ASSIGNMENT 3: CMDS

unzip, word count, list words from a word list

```
$ gunzip /usr/share/wordlists/rockyou.txt.gz
$ wc /usr/share/wordlists/rockyout.txt
$ cat /usr/share/wordlists/rockyout.txt
```

count the number of entries with password1

```
$ cat /usr.share.wordlists.rockyou.txt | grep password1 | wc
```

word count, list words from a word list

```
$ cat /usr/share/wordlists/fasttrack.txt | grep letmein
$ cat /usr.share.wordlists.rockyou.txt | grep letmein
```

Reply like a real ssh server on port 2222

```
$ (while true; do echo -e "SSH-2.0-OpenSSH_8.2p1 Ubuntun-4ubuntu0.3" | nc -l -p
2222 -q 1; done)
```

Test the fake ssh

```
$ hydra -V -f -t 4 -l testing -P /usr/share.wordlists.fasttract.txt
ssh://192.168.1.16:2222
```

Start real ssh server

```
$ service ssh start
```

hydra ssh with specific username and word list

```
$ hydra -V -f -t 4 -l luser1 -P /usr/shaare/wordlists/fasttrack.txt
ssh://192.168.1.29
```

search word list for a result

```
$ car /usr/share/wordlists/fastrack.txt | grep letmein
$ car /usr/share/wordlists/rockyou.txt
```

START SSH

```
$ sudo service ssh start
```

STOP SSH

```
$ sudo service ssh stop
```

NETCAT STUFF: # Listen

```
$ nc -l 10.0.2.15 -p 31337
$ nc -l -p 31337
```

Connect

```
$ nc 10.0.2.15 31337
```

Portscan

```
$ nc -z -n -v 10.0.2.15 1-99999
```

Receive File

```
$ nc -l 4444 > recieved_file
```

Send File

```
# nc domain.com 4444 < original_file
```

Host a local webpage

```
$ python2 -m SimpleHTTPServer 8080
```

Honeypot Script

```
$ !/bin/bash
$ (while true; do echo -e "HTTP/1.1 200 OK\n\n $(date)" | nc -l -p 80 -q 1; done)
&
$ (while true; do echo -e "RDP/1.1 200 OK\n\n $(date)" | nc -l -p 3389 -q 1; done)
&
$ (while true; do echo -e "HTTPS/1.1 200 OK\n\n $(date)" | nc -l -p 443 -q 1;
done) &
$ (while true; do echo -e "31337/1.1 200 OK\n\n $(date)" | nc -l -p 31337 -q 1;
done) &
```

Port Scan

```
$ nmap -p 1-65535 -T4 -A -v 192.168.1.18
$ nmap -p 8000 -T4 -A -v ip_address
$ nmap -p 1-65535 -T4 -A -v ip_address
```

Hashing Passwords # 0d107d09f5bbe40cade3de5c71e9e9b7

```
$ echo -n letmein | md5sum
```