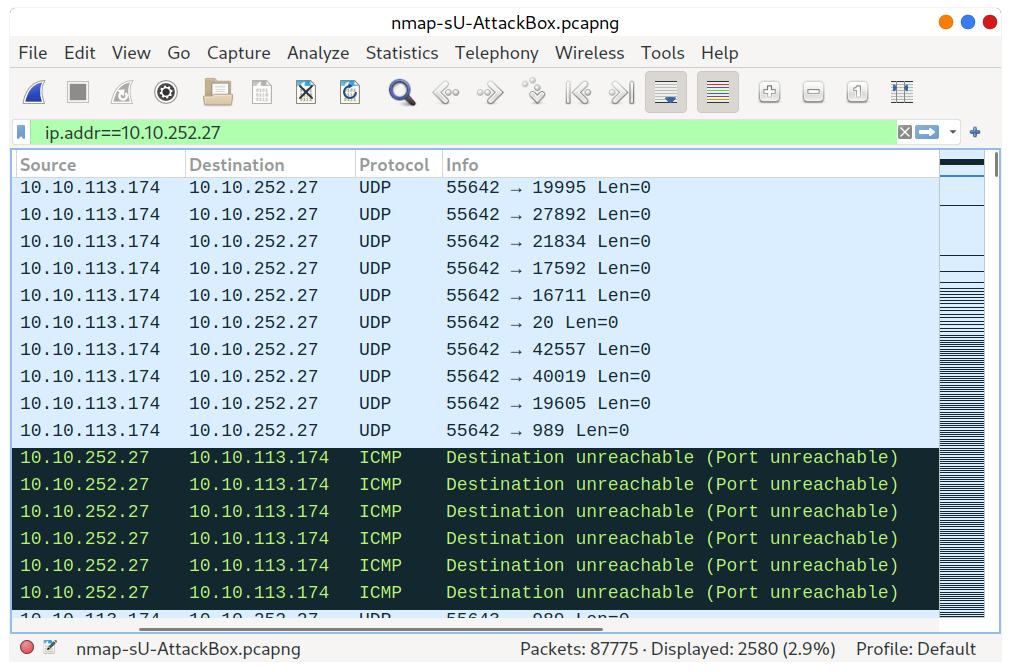
**UDP Scan**

UDP là 1 giao thức phi trạng thái. Do vậy, nó không yêu cầu bất cứ handshake nào để thiết lập kết nối. Chúng ta không thể đảm bảo 1 dịch vụ đang nghe ở cổng UDP sẽ phản hồi. Tuy nhiên, nếu 1 gói tin UDP được gửi đến 1 cổng đang đóng, thông báo lỗi ICMP sẽ được trả về. Bạn có thể quét UDP bằng -sU; Hơn nữa, bạn có thể kết hợp nó với TCP scan.

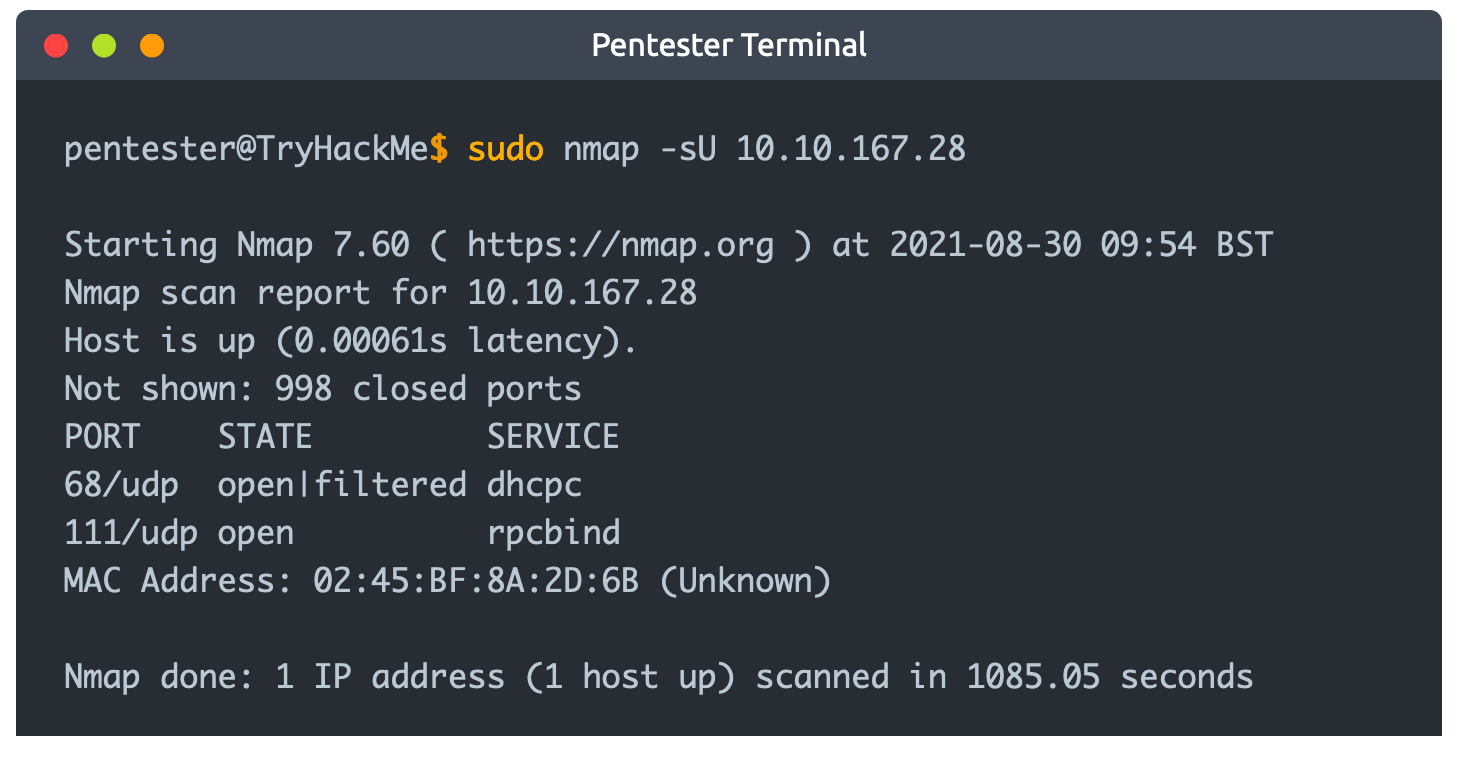




Trong Wireshark, chúng ta có thể thấy mỗi cổng đã đóng sẽ tạo ra 1 gói tin ICMP (port unreachable)



Scan UDP với máy chủ Linux này, chúng ta thấy cổng 111 đang mở. Mặc khác, Nmap không thể xác định UDP cổng 68 đang mở hay bị lọc.



**Phạm vi và hiệu suất:**

Bạn có thể chỉ định số cổng mà bạn muốn quét. Cùng xem 1 số ví dụ:

* Danh sách cổng: -p22,80,443
* Phạm vi cổng: -p1-1023

Bạn có thể yêu cầu quét tất cả cổng bằng việc sử dụng -p- (65535 cổng). Nếu bạn muốn quét 100 cổng phổ biến nhất thêm -F. Sử dụng - -top-ports 10 sẽ kiểm tra 10 cổng phổ biến nhất.

Bạn có thể kiểm soát thời gian quét bằng cách dùng -T<0-5>. -T0 là chậm nhất (paranoid), trong khi -T5 là nhanh nhất. Theo hướng dẫn của Nmap, có 6 mức độ:

* paranoid (0)
* sneaky (1)
* polite (2)
* normal (3)
* aggressive (4)
* insane (5)

Để tránh những cảnh báo của IDS, bạn có thể cân nhắc -T0 hoặc -T1. -T0 quét 1 cổng 1 lần và đợi 5 phút để quét cổng tiếp theo, vì vậy bạn có thể đoán việc quét một đối tượng mất bao nhiêu thời gian để hoàn thành. Nếu bạn không chỉ định thời gian, nmap mặc định dùng -T3.

Chú ý là -T5 là nhanh nhất; Tuy nhiên có thể ảnh hưởng đến mức độ chính xác của kết quả quét vì có những gói tin bị mất.

Chú ý là -T4 thường được dùng trong CTFs và khi học quét trên các đối tượng, trong khi -T1 thường được dùng trong thực tế, nơi mà khả năng ẩn mình rất quan trọng

Ngoài ra bạn có thể kiểm soát tốc đọ gói tin bằng –min-rate <number> và –max-rate <number>. Ví dụ, --max-rate 10 đảm bảo máy quét của bạn không gửi hơn 10 gói tin mỗi giây.

Hơn nữa, bạn có thể kiểm soát sự song song bằng –min-parallelism <numprobes> và –max-parallelism <numprobes>. Nmap thăm dò những đối tượng để khám phá những máy chủ đang chạy và cổng nào đang mở. Thăm dò sự song song chỉ định số lượng thăm dò có thể được chạy song song. Ví dụ, --min-parallelism=512 đẩy Nmap để duy trì ít nhất 512 đầu dò song song; 512 đầu dò liên quan đến việc khám phá máy chủ và những cổng đang mở.