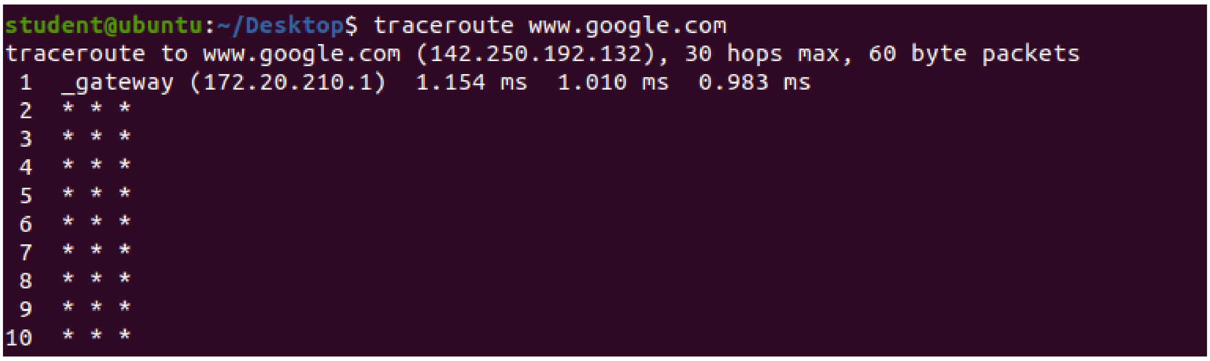
Experiment 6

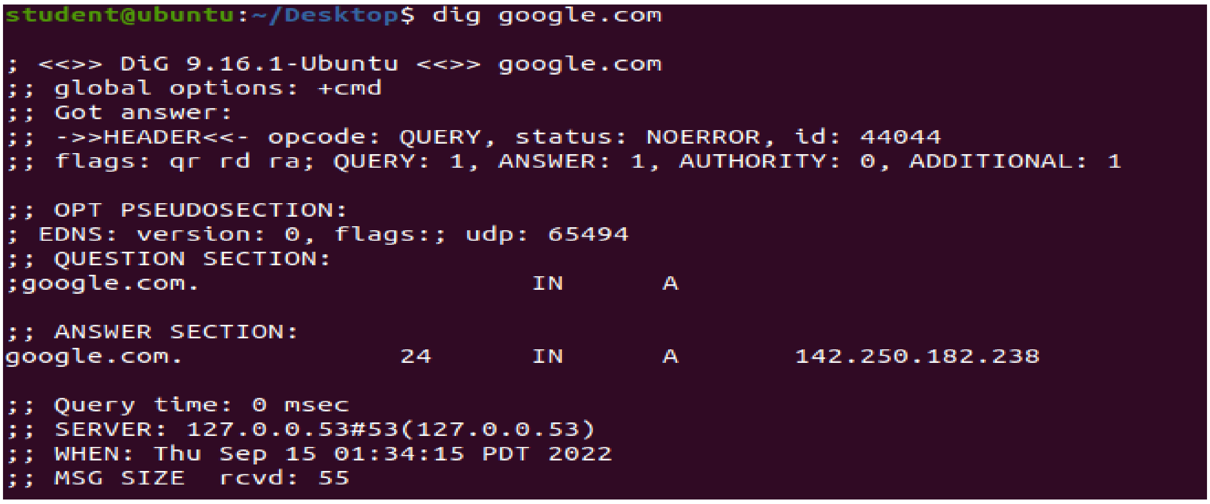
Output:

Traceroute



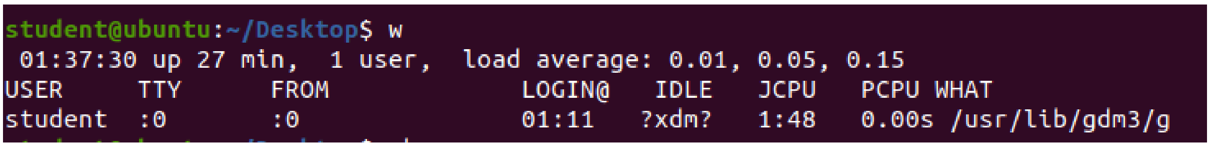
```
student@ubuntu:~/Desktop$ traceroute www.google.com
traceroute to www.google.com (142.250.192.132), 30 hops max, 60 byte packets
 1  _gateway (172.20.210.1)  1.154 ms  1.010 ms  0.983 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
```

Dig



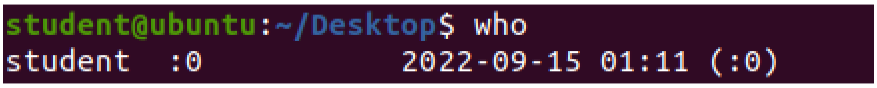
```
student@ubuntu:~/Desktop$ dig google.com

; <<>> DiG 9.16.1-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44044
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             24      IN      A       142.250.182.238

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Sep 15 01:34:15 PDT 2022
;; MSG SIZE  rcvd: 55
```

W



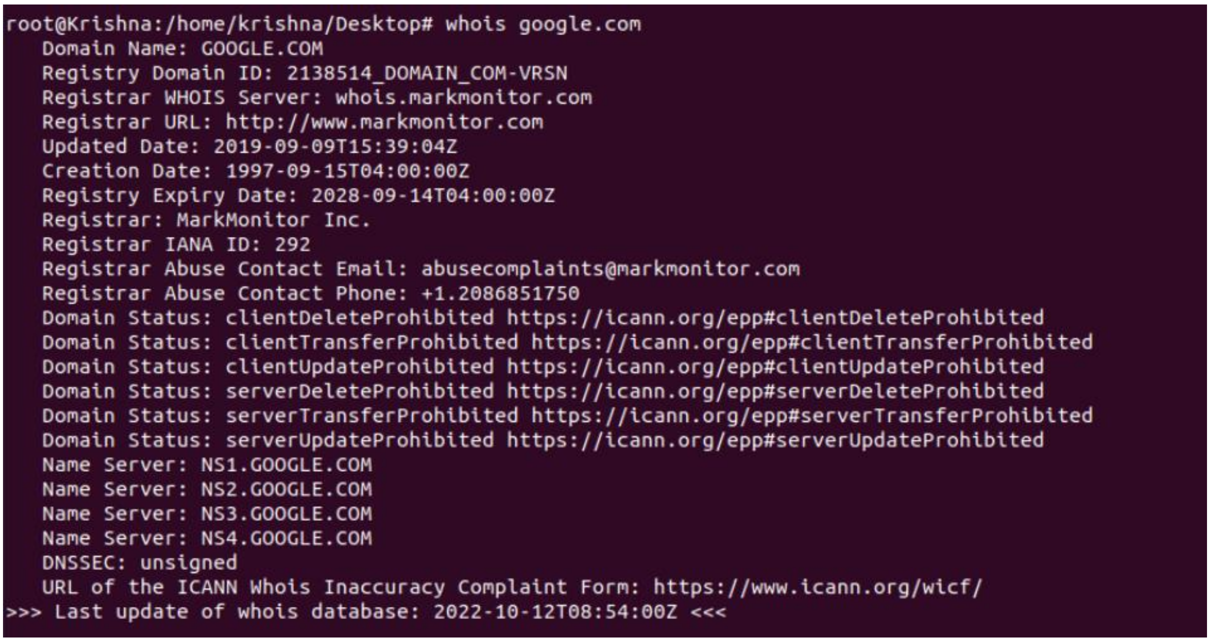
```
student@ubuntu:~/Desktop$ w
 01:37:30 up 27 min,  1 user,  load average: 0.01, 0.05, 0.15
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
student  :0       :0               01:11   ?xdm?   1:48   0.00s /usr/lib/gdm3/g
```

Who



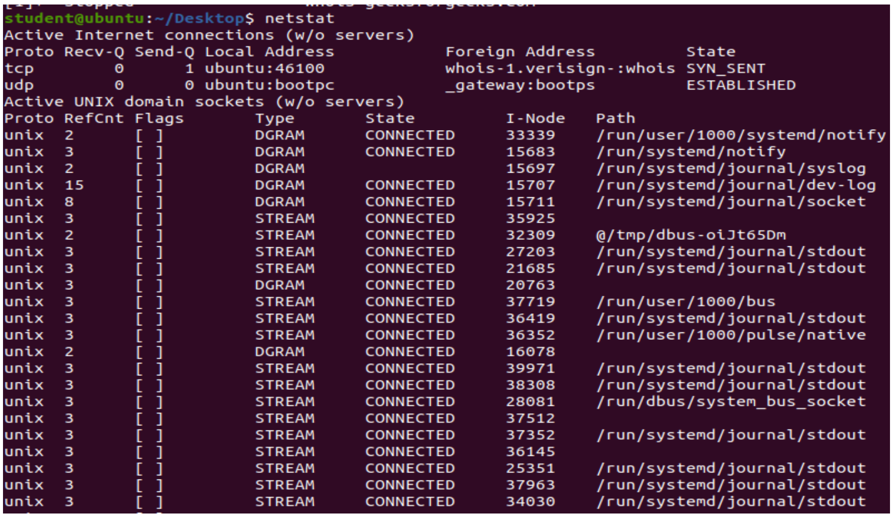
```
student@ubuntu:~/Desktop$ who
student  :0           2022-09-15 01:11 (:0)
```

Whois



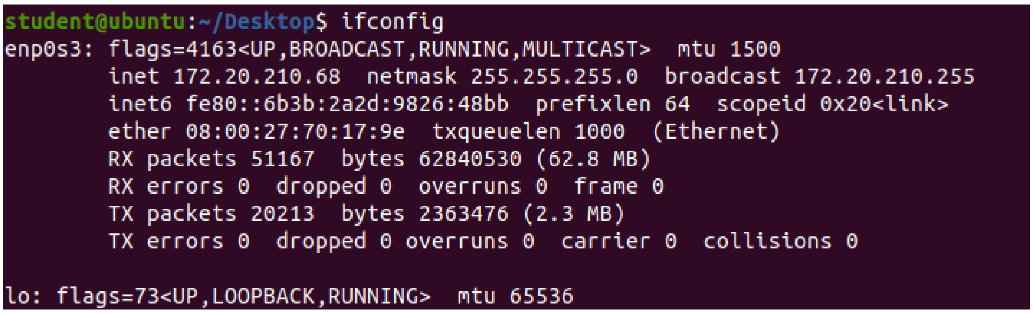
```
root@Krishna:/home/krishna/Desktop# whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: whois.markmonitor.com
   Registrar URL: http://www.markmonitor.com
   Updated Date: 2019-09-09T15:39:04Z
   Creation Date: 1997-09-15T04:00:00Z
   Registry Expiry Date: 2028-09-14T04:00:00Z
   Registrar: MarkMonitor Inc.
   Registrar IANA ID: 292
   Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
   Registrar Abuse Contact Phone: +1.2086851750
   Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
   Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
   Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
   Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
   Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
   Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
   Name Server: NS1.GOOGLE.COM
   Name Server: NS2.GOOGLE.COM
   Name Server: NS3.GOOGLE.COM
   Name Server: NS4.GOOGLE.COM
   DNSSEC: unsigned
   URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2022-10-12T08:54:00Z <<<
```

Netstat



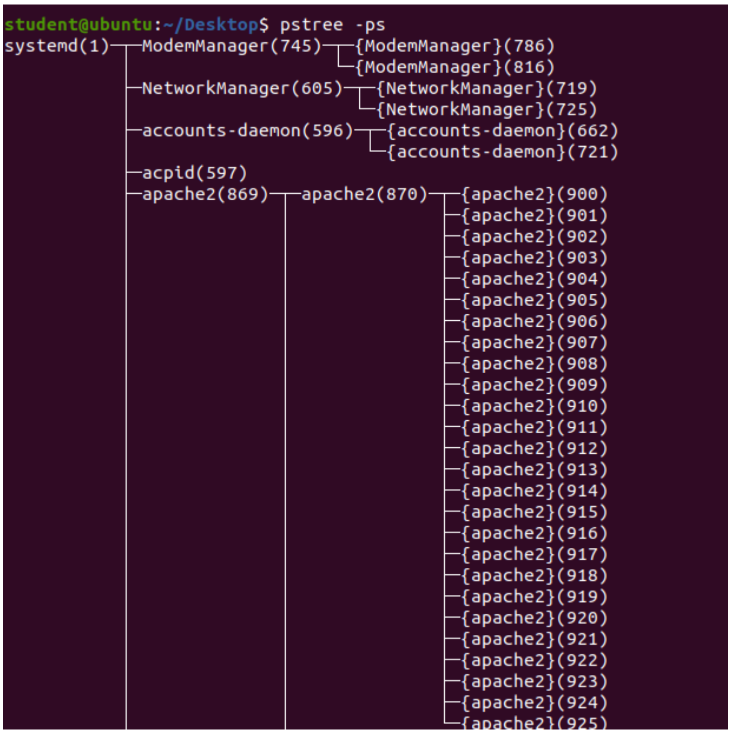
```
student@ubuntu:~/Desktop$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      1 ubuntu:46100            whois-1.verisign-:whois SYN_SENT
udp        0      0 ubuntu:bootpc           _gateway:bootps         ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM      CONNECTED     33339    /run/user/1000/systemd/notify
unix  3      [ ]         DGRAM      CONNECTED     15683    /run/systemd/notify
unix  2      [ ]         DGRAM                    15697    /run/systemd/journal/syslog
unix  15     [ ]         DGRAM      CONNECTED     15707    /run/systemd/journal/dev-log
unix  8      [ ]         DGRAM      CONNECTED     15711    /run/systemd/journal/socket
unix  3      [ ]         STREAM     CONNECTED     35925
unix  2      [ ]         STREAM     CONNECTED     32309    @/tmp/dbus-oiJt65Dm
unix  3      [ ]         STREAM     CONNECTED     27203    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21685    /run/systemd/journal/stdout
unix  3      [ ]         DGRAM      CONNECTED     20763
unix  3      [ ]         STREAM     CONNECTED     37719    /run/user/1000/bus
unix  3      [ ]         STREAM     CONNECTED     36419    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     36352    /run/user/1000/pulse/native
unix  2      [ ]         DGRAM      CONNECTED     16078
unix  3      [ ]         STREAM     CONNECTED     39971    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     38308    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     28081    /run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     37512
unix  3      [ ]         STREAM     CONNECTED     37352    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     36145
unix  3      [ ]         STREAM     CONNECTED     25351    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     37963    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     34030    /run/systemd/journal/stdout
```

Ifconfig



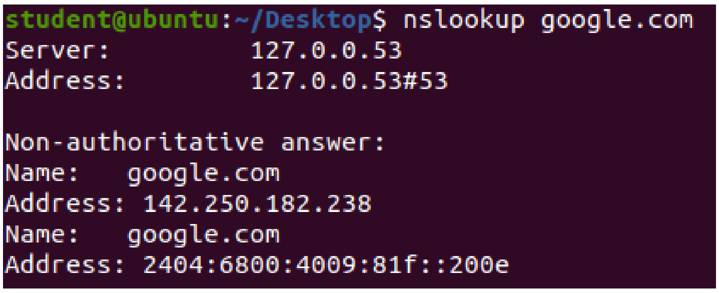
```
student@ubuntu:~/Desktop$ ifconfig
enp0s3: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.20.210.68  netmask 255.255.255.0  broadcast 172.20.210.255
        inet6 fe80::6b3b:2a2d:9826:48bb  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:70:17:9e  txqueuelen 1000  (Ethernet)
        RX packets 51167  bytes 62840530 (62.8 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20213  bytes 2363476 (2.3 MB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
```

Pstrea -noa



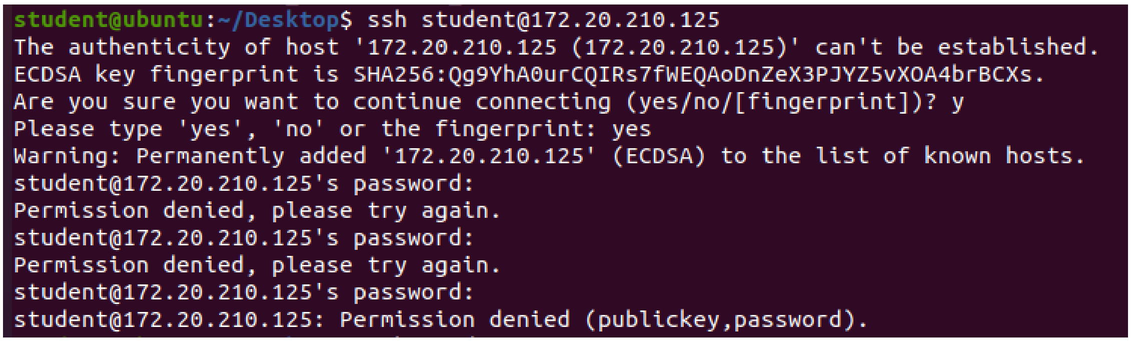
```
student@ubuntu:~/Desktop$ pstree -ps
systemd(1)─┬─ModemManager(745)─┬─{ModemManager}(786)
           │                   └─{ModemManager}(816)
           ├─NetworkManager(605)─┬─{NetworkManager}(719)
           │                     └─{NetworkManager}(725)
           ├─accounts-daemon(596)─┬─{accounts-daemon}(662)
           │                      └─{accounts-daemon}(721)
           ├─acpid(597)
           ├─apache2(869)─┬─apache2(870)─┬─{apache2}(900)
           │              │              ├─{apache2}(901)
           │              │              ├─{apache2}(902)
           │              │              ├─{apache2}(903)
           │              │              ├─{apache2}(904)
           │              │              ├─{apache2}(905)
           │              │              ├─{apache2}(906)
           │              │              ├─{apache2}(907)
           │              │              ├─{apache2}(908)
           │              │              ├─{apache2}(909)
           │              │              ├─{apache2}(910)
           │              │              ├─{apache2}(911)
           │              │              ├─{apache2}(912)
           │              │              ├─{apache2}(913)
           │              │              ├─{apache2}(914)
           │              │              ├─{apache2}(915)
           │              │              ├─{apache2}(916)
           │              │              ├─{apache2}(917)
           │              │              ├─{apache2}(918)
           │              │              ├─{apache2}(919)
           │              │              ├─{apache2}(920)
           │              │              ├─{apache2}(921)
           │              │              ├─{apache2}(922)
           │              │              ├─{apache2}(923)
           │              │              ├─{apache2}(924)
           │              │              └─{apache2}(925)
```

Nslookup



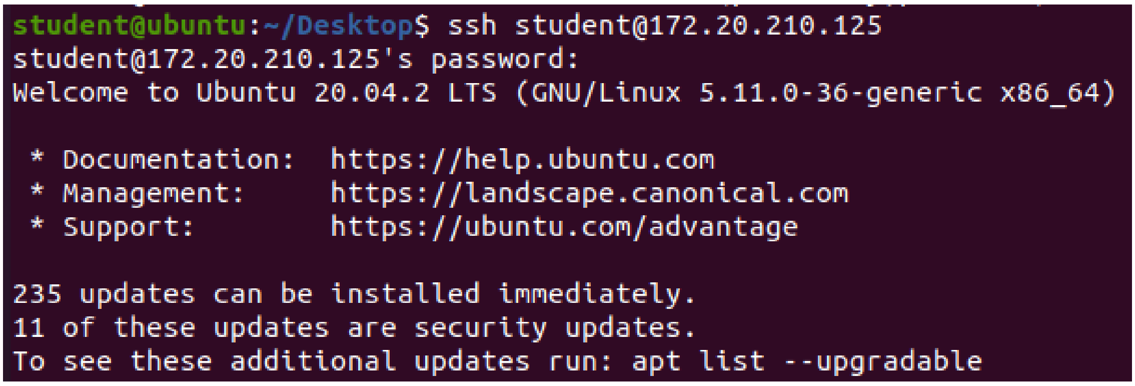
```
student@ubuntu:~/Desktop$ nslookup google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   google.com
Address: 142.250.182.238
Name:   google.com
Address: 2404:6800:4009:81f::200e
```

3 Wrong attempts



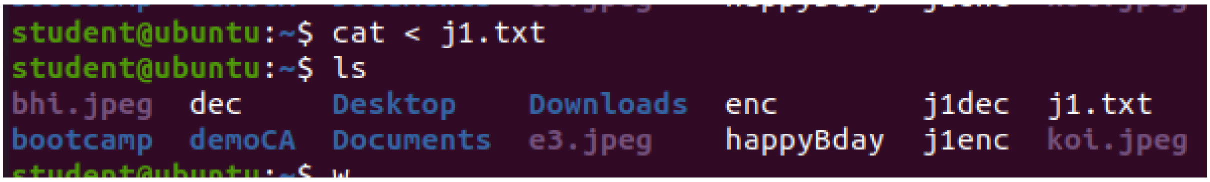
```
student@ubuntu:~/Desktop$ ssh student@172.20.210.125
The authenticity of host '172.20.210.125 (172.20.210.125)' can't be established.
ECDSA key fingerprint is SHA256:Qg9YhA0urCQIRs7fWEQAoDnZeX3PJYZ5vXOA4brBCXs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '172.20.210.125' (ECDSA) to the list of known hosts.
student@172.20.210.125's password:
Permission denied, please try again.
student@172.20.210.125's password:
Permission denied, please try again.
student@172.20.210.125's password:
student@172.20.210.125: Permission denied (publickey,password).
```

1 Correct attempt



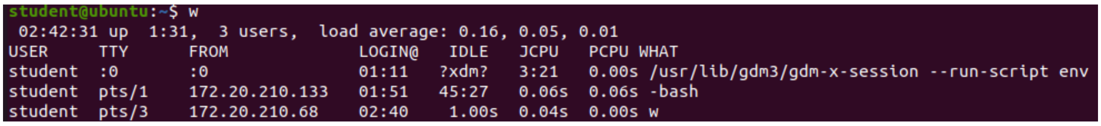
```
student@ubuntu:~/Desktop$ ssh student@172.20.210.125
student@172.20.210.125's password:
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 5.11.0-36-generic x86_64)

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

235 updates can be installed immediately.
11 of these updates are security updates.
To see these additional updates run: apt list --upgradable
```

File Change



```
student@ubuntu:~$ cat < j1.txt
student@ubuntu:~$ ls
bhi.jpeg   dec      Desktop    Downloads  enc        j1dec  j1.txt
bootcamp   demoCA   Documents  e3.jpeg    happyBday  j1enc  koi.jpeg
student@ubuntu:~$ w
```

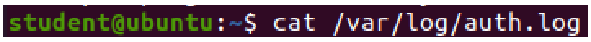
How he gains access to pc:



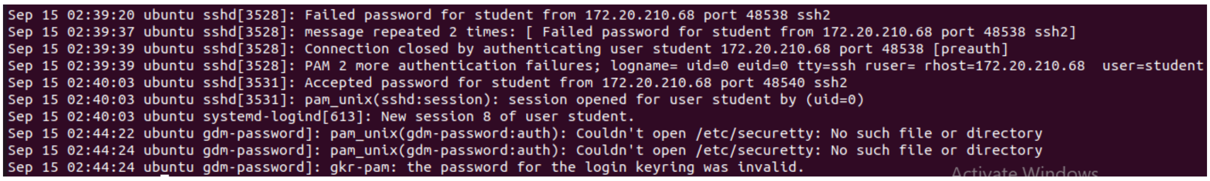
```
student@ubuntu:~$ w
 02:42:31 up  1:31,  3 users,  load average: 0.16, 0.05, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
student  :0       :0               01:11   ?xdm?   3:21   0.00s /usr/lib/gdm3/gdm-x-session --run-script env
student  pts/1    172.20.210.133   01:51   45:27   0.06s  0.06s -bash
student  pts/3    172.20.210.68    02:40    1.00s  0.04s  0.00s w
```

cat /var/log/auth.log

Time period he stayed in the pc:



```
student@ubuntu:~$ cat /var/log/auth.log
```



```
Sep 15 02:39:20 ubuntu sshd[3528]: Failed password for student from 172.20.210.68 port 48538 ssh2
Sep 15 02:39:37 ubuntu sshd[3528]: message repeated 2 times: [ Failed password for student from 172.20.210.68 port 48538 ssh2]
Sep 15 02:39:39 ubuntu sshd[3528]: Connection closed by authenticating user student 172.20.210.68 port 48538 [preauth]
Sep 15 02:39:39 ubuntu sshd[3528]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.210.68  user=student
Sep 15 02:40:03 ubuntu sshd[3531]: Accepted password for student from 172.20.210.68 port 48540 ssh2
Sep 15 02:40:03 ubuntu sshd[3531]: pam_unix(sshd:session): session opened for user student by (uid=0)
Sep 15 02:40:03 ubuntu systemd-logind[613]: New session 8 of user student.
Sep 15 02:44:22 ubuntu gdm-password]: pam_unix(gdm-password:auth): Couldn't open /etc/securetty: No such file or directory
Sep 15 02:44:24 ubuntu gdm-password]: pam_unix(gdm-password:auth): Couldn't open /etc/securetty: No such file or directory
Sep 15 02:44:24 ubuntu gdm-password]: gkr-pam: the password for the login keyring was invalid.
```