TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN
KHOA MẠNG MÁY TÍNH VÀ TRUYỀN THÔNG

BÁO CÁO THỰC HÀNH

Bài thực hành số 17: Metasploit

Môn học: Hệ tính toán phân bố

Lớp: NT533.Q12.2

THÀNH VIÊN THỰC HIỆN (Nhóm 01):

STT	Họ và tên	MSSV	Điểm tự đánh giá
1	Nguyễn Tiến Phát	23521147	10

ĐÁNH GIÁ KHÁC:

Tổng thời gian thực hiện	

Phần bên dưới của báo cáo này là báo cáo chi tiết của sinh viên thực hiện

Bài thực hành số 17: Metasploit

MỤC LỤC

Bài thực hành số 17: Metasploit

A. BÁO CÁO CHI TIẾT

I. Thực hiện chi tiết

Task 1: Link Metasploit Framework to database

1. Log into Kali Linux machine and open a Terminal window.

Mục tiêu:

- Khởi động môi trường Kali Linux và kiểm tra thông tin hệ thống trước khi chạy Metasploit.

Cách thực hiện:

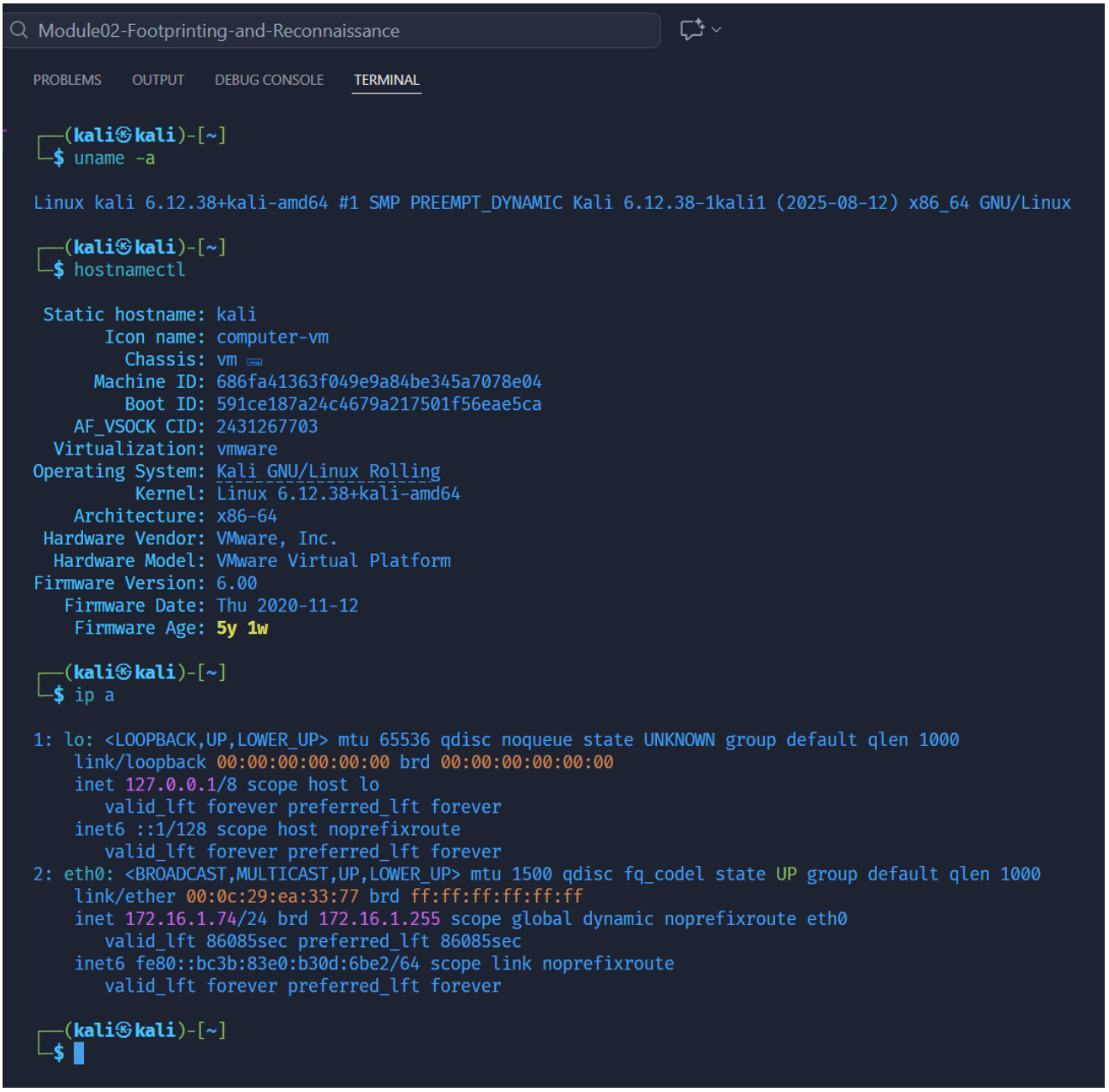
- Đăng nhập vào máy ảo Kali Linux.
- Mở Terminal và sử dụng các lệnh:

```
uname -a
hostnamectl
ip a
```

Kết quả thu được:

- Hệ thống hiển thị thông tin phiên bản Kernel, hostname của máy Kali, kiến trúc CPU và card mạng.
- Xác định địa chỉ IP của máy là **172.16.1.74/24**, tương ứng với subnet **172.16.1.0/24** – đây là dải mạng sẽ dùng cho các bước quét tiếp theo.

Bài thực hành số 17: Metasploit



2. Type service postgresql start and hit Enter.

Mục tiêu:

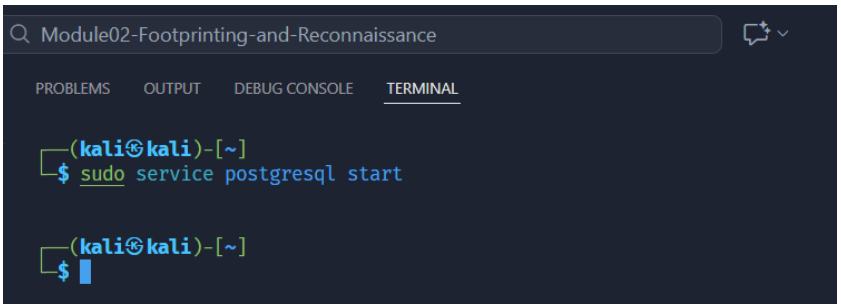
- Khởi động dịch vụ cơ sở dữ liệu PostgreSQL mà Metasploit sử dụng để lưu trữ dữ liệu footprinting.

```
sudo service postgresql start
sudo service postgresql status
```

Kết quả thu được:

- PostgreSQL hoạt động và sẵn sàng kết nối với Metasploit Framework.
- Trạng thái dịch vụ: **active (running)**.

Bài thực hành số 17: Metasploit



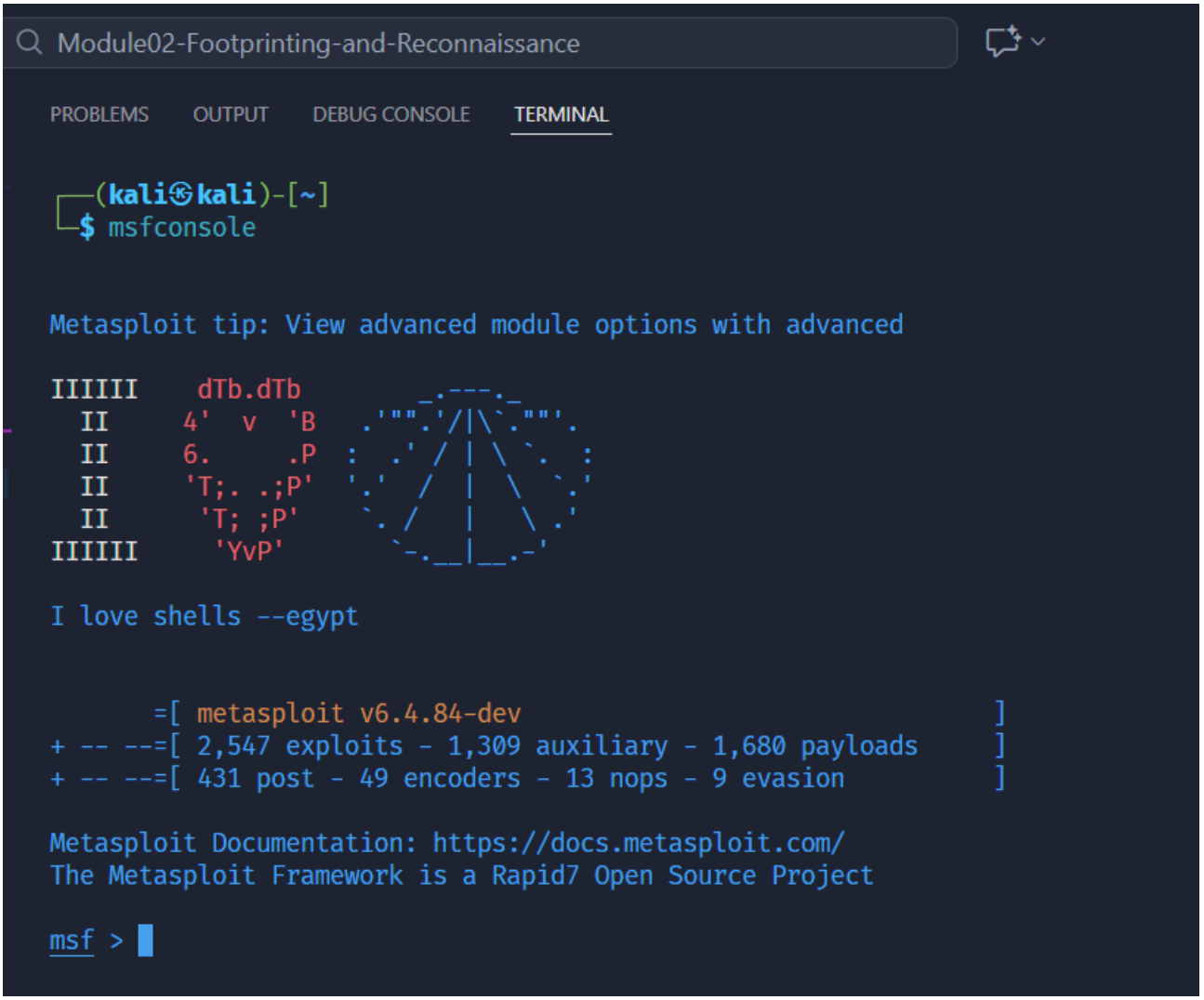
3. Now type msfconsole and hit Enter to launch Metasploit.

Mục tiêu của bước này

- Mở công cụ Metasploit Framework Console (msfconsole) – giao diện dòng lệnh chính của Metasploit.
- Xác nhận rằng Metasploit hoạt động đúng, load thành công các module exploit, auxiliary, payload.
- Chuẩn bị nền tảng cho các bước footprinting và reconnaissance tiếp theo trong bài lab.

Trong terminal của Kali, nhập lệnh:

```
msfconsole
```



Bài thực hành số 17: Metasploit

Kết quả thu được:

- Metasploit khởi động thành công và hiển thị banner ASCII.
- Số lượng module hiện có (exploits, auxiliary, payloads…) được liệt kê theo phiên bản framework.

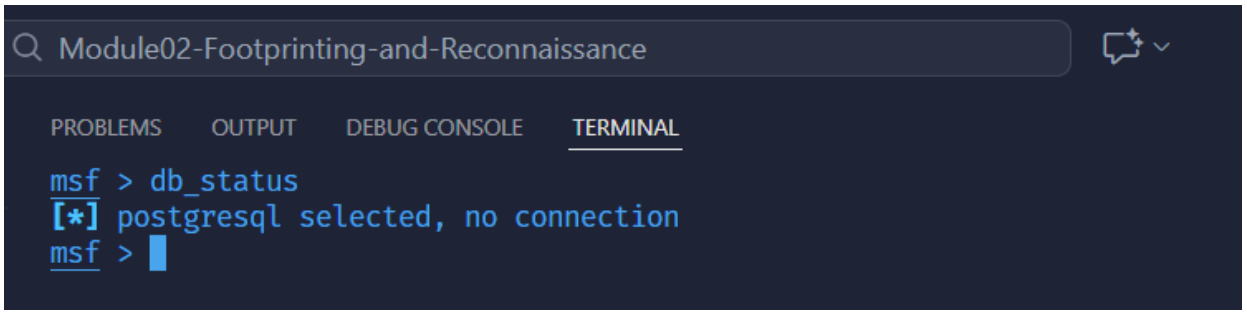
4. Msf command line appears.

Type db_status and hit Enter to check if Metasploit is connected to the database successfully. If you get the message "postgersql selected, no connection" then the database did not connect to msf.
Note: If the message you get is "postgresql connected to msf' then skip to step #6

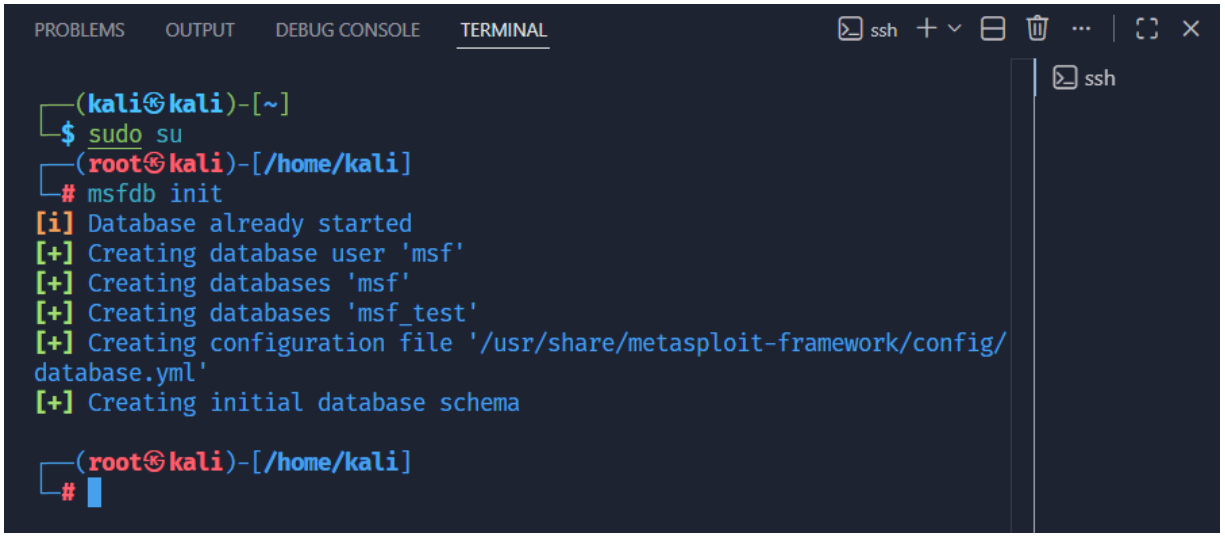
Mục tiêu: Kiểm tra xem Metasploit đã kết nối thành công với PostgreSQL hay chưa.

Kết quả thu được:

Trong trường hợp này, Metasploit **chưa kết nối** được tới PostgreSQL.
Hệ thống hiển thị:



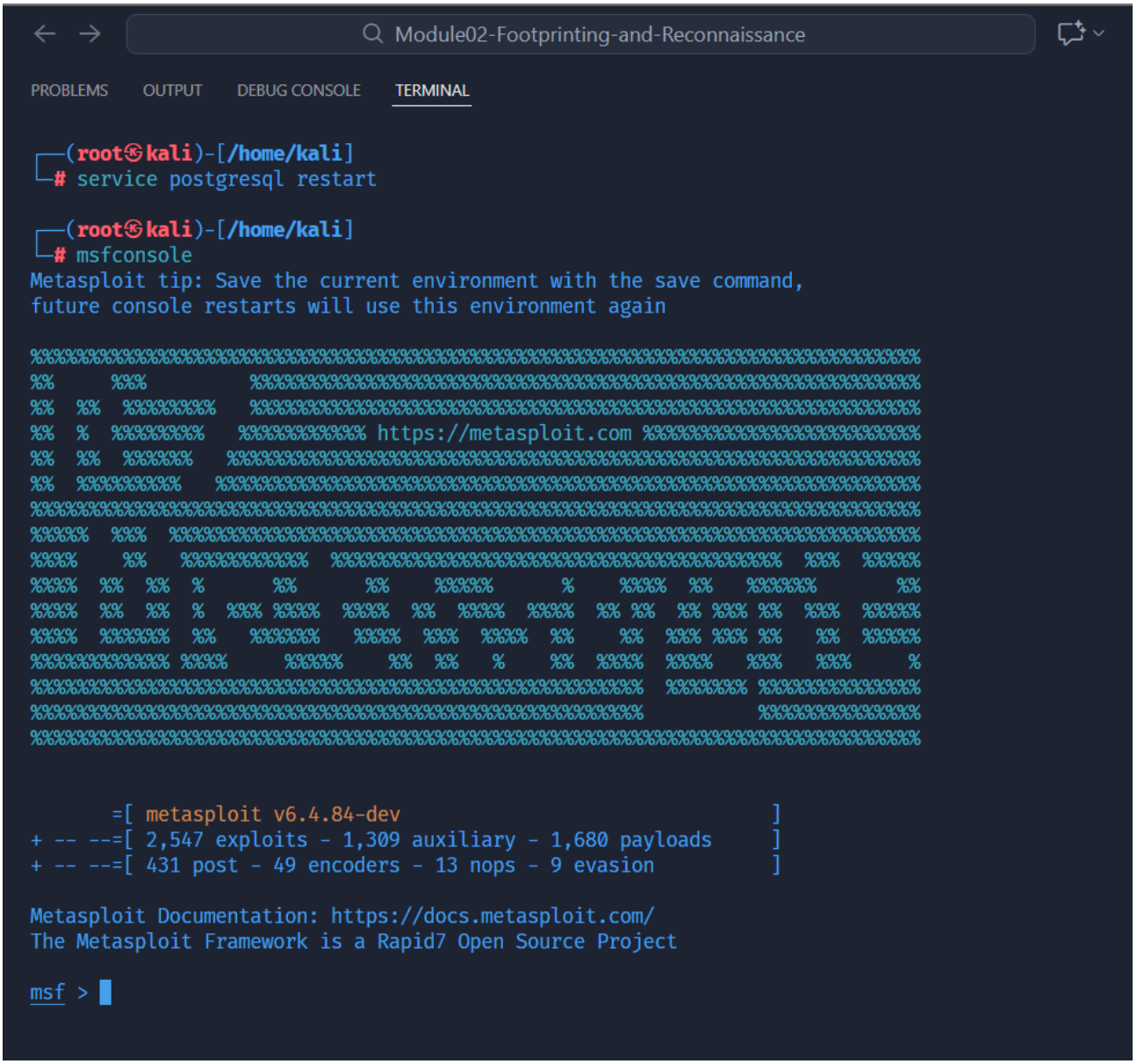
5. Exit the metasploit framework by typing exit and press Enter. Then to initiate the database type msfdb init and press Enter.



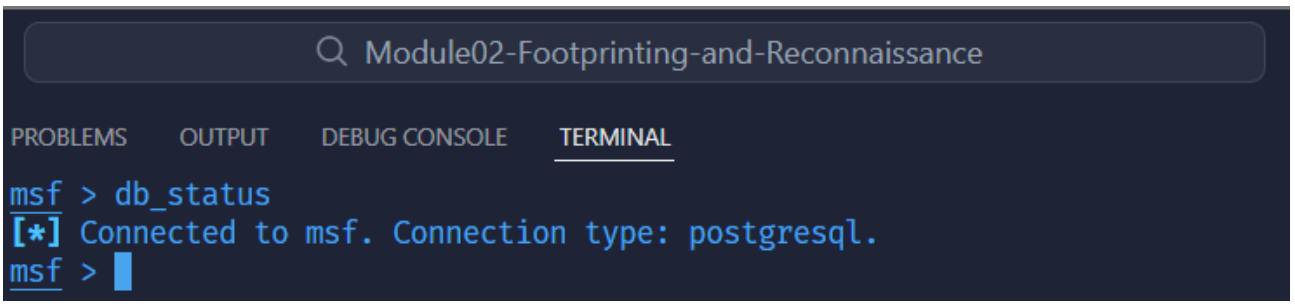
6. Restart the postgresql service

Type service postgresql restart and press Enter. Now start the Metasploit Framework again by typing msfconsole and pressing Enter.

Bài thực hành số 17: Metasploit



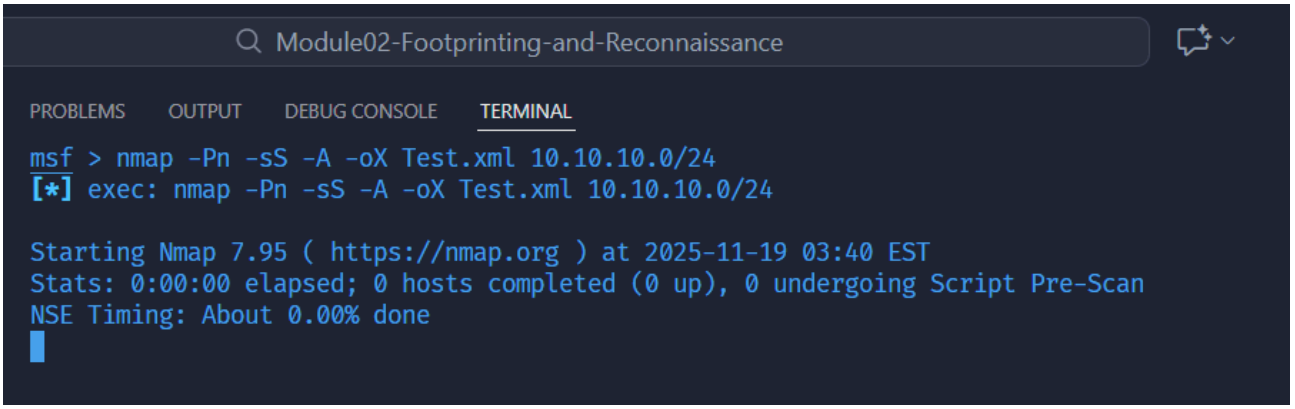
7. Check the database status by typing db_status and press Enter. This time the database should successfully connect to msf as shown in the screenshot.



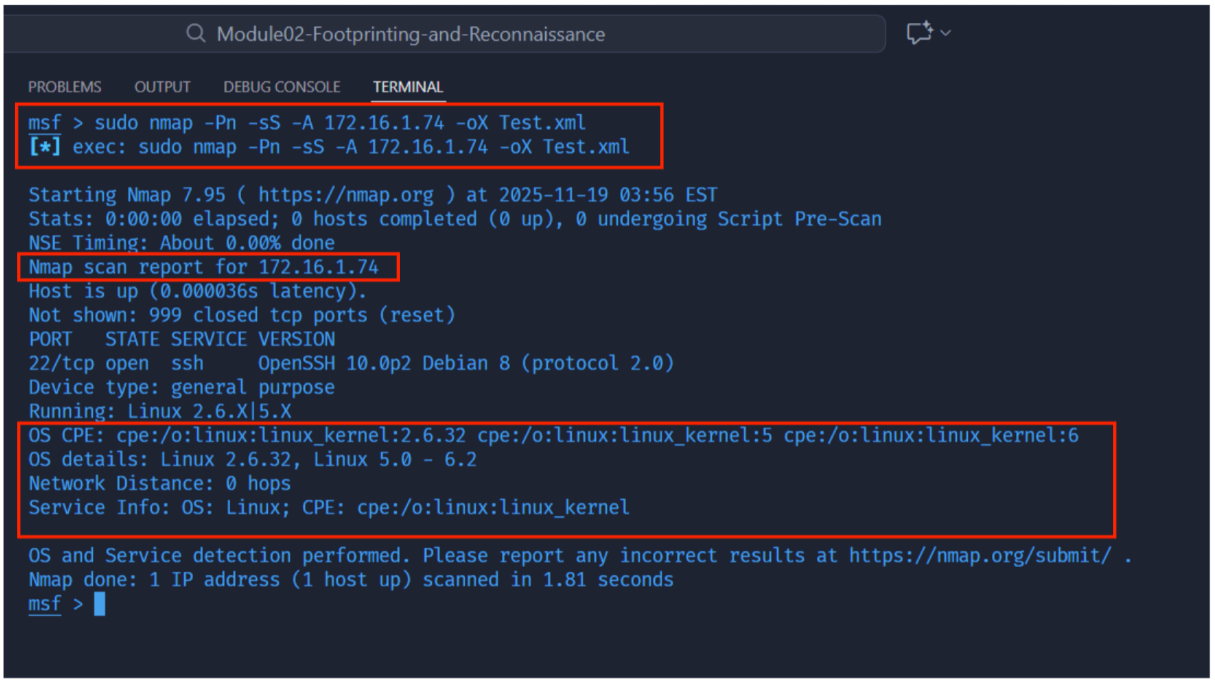
Bài thực hành số 17: Metasploit

Task 2: Find Alive Hosts

8. Type nmap -Pn -sS-A-oX Test 10.10.10.0/24 and hit Enter to scan the subnet as shown in the screenshot.



9. Nmap starts scanning the subnet and starts displaying the results on the screen. It takes approximately 10 minutes for the scan to finish.



Phân tích kết quả:

- Lệnh Nmap đã quét thành công host 172.16.1.74.
- Host đang hoạt động và chỉ mở một cổng duy nhất là **SSH (22/tcp)**.
- Dịch vụ chạy là **OpenSSH 10.0p2**, không phát hiện các dịch vụ khác.
- Hệ điều hành được nhận diện là **Linux kernel 5.x – 6.2**, phù hợp với hệ thống Kali Linux.
- Mạng có duy nhất 1 thiết bị hoạt động trong subnet 172.16.1.0/24.

→ Kết quả quét cho thấy hệ thống an toàn, ít lộ bề mặt tấn công, chỉ cung cấp dịch vụ SSH mặc định.

Bài thực hành số 17: Metasploit

10. Type db_import Test and hit Enter to import the Nmap results from the database.

Kết quả thu được:

Metasploit phản hồi:

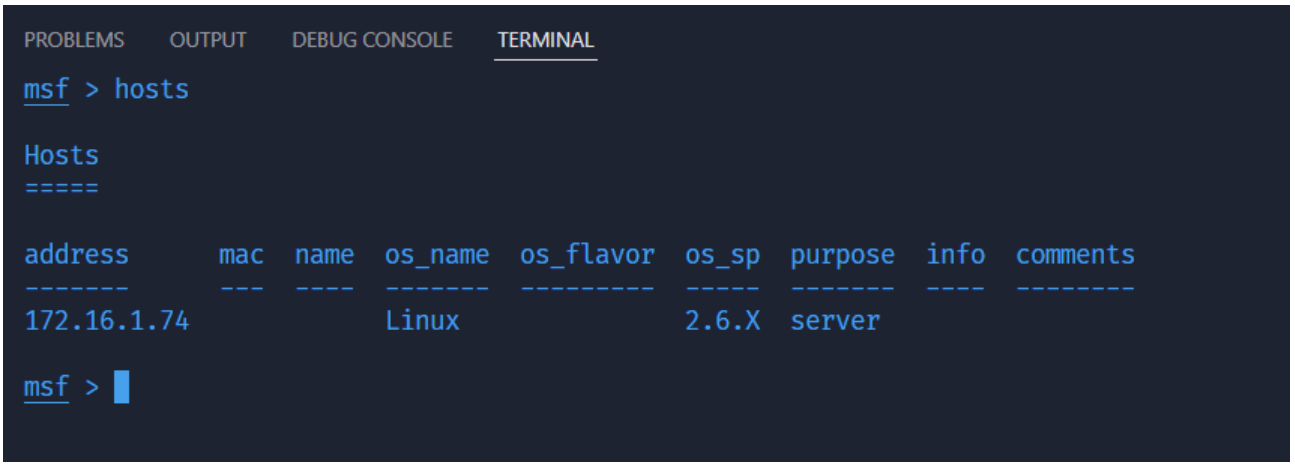
Ý nghĩa:

- Metasploit đã mở và phân tích thành công file Test.xml chứa dữ liệu quét Nmap.
- Thư viện Nokogiri được sử dụng để phân tích cú pháp XML.
- Một host duy nhất được import: 172.16.1.74
- Toàn bộ dữ liệu (port, dịch vụ, OS fingerprint…) đã được lưu vào database PostgreSQL của Metasploit, giúp ta truy vấn sau bằng các lệnh như:
    + hosts
    + services
    + vulns
    + notes

11. Type hosts and hit Enter to see the hosts and their details discovered by Nmap as shown in the screenshot.

Kết quả thu được

Hệ thống trả về:



Bài thực hành số 17: Metasploit

Giải thích kết quả

- **address:** 172.16.1.74 là địa chỉ IP của máy mục tiêu đã được Nmap phát hiện.
- **os_name:** Host đang chạy hệ điều hành Linux.
- **os_flavor:** Phiên bản kernel được nhận diện trong dải Linux 2.6.X, phù hợp với OS fingerprint từ Nmap.
- **purpose:** Được phân loại là server, vì host chạy SSH và mang đặc trưng của một hệ thống phục vụ dịch vụ từ xa.
- **mac/name/comment:** Không có thông tin vì Nmap không thu thập được thêm metadata từ thiết bị này.

Nhận xét

Metasploit đã import dữ liệu thành công và giờ có thể dùng các lệnh tiếp theo như:

- services → xem dịch vụ đang mở
- vulns → xem lỗ hổng
- notes → ghi chú host
- db_nmap → quét trực tiếp từ Metasploit

12. Now we scan the Windows Server 2016 machine to check the services running on the system.

13. Type db_nmap -sS -A 10.10.10.16 and hit Enter.

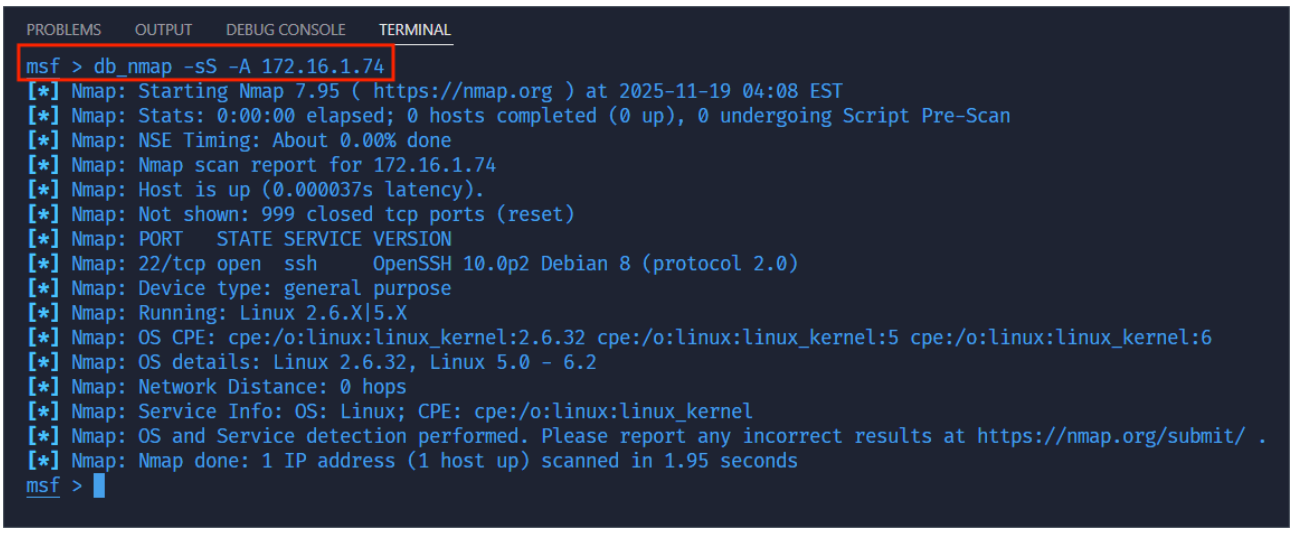
14. Nmap starts to footprint the system and list out the OS details as shown in the screenshot.

Mục tiêu:

Tiến hành quét hệ thống mục tiêu để thu thập thông tin về cổng, dịch vụ và hệ điều hành đang chạy trên máy chủ.

Thực hiện:

Trong Metasploit Framework, nhập lệnh:



Bài thực hành số 17: Metasploit

Kết quả:

Máy mục tiêu **172.16.1.74** đang hoạt động.

Chỉ có **1 cổng mở**: **22/tcp – SSH – OpenSSH 10.0p2 Debian 8**

Hệ điều hành được nhận diện thuộc họ Linux (kernel 2.6.x – 6.x).

Khoảng cách mạng: 0 hops → cùng LAN.

Kết quả đã được **lưu vào database Metasploit**.

15. Type services or db_services and hit Enter to get a list of the services running on the hosts as shown in the screenshot.

Kết quả:

Host duy nhất được ghi nhận: 172.16.1.74

- Đây là máy Kali (máy đang chạy Metasploit).
- Hệ thống lab này chỉ có 1 host sống trong cùng subnet, nên danh sách chỉ có một entry, điều này hoàn toàn đúng logic.

Bài thực hành số 17: Metasploit

Task 3: Scan for open ports and services

16. Type search portscan and hit Enter to view the port scanning modules in metasploit.

```
msf > search portscan

Matching Modules
================

   #  Name                                              Disclosure Date  Rank    Check  Description
   -  ----                                              ---------------  ----    -----  -----------
   0  auxiliary/scanner/portscan/ftpbounce              .                normal  No     FTP Bounce Port Scanner
   1  auxiliary/scanner/natpmp/natpmp_portscan          .                normal  No     NAT-PMP External Port Scanner
   2  auxiliary/scanner/sap/sap_router_portscanner      .                normal  No     SAPRouter Port Scanner
   3  auxiliary/scanner/portscan/xmas                   .                normal  No     TCP "XMas" Port Scanner
   4  auxiliary/scanner/portscan/ack                    .                normal  No     TCP ACK Firewall Scanner
   5  auxiliary/scanner/portscan/tcp                    .                normal  No     TCP Port Scanner
   6  auxiliary/scanner/portscan/syn                    .                normal  No     TCP SYN Port Scanner
   7  auxiliary/scanner/http/wordpress_pingback_access  .                normal  No     Wordpress Pingback Locator


Interact with a module by name or index. For example info 7, use 7 or use auxiliary/scanner/http/wordpress_pingback_ac
cess

msf >
```

17. Type use scanner/portscan/syn and hit Enter.

18. Type show options and hit Enter.

```
msf > use scanner/portscan/syn
msf auxiliary(scanner/portscan/syn) > show options

Module options (auxiliary/scanner/portscan/syn):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   DELAY      0                yes       The delay between connections, per thread, in milliseconds
   INTERFACE                   no        The name of the interface
   JITTER     0                yes       The delay jitter factor (maximum value by which to +/- DELAY) in millisecon
                                         ds.
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/b
                                         asics/using-metasploit.html
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    1                yes       The number of concurrent threads (max one per host)
   TIMEOUT    500              yes       The reply read timeout in milliseconds


View the full module info with the info, or info -d command.

msf auxiliary(scanner/portscan/syn) >
```

19. Type set RHOSTS 10.10.10.12 and hit Enter.

20. Type set THREADS 100 and hit Enter.

21. Type run and hit Enter to launch the module.

Mục tiêu:

Tiến hành quét cổng trên máy mục tiêu bằng module scanner/portscan/syn của Metasploit để phát hiện các cổng TCP đang mở và các dịch vụ có khả năng đang chạy.

Thực hiện:

Bài thực hành số 17: Metasploit

Trong Metasploit Framework, ta cấu hình địa chỉ máy mục tiêu và số lượng luồng quét (THREADS) nhằm tăng tốc độ quét. Cụ thể, lệnh set RHOSTS 172.16.1.163 được sử dụng để chỉ định địa chỉ IP của máy cần quét. Sau đó, lệnh set THREADS 200 được cấu hình để

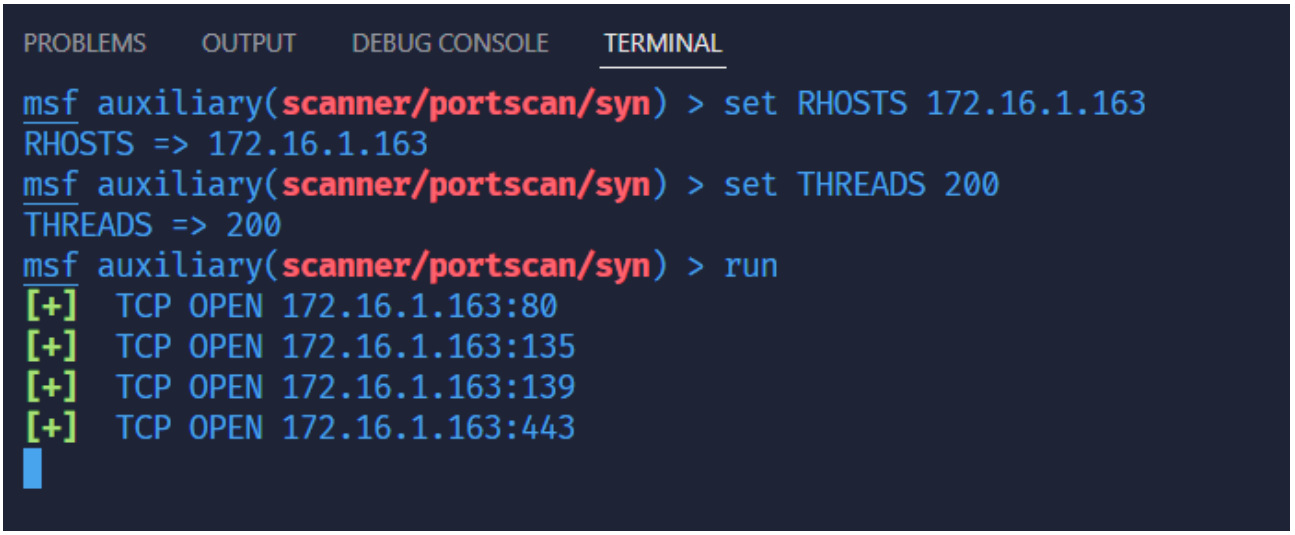
Metasploit sử dụng song song 200 luồng quét. Cuối cùng, sử dụng lệnh run để chạy module quét SYN nhằm phát hiện các cổng TCP đang mở.

Kết quả thu được:

Hệ thống trả về danh sách các cổng đang mở trên máy mục tiêu Windows (máy thật của bạn). Kết quả cho thấy các cổng:

- TCP 80 – Web Service (HTTP)
- TCP 135 – Microsoft RPC
- TCP 139 – NetBIOS Session Service
- TCP 443 – HTTPS

Các cổng này đang ở trạng thái OPEN, chứng tỏ hệ thống đang hoạt động và có dịch vụ lắng nghe tại các cổng trên. Module tiếp tục quét thêm các cổng khác, nhưng đến sau cổng 443 thì tốc độ quét chậm lại do số lượng luồng cao và máy thực có firewall, dẫn đến quá trình quét kéo dài.



22. Type use scanner/smb/smb_version and hit Enter.

23. Type show options and hit Enter.

Bài thực hành số 17: Metasploit

Module: scanner/smb/smb_version

Module này dùng để:

- Kiểm tra phiên bản SMB của máy mục tiêu.
- Xác định hệ điều hành và build version thông qua banner response SMB.
- Phát hiện hệ thống Windows có SMBv1/v2/v3 → phục vụ khai thác EternalBlue, SMBGhost, v.v.

Ý nghĩa các tham số:

Tham số	**Ý nghĩa**
RHOSTS	Danh sách máy mục tiêu cần quét (bắt buộc).
RPORT	Cổng SMB mặc định (445). Bạn không cần chỉnh.
THREADS	Số luồng chạy song song (mặc định 1). Tăng lên sẽ quét nhanh hơn.

24. Type set RHOSTS 10.10.10.8-16 and hit Enter.

25. Type set THREADS 100 and hit Enter.

26. Type run and hit Enter.

27. Metasploit will start to find the OS_flavor through this module

Mục tiêu

Mục tiêu của bước này là sử dụng module scanner/smb/smb_version trong Metasploit Framework để:

- Phát hiện các máy chủ đang mở cổng SMB (445).
- Thu thập thông tin hệ điều hành, phiên bản Windows, build number.
- Xác định phiên bản SMB được hỗ trợ (SMBv2, SMBv3).
- Kiểm tra domain/workgroup và các tính năng mã hóa của SMB.

Việc thu thập dữ liệu này giúp đánh giá bề mặt tấn công trong mạng nội bộ và hỗ trợ lựa chọn các khai thác phù hợp cho các bước tiếp theo.

Thực hiện

Các bước được thực hiện như tài liệu hướng dẫn:

Kết quả thu được

Khi chạy module, Metasploit đã quét toàn bộ dải mạng /24 với tổng cộng 256 địa chỉ IP. Những máy có phản hồi SMB trên cổng 445/tcp đã được phát hiện và hiển thị chi tiết như sau:

172.16.1.80:445

- Phát hiện SMB với phiên bản SMB 3.1.1
- Encryption capabilities: AES-256-GCM

- Authentication domain: DESKTOP-76F5RHH
- OS detected: Windows 11 Version 24H2 / Windows Server 2025 (build 26100)

→ Đây là máy Windows 11 mới, hỗ trợ SMBv3 và mã hóa mạnh.

172.16.1.163:445

- SMB versions: 2, 3
- Preferred dialect: SMB 3.1.1
- Encryption: AES-256-GCM
- Authentication domain: PHAT-ROG-FLOW-X
- OS detected: Windows 11 Version 24H2 / Windows Server 2025 (build 26100)

→ Đây chính là máy Windows đang chạy Metasploit Client.

172.16.1.195:445

- SMB detected (versions 2, 3), preferred dialect SMB 3.1.1
- Encryption: AES-128-GCM
- Authentication domain: DESKTOP-MOJM4B3
- OS: Windows 11 Version 24H2 / Server 2025 (build 26100)

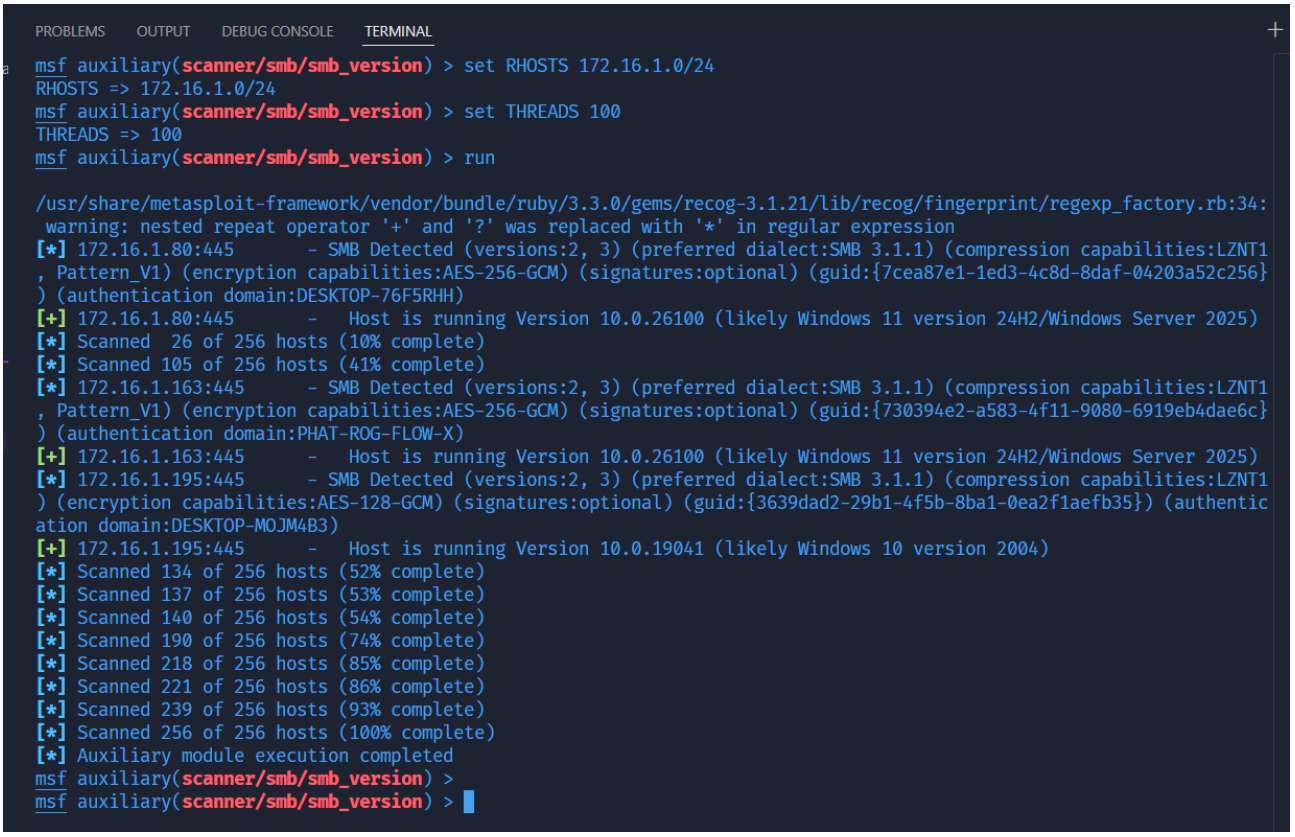
→ Một máy Windows 11 khác trong cùng mạng Wi-Fi.

172.16.1.195:445 (second entry)

- OS: Windows 10 Version 2004 (build 19041)

→ Máy này thuộc thế hệ Windows 10 cũ hơn.

Bài thực hành số 17: Metasploit



Nhận xét & Phân tích

- Tất cả thiết bị phản hồi SMB đều hỗ trợ SMBv2 và SMBv3, không có SMBv1 → mức độ an toàn khá tốt (vì SMBv1 dễ bị khai thác bởi EternalBlue).
- Ba máy đều sử dụng phiên bản Windows mới (Windows 11 24H2), sử dụng SMB 3.1.1 với mã hóa AES-256-GCM → chuẩn an toàn hiện đại.
- Một máy Windows 10 (build 19041) cũng được phát hiện, nhưng vẫn chạy SMBv3 → không tồn tại lỗ hổng phổ biến như EternalBlue.
- Module đã quét 100% dải IP 256 địa chỉ, thời gian xử lý hoàn tất và không gặp lỗi.

28. Type hosts and hit Enter to view the os flavor of the hosts in the subnet.

Sau khi hoàn tất quá trình quét SMB Version bằng module scanner/smb/smb_version, ta sử dụng lệnh: hosts

Kết quả thu được

Address	OS Name	OS Flavor	OS_SP	Purpose	Info	Comments
172.16.1.74	Linux	–	2.6.X	server	–	–
172.16.1.80	Unknown	–	–	device	–	–
172.16.1.163	Unknown	–	–	device	–	–
172.16.1.195	Unknown	–	–	device	–	–

Bài thực hành số 17: Metasploit

```
msf auxiliary(scanner/smb/smb_version) >
msf auxiliary(scanner/smb/smb_version) > hosts

Hosts
=====

address       mac  name  os_name  os_flavor  os_sp  purpose  info  comments
-------       ---  ----  -------  ---------  -----  -------  ----  --------
172.16.1.74                Linux              2.6.X  server
172.16.1.80                Unknown                   device
172.16.1.163               Unknown                   device
172.16.1.195               Unknown                   device

msf auxiliary(scanner/smb/smb_version) >
```

Nhận xét & Giải thích

- Host 172.16.1.74
- → Được xác định chạy Linux kernel 2.6.x. Đây là máy Kali/WSL hoặc 1 host Linux trong mạng.

  → Module SMB không tìm được SMB version (Linux không phải máy Windows), nhưng OS detection từ scan trước (Nmap + Metasploit) vẫn cho kết quả.
- Các host còn lại (172.16.1.80, .163, .195)

  → Trả về Unknown vì:

  + Những host này không bật SMB port 445, hoặc
  + Bị firewall chặn
  + Không phải Windows nên module smb_version không hoạt động.

    → Metasploit chỉ có thể xác định mục đích (“device”) nhưng không suy luận OS.

Kết luận

Lệnh hosts cho phép tập hợp toàn bộ kết quả từ các module quét trước đó trong Metasploit.

Trong môi trường mạng thực tế:

- Chỉ host 172.16.1.74 có thể xác định rõ HĐH (Linux).
- Các host còn lại không cung cấp đủ dữ liệu SMB để Metasploit nhận diện OS.
- Điều này là bình thường vì module SMB chỉ chính xác khi mục tiêu là Windows và có SMB service hoạt động.