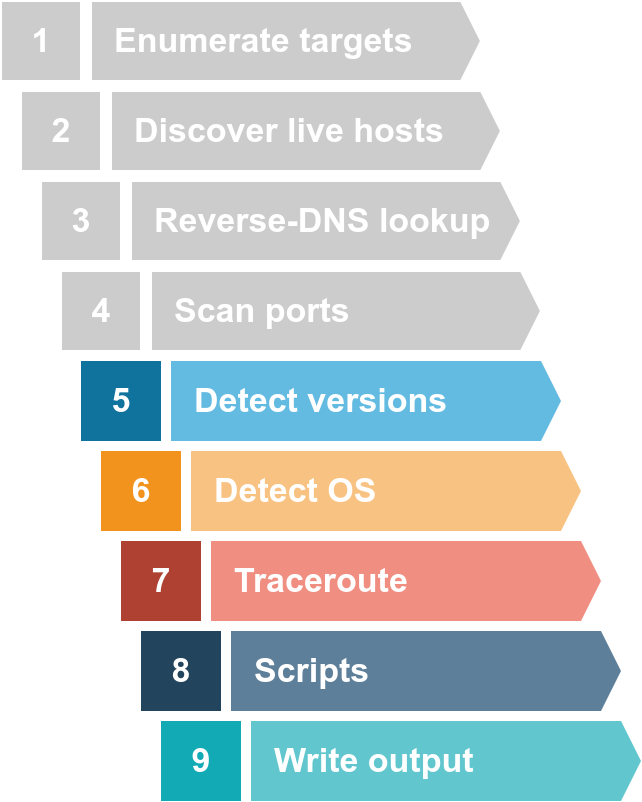
Trong phòng cuối, chúng ta sẽ tập trung vào cách Nmap có thể được dùng để:

* Phát hiện những phiên bản của các dịch vụ đang chạy
* Phát hiện hệ điều hành
* Chạy traceroute của Nmap
* Chạy những tập lệnh của Nmap
* Lưu trữ kết quả quét ở nhiều định dạng



**Phát hiện dịch vụ**

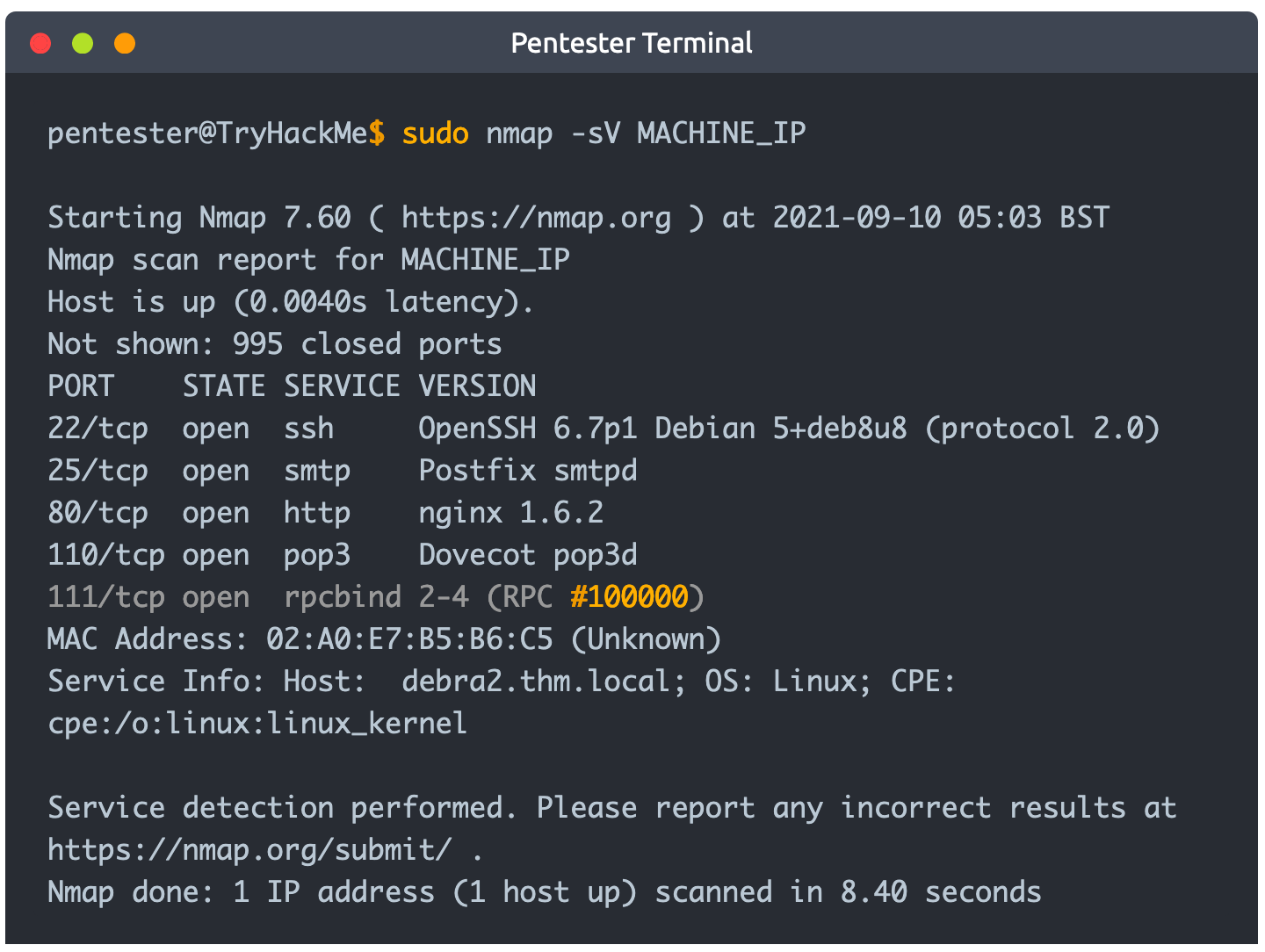
Khi Nmap khám phá những cổng đang mở, bạn có thể phát hiện những dịch vụ đang chạy.

Thêm -sV: Nmap sẽ thu thập và xác định dịch vụ và phiên bản cho những cổng đang mở.

Điều đáng chú ý là dùng -sV sẽ bắt Nmap thực hiện TCP 3-way handshake và thiết lập kết nối. Ngoài ra SYN scan -sS sẽ không khả thi khi -sV được dùng.

Thêm -sV sẽ thêm 1 cột mới hiển thị phiên bản của mỗi dịch vụ được phát hiện.

Ví dụ cổng 22 đang mở, thay vì 22/tcp open ssh, chúng ta nhận được 22/tcp open ssh OpenSSH 6.7p1 Debian 5+deb8u8 (protocol 2.0). Điều đáng chú ý là giao thức SSH được đoán là dịch vụ vì cổng TCP 22 đang mở; Nmap không cần kết nối với cổng 22 để kiểm tra. Tuy nhiên, -sV yêu cầu kết nối đến cổng đang mở để lấy được thông tin của dịch vụ và phiên bản của nó như nginx 1.6.2. Do đó, cột phiên bản không dễ đoán như cột dịch vụ.

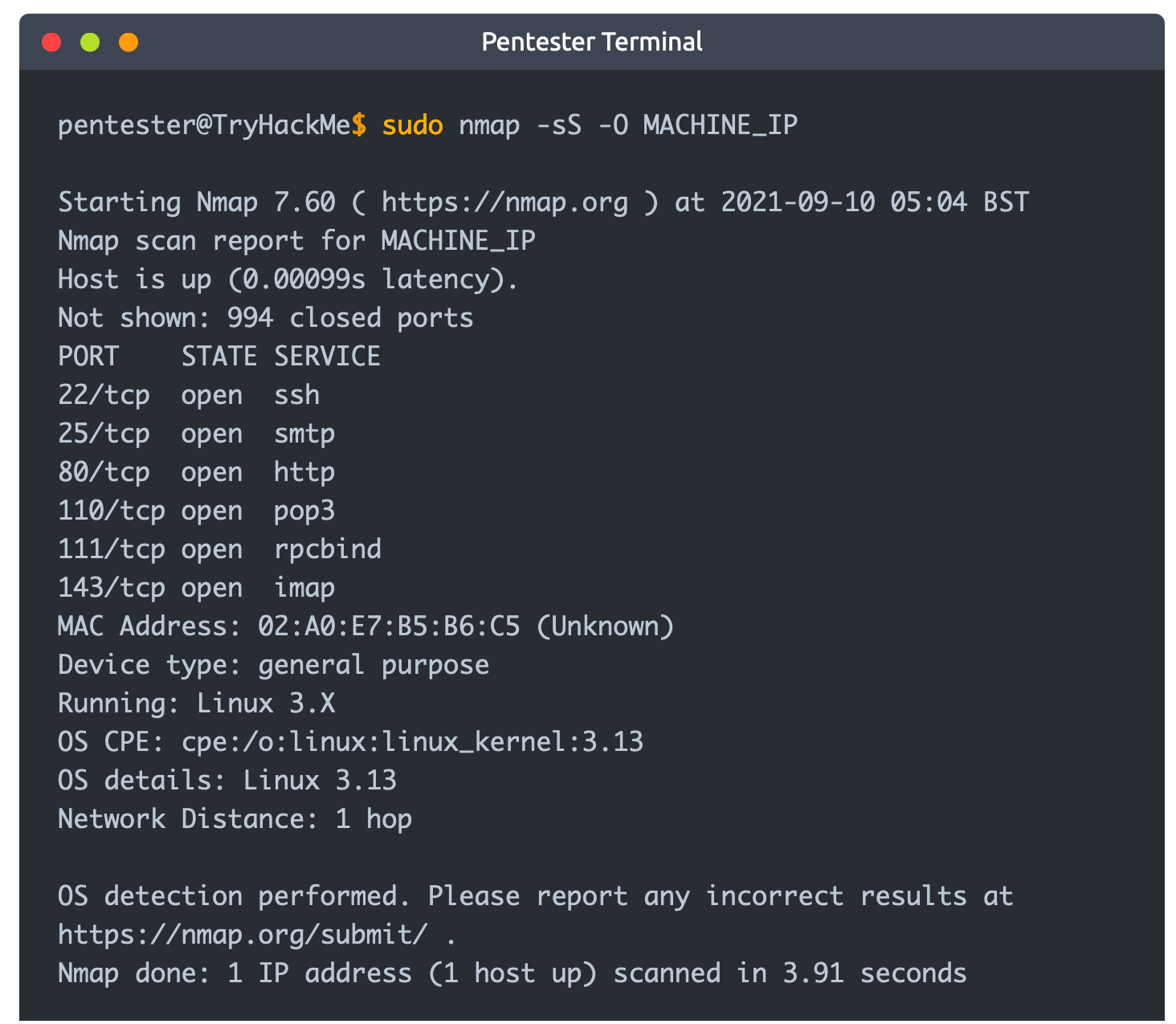


Chú ý là nhiều lựa chọn Nmap yêu cầu đặc quyền root.

**Phát hiện hệ điều hành và Traceroute**

**Phát hiện hệ điều hành:**

Nmap có thể phát hiện hệ điều hành dựa trên hành vi và dấu hiệu trong phản hồi của máy chủ. Phát hiện hệ điều hành có thể dùng -O. Ví dụ, nmap -sS -O MACHINE\_IP. Nmap phát hiện hệ điều hành là Linux 3.X và sau đó đoán nó đang chạy kernel 3.13



Phát hiện hệ điều hành rất tiện lợi, nhưng rất nhiều yếu tố có thể ảnh hưởng đến độ chính xác. Đầu tiên và quan trọng nhất, Nmap cần tìm ít nhất 1 cổng đang mở và 1 cổng đã đóng trên đối tượng để dễ đoán hơn. Hơn nữa, những dấu hiệu để đoán hệ điều hành có thể bị bóp méo vì sử dụng sự ảo hóa và công nghệ tương tự. Do đó, hãy luôn coi trọng phiên bản hệ điều hành.

**Traceroute:**

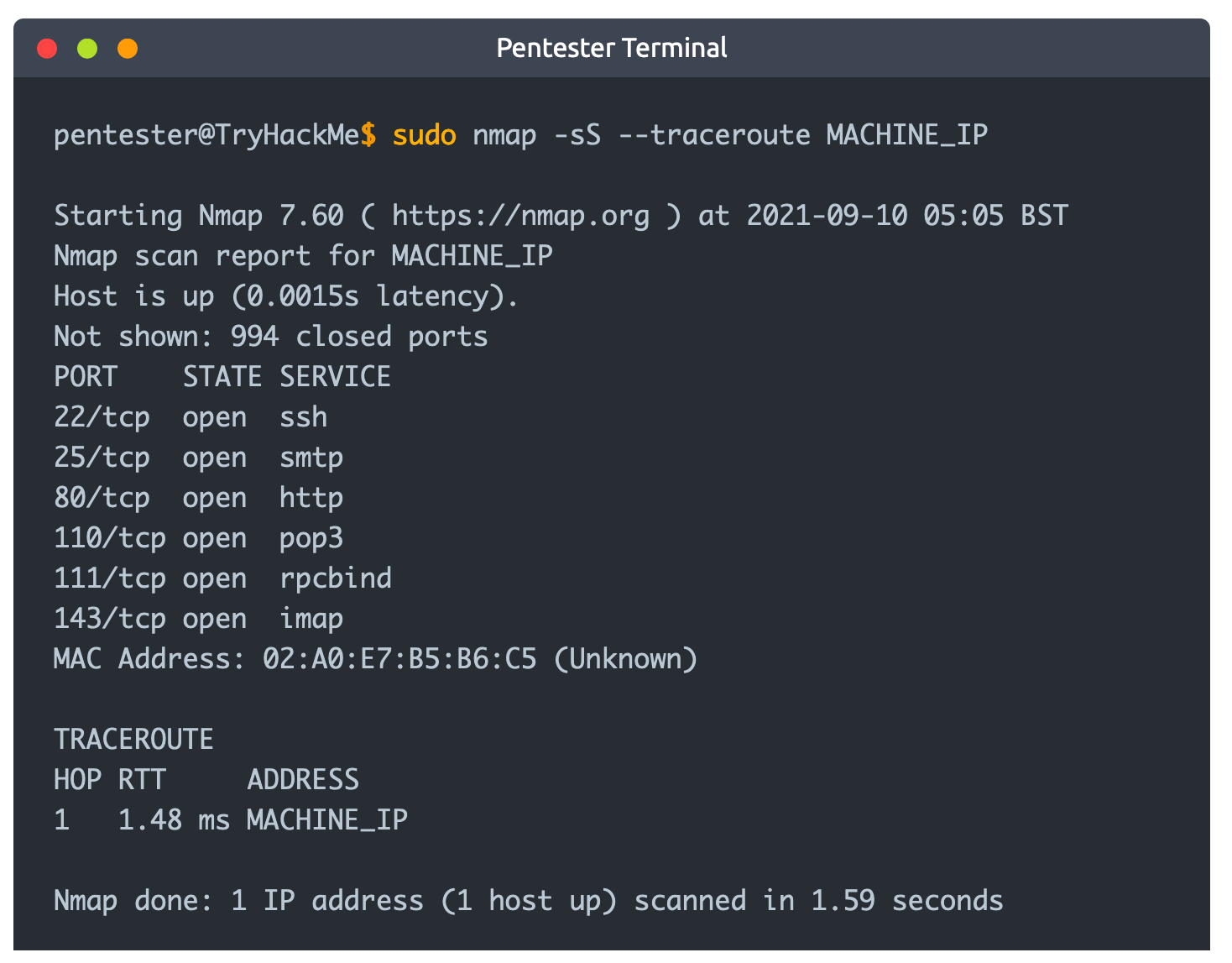
Nếu bạn muốn Nmap tìm những định tuyến giữa bạn và đối tượng, chỉ cần thêm

--traceroute. Lưu ý là traceroute của Nmap hoạt động hơi khác với lệnh traceroute. Traceroute tiêu chuẩn bắt đầu với 1 gói tin có TTL thấp (Time to Live) và tăng lên cho đến khi nó chạm được đối tượng. Traceroute của Nmap bắt đầu với gói tin có TTL cao và tiếp tục giảm nó.

Ở ví dụ sau, chúng ta thực thi lệnh

nmap -sS --traceroute MACHINE\_IP

Chúng ta có thể thấy không có routers/hops giữa hai thiết bị được kết nối trực tiếp với nhau.

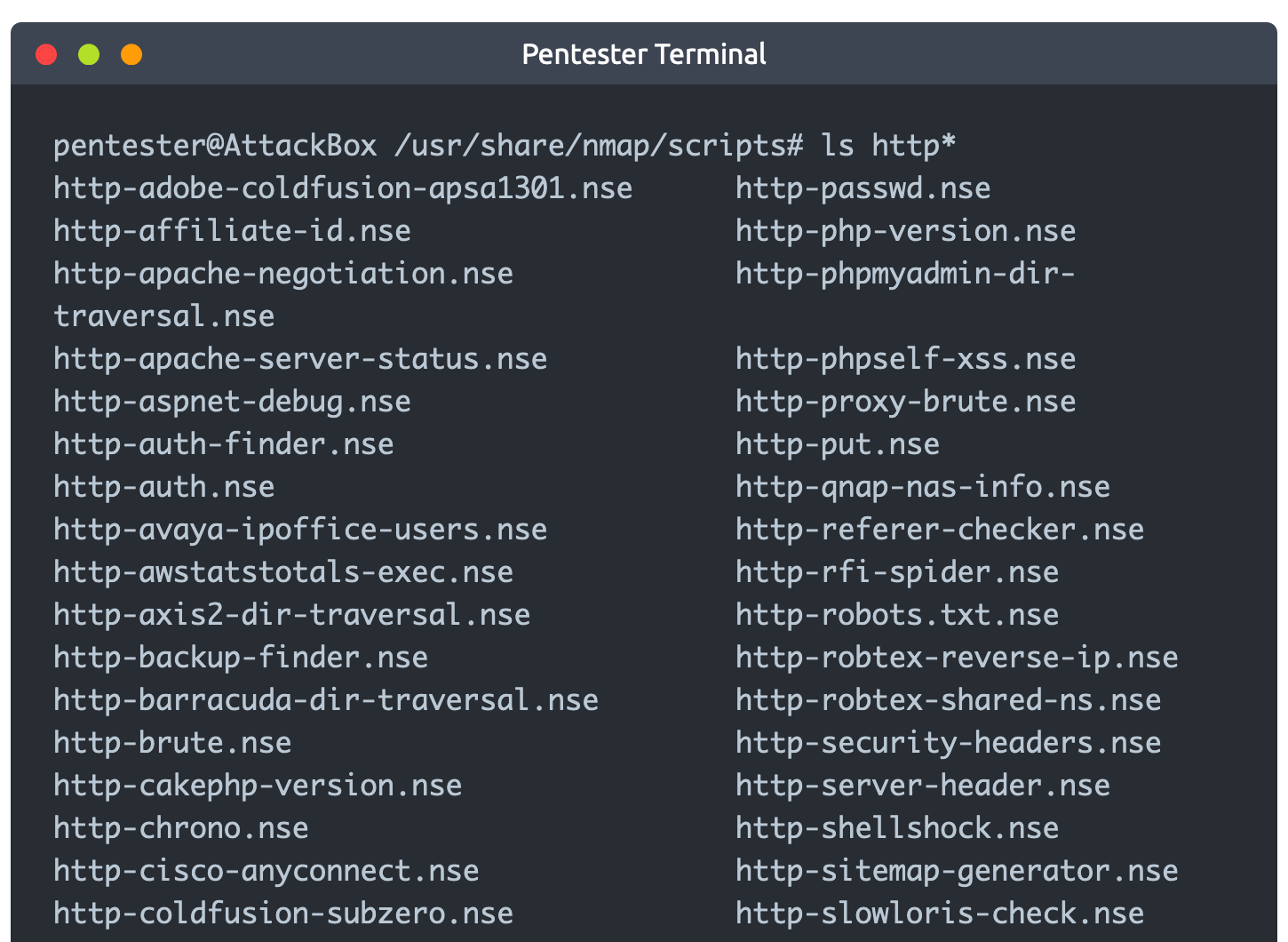


Điều đáng lưu ý là rất nhiều bộ định tuyến được cấu hình không gửi ICMP Time-to-Live exceeded, sẽ ngăn chặn chúng ta khám phá địa chỉ IP của chúng.

**Nmap Scripting Engine (NSE)**

Script là 1 tập lệnh không cần được thực thi. Nói cách khác, nó giữ ở định dạng con người có thể đọc được và không cần chuyển qua ngôn ngữ máy. Rất nhiều chương trình cung cấp thêm chức năng qua những tập lệnh; Hơn nữa, scripts giúp tùy chỉnh chức năng không tồn tại qua những câu lệnh đã được dựng sẵn. Tương tự, Nmap cũng hỗ trợ những tập lệnh qua ngôn ngữ Lua. 1 phần của Nmap, NSE là 1 trình thông dịch Lua cho phép Nmap thực thi tập lệnh Nmap được viết bằng ngôn ngữ Lua. Tuy nhiên, chúng ta không cần học Lua để sử dụng Nmap scripts.

Việc cài đặt Nmap mặc định đã có sẵn 600 scripts.



Bạn có thể chỉ định sử dụng những tập lệnh đã được cài đặt. Hơn nữa, bạn có thể cài đặt thêm những tập lệnh của người dùng khác và dùng nó để quét.

Bạn có thể chạy scripts trong danh mục mặc định bằng --script=default hay -sC. Ngoài ra còn có những danh mục khác như auth, broadcast, brute, default, discovery, dos, exploit,…

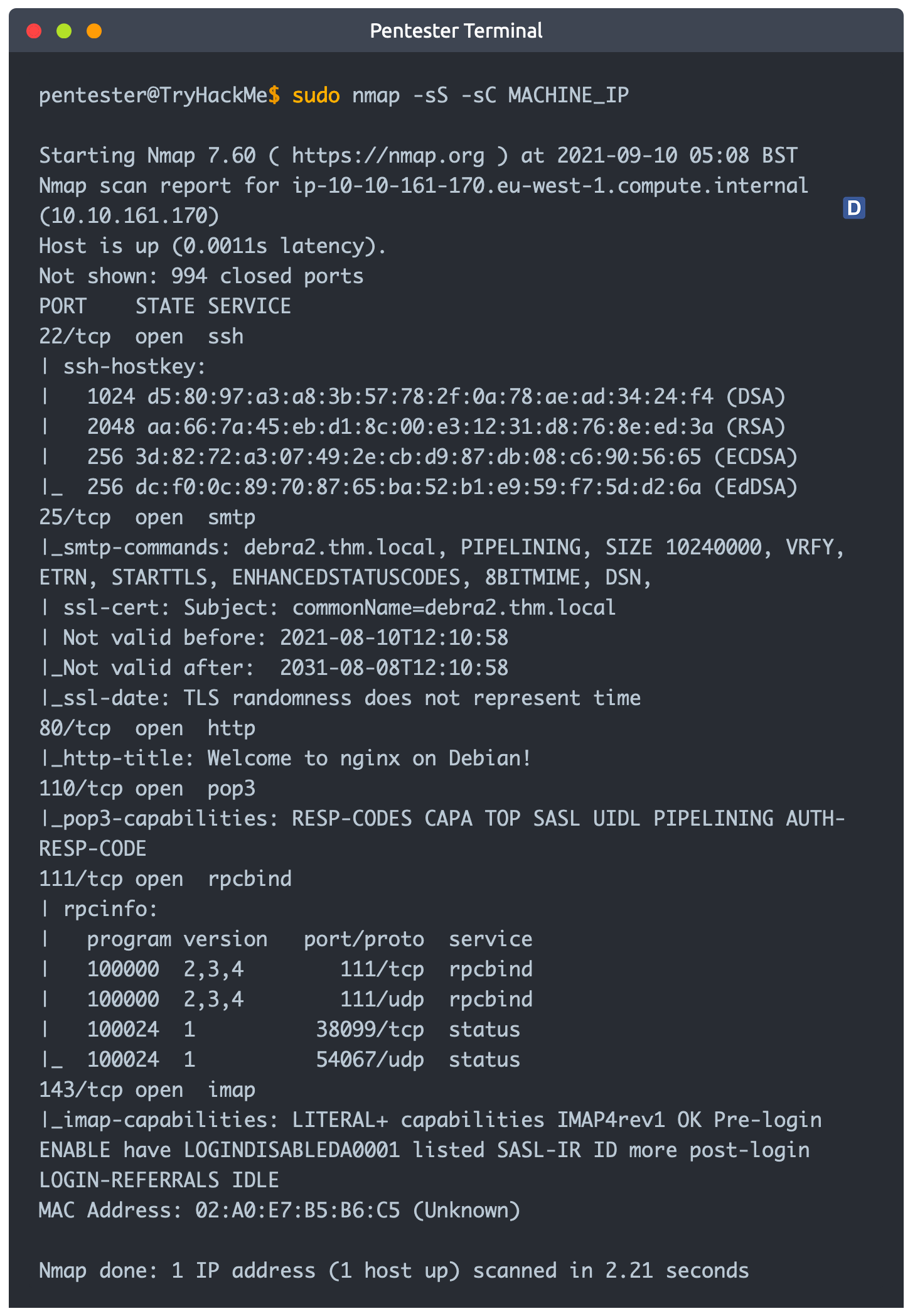
| **Script Category** | **Description** |
| --- | --- |
| auth | Authentication related scripts |
| broadcast | Discover hosts by sending broadcast messages |
| brute | Performs brute-force password auditing against logins |
| default | Default scripts, same as -sC |
| discovery | Retrieve accessible information, such as database tables and DNS names |
| dos | Detects servers vulnerable to Denial of Service (DoS) |
| exploit | Attempts to exploit various vulnerable services |
| external | Checks using a third-party service, such as Geoplugin and Virustotal |
| fuzzer | Launch fuzzing attacks |
| intrusive | Intrusive scripts such as brute-force attacks and exploitation |
| malware | Scans for backdoors |
| safe | Safe scripts that won’t crash the target |
| version | Retrieve service versions |
| vuln | Checks for vulnerabilities or exploit vulnerable services |

Một vài scripts thuộc về nhiều hơn 1 danh mục. Hơn nữa, một vài scripts thực hiện những cuộc tấn công dồn dập chống lại các dịch vụ, trong khi đó số khác thực hiện tấn công DOS và khai thác các hệ thống. Do đó, phải cẩn thận khi chọn script để chạy nếu bạn không muốn làm hư các dịch vụ và khai thác chúng.

Chúng ta dùng Nmap để chạy SYN scan với MACHINE\_IP và thực thi những tập lệnh mặc định.

sudo nmap -sS -sC MACHINE\_IP

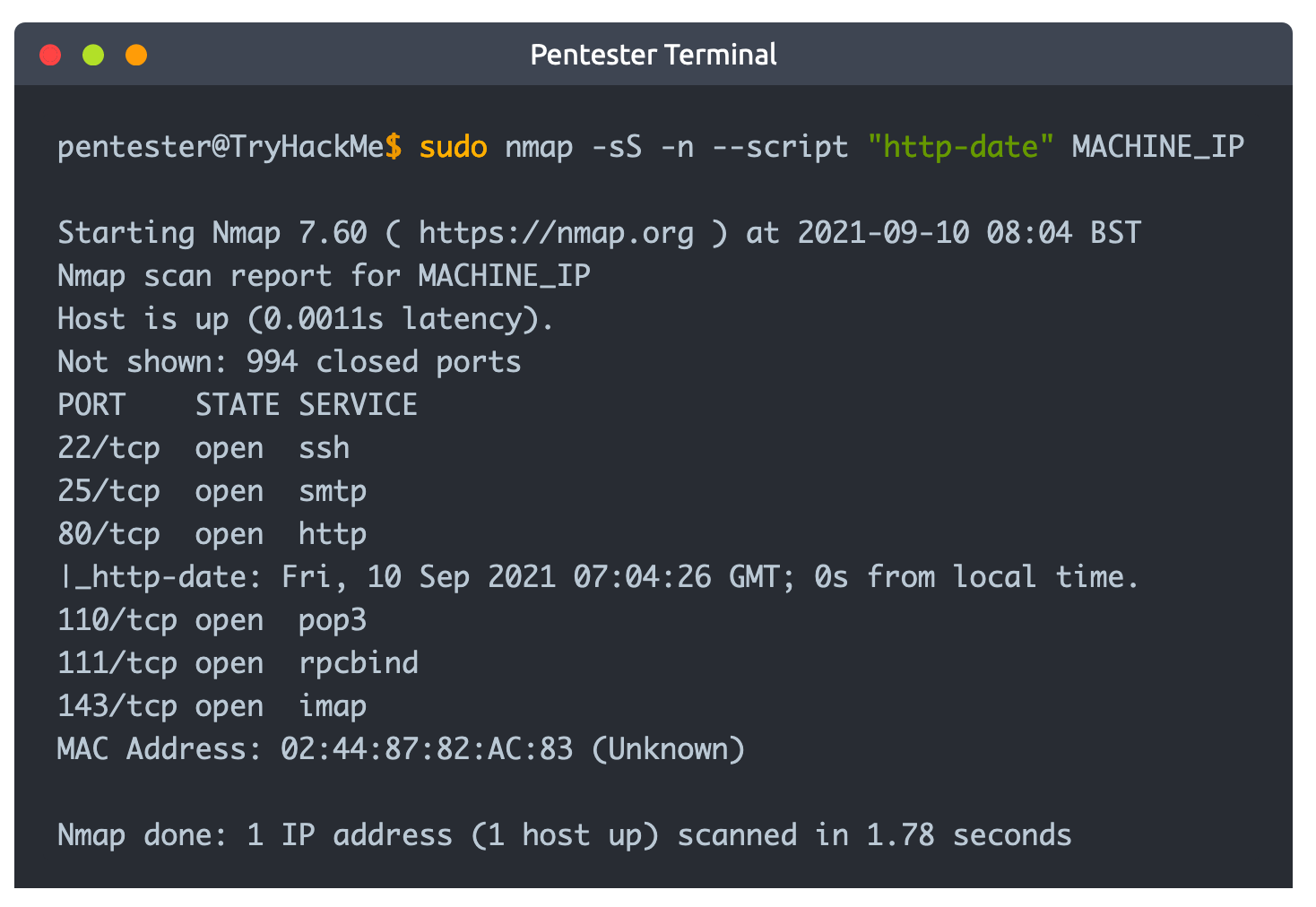
-sC sẽ đảm bảo Nmap thực thi những tập lệnh mặc định theo SYN scan. Có một vài thông tin mới xuất hiện bên dưới. Nhìn vào dịch vụ SSH ở cổng 22; Nmap đã phục hồi 4 puclic keys liên quan đến việc chạy máy chủ. Xem xét 1 ví dụ khác, dịch vụ HTTP ở cổng 80; Nmap truy suất tiêu đề của trang mặc định. Chúng ta có thể thấy trang đã được để mặc định.



Bạn cũng có thể chỉ định tập lệnh bằng cách --script “SCRIPT-NAME” hay --script “fpt\*”, sẽ chứa fpt-brute. Nếu bạn không chắc chắn tập lệnh có thể làm gì bạn có thể mở tập tin để xem. Trong trường hợp fpt-brute, nó nhấn mạnh “tấn công dồn dập mật khẩu với các máy chủ FTP”. Bạn phải cẩn thận vì những tập lệnh này rất dễ bị phát hiện xâm nhập. Hơn nữa, một vài scripts chỉ phù hợp với một số máy chủ nhất đinh, nếu chọn ngẫu nhiên, sẽ mất thời gian mà không có lợi gì. Phải đảm bảo bạn được phân quyền kiểm thử trên máy chủ đích.

Cùng xem xét 1 tập lệnh nhẹ, http-date, chúng ta đoán sẽ truy suất ngày và giờ của máy chủ http.

sudo nmap -sS -n --script “http-date” MACHINE\_IP



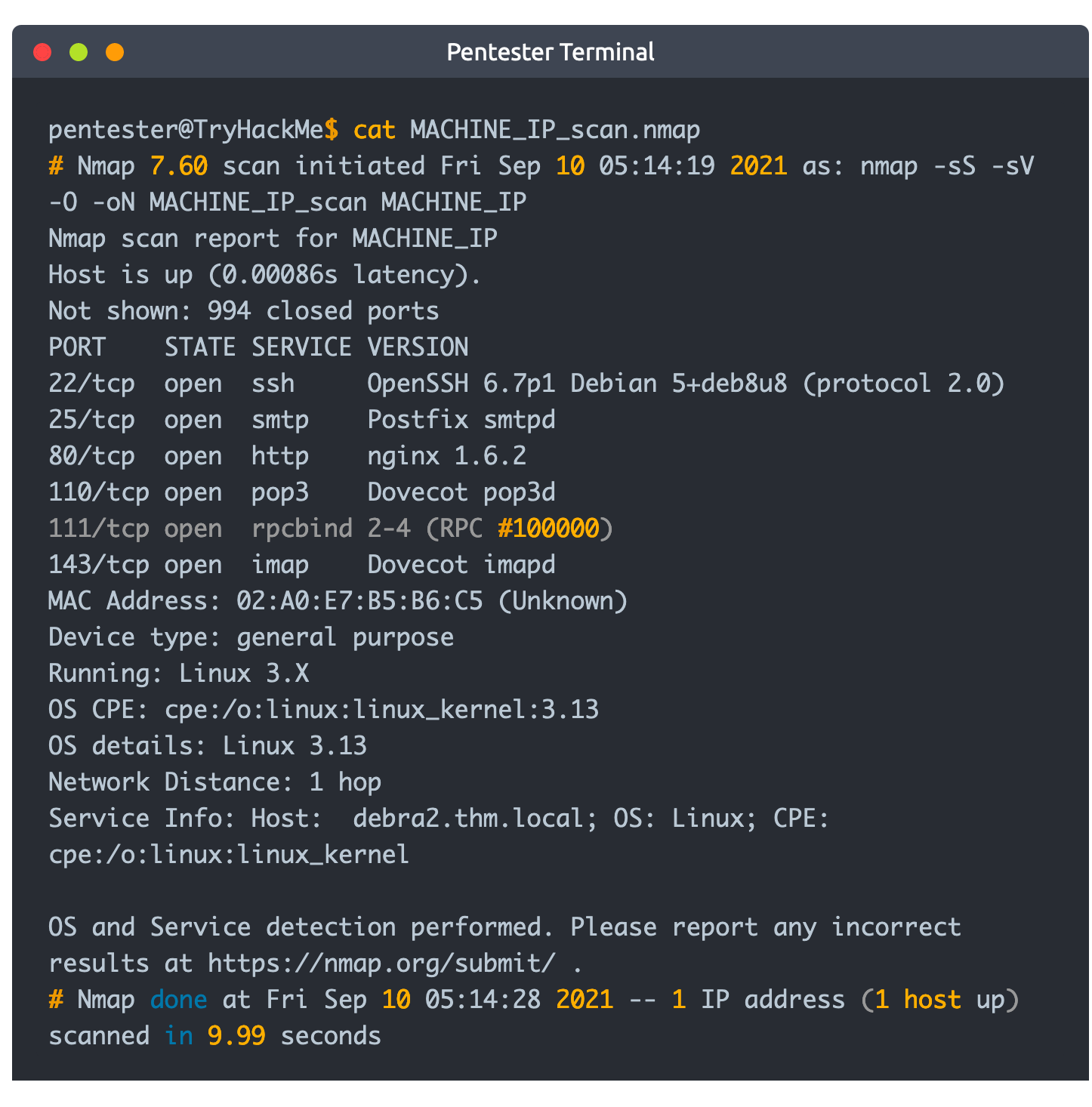
**Saving Output**

Khi bạn chạy Nmap scan, chỉ hợp lí khi lưu kết quả trong 1 tập tin. Việc chọn và áp dụng những qui ước để đặt tên cho tập tin của bạn rất quan trọng. Số lượng tập tin có thể ngày càng lớn và cản trở khả năng tìm thấy kết quả đã quét trước đó của bạn. Có ba định dạng chính sau:

1. Normal
2. Grepable (grepable)
3. XML

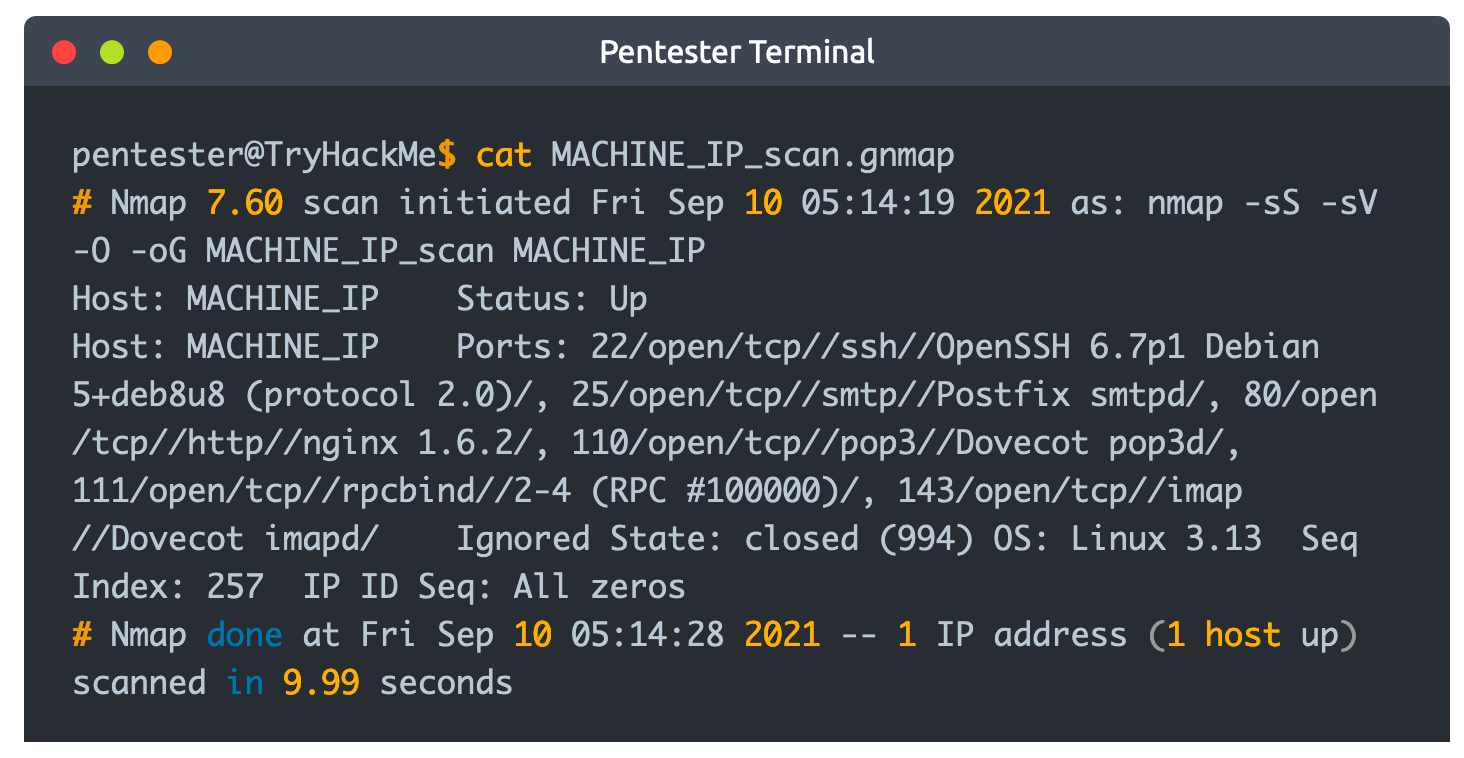
**Normal:**

Định dạng bình thường giống như đầu ra bạn thấy trên màn hình khi quét 1 đối tượng. Bạn có thể lưu quá trình quét của mình ở định dạng bình thường bằng việc dùng -oN FILENAME; N đại diện cho normal.

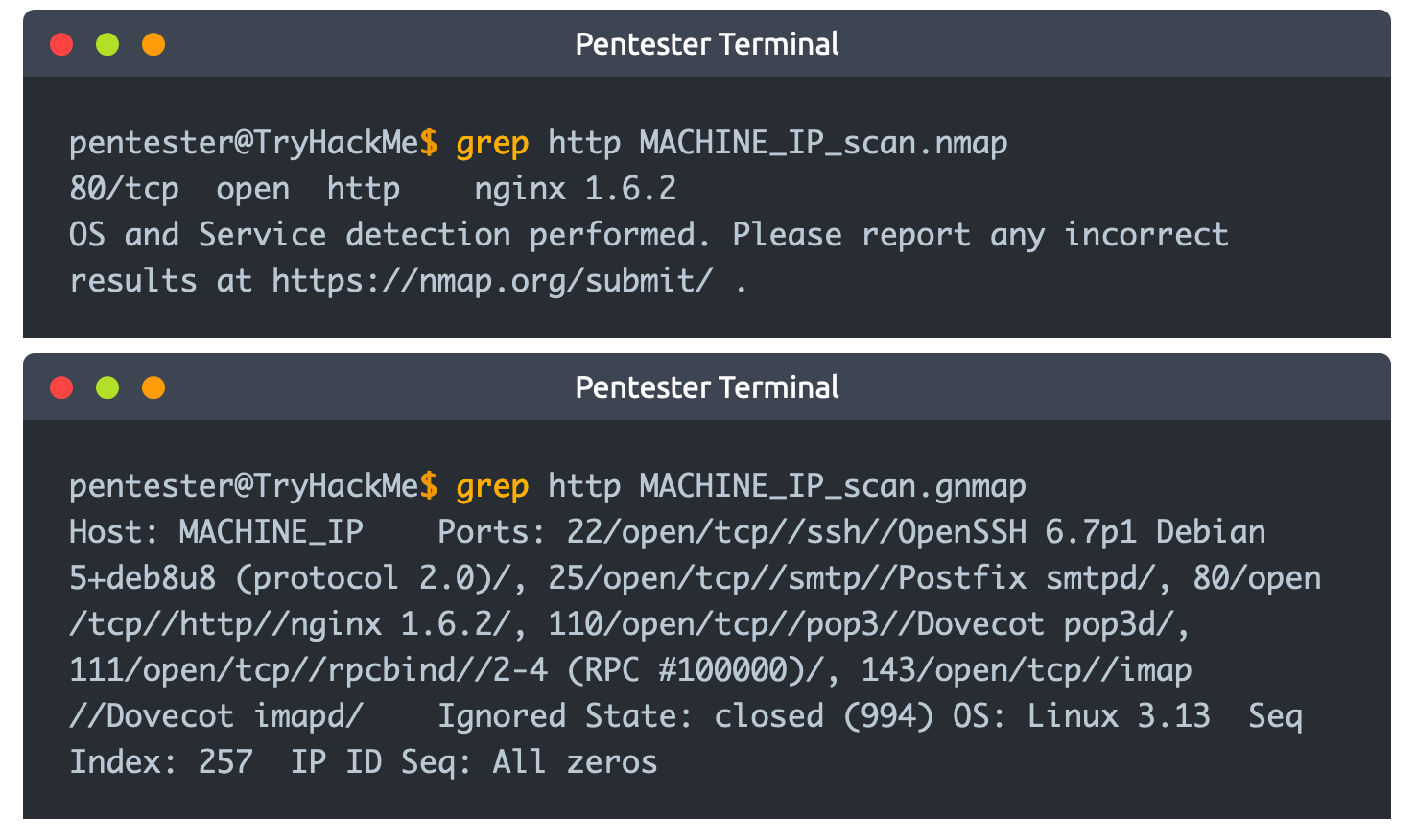


**Grepable:**

Nó sàng lọc đầu ra của quá trình quét bằng những từ khóa đặc biệt. Bạn có thể lưu kết quả quét ở định dạng Grep bằng việc dùng -oG FILENAME. Kết quả bình thường có 21 dòng; tuy nhiên ở định dạng grep chỉ có 4 dòng. Lí do chính là Nmap muốn làm cho mỗi dòng có ý nghĩa và đầy đủ. Ở định dạng này, những dòng rất dài và bất tiện để đọc.



Một ví dụ dùng grep nữa là grep KEYWORD TEXT\_FILE; Lệnh này sẽ hiển thị tất cả các dòng chứa từ khóa được cung cấp. Bạn sẽ chú ý thấy định dạng này không cung cấp địa chỉ IP của máy chủ. Thay vào đó, nó trả về 80/tcp open http nginx 1.6.2, rất bất tiện nếu bạn đang sàng lọc kết quả quét của nhiều hệ thống. Tuy nhiên, cái sau cung cấp đủ thông tin, chẳng hạn như địa chỉ IP của máy chủ.



**XML:**

Bạn có thể lưu kết quả quét ở định dạng XML bằng việc dùng -oX FILENAME. Định dạng XML sẽ là tiện lợi nhất để xử lí đầu ra trong những chương trình khác.

**Summary:**

| **Option** | **Meaning** |
| --- | --- |
| -sV | determine service/version info on open ports |
| -sV --version-light | try the most likely probes (2) |
| -sV --version-all | try all available probes (9) |
| -O | detect OS |
| --traceroute | run traceroute to target |
| --script=SCRIPTS | Nmap scripts to run |
| -sC or --script=default | run default scripts |
| -A | equivalent to -sV -O -sC --traceroute |
| -oN | save output in normal format |
| -oG | save output in grepable format |
| -oX | save output in XML format |
| -oA | save output in normal, XML and Grepable formats |