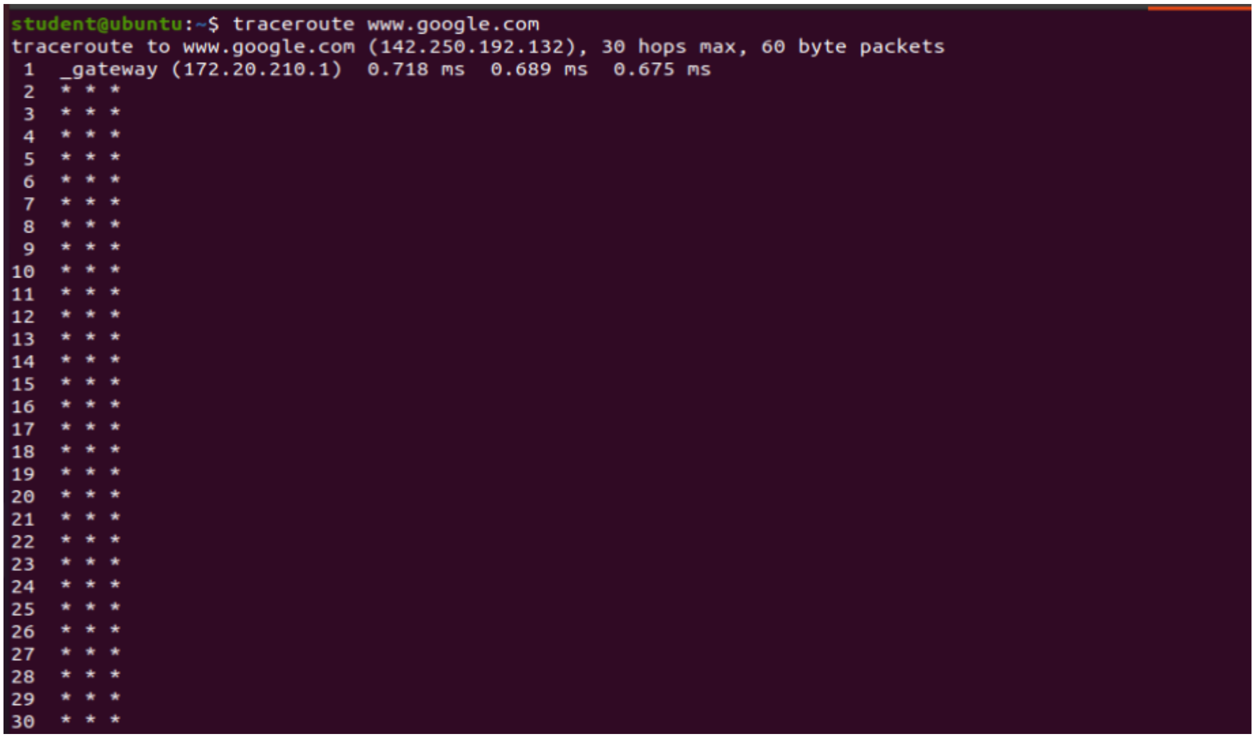
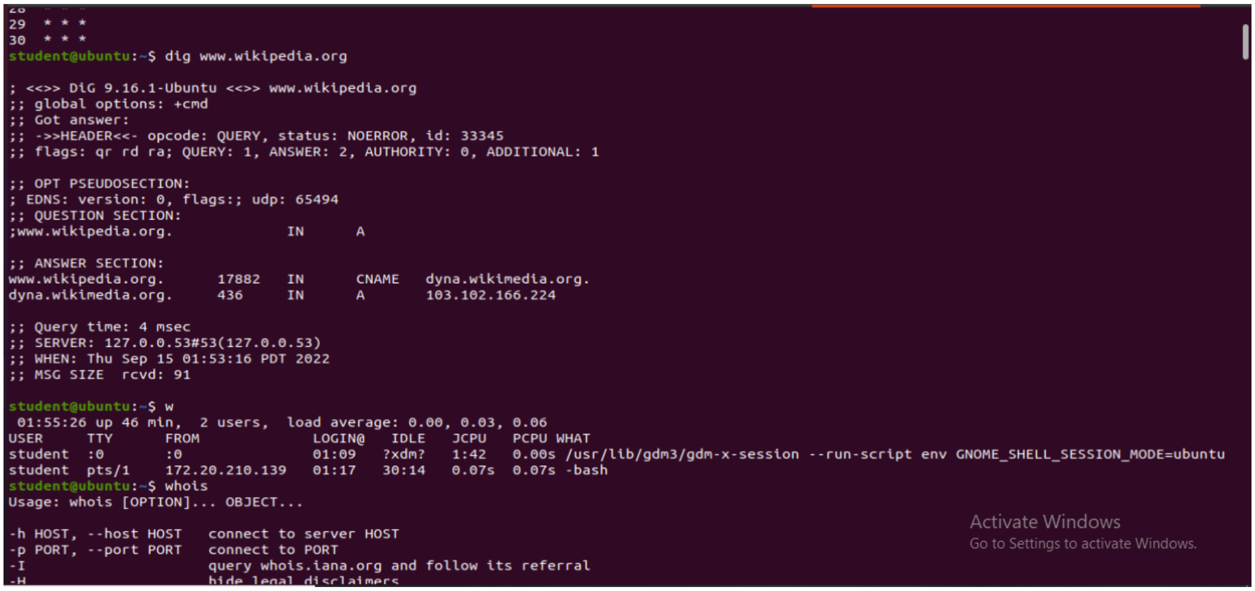
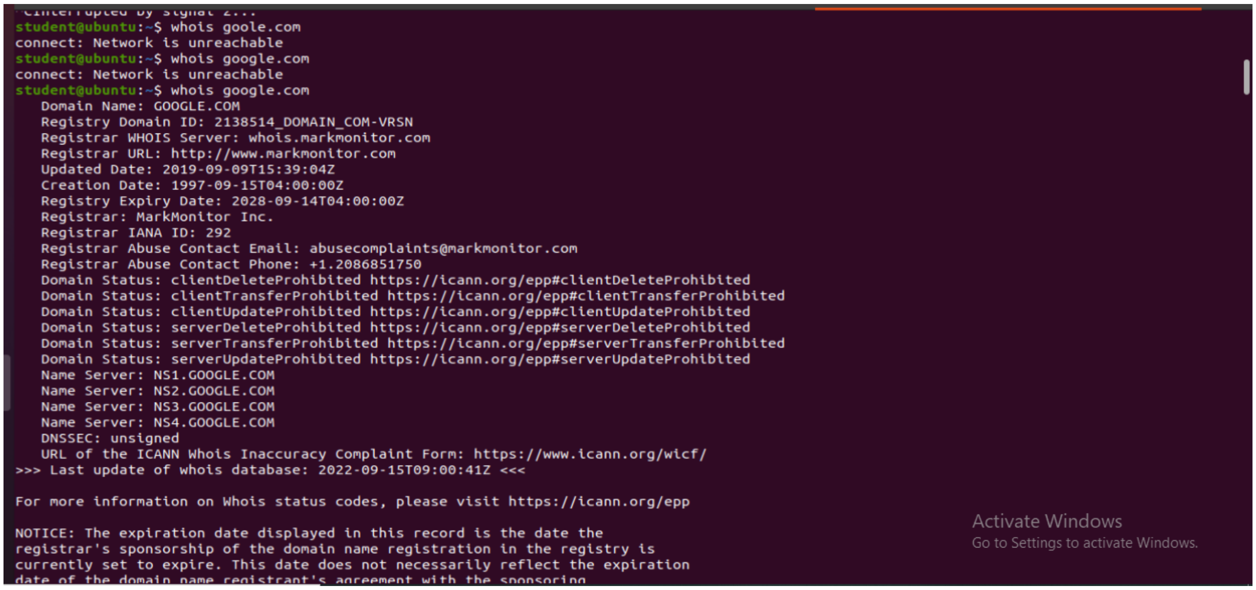


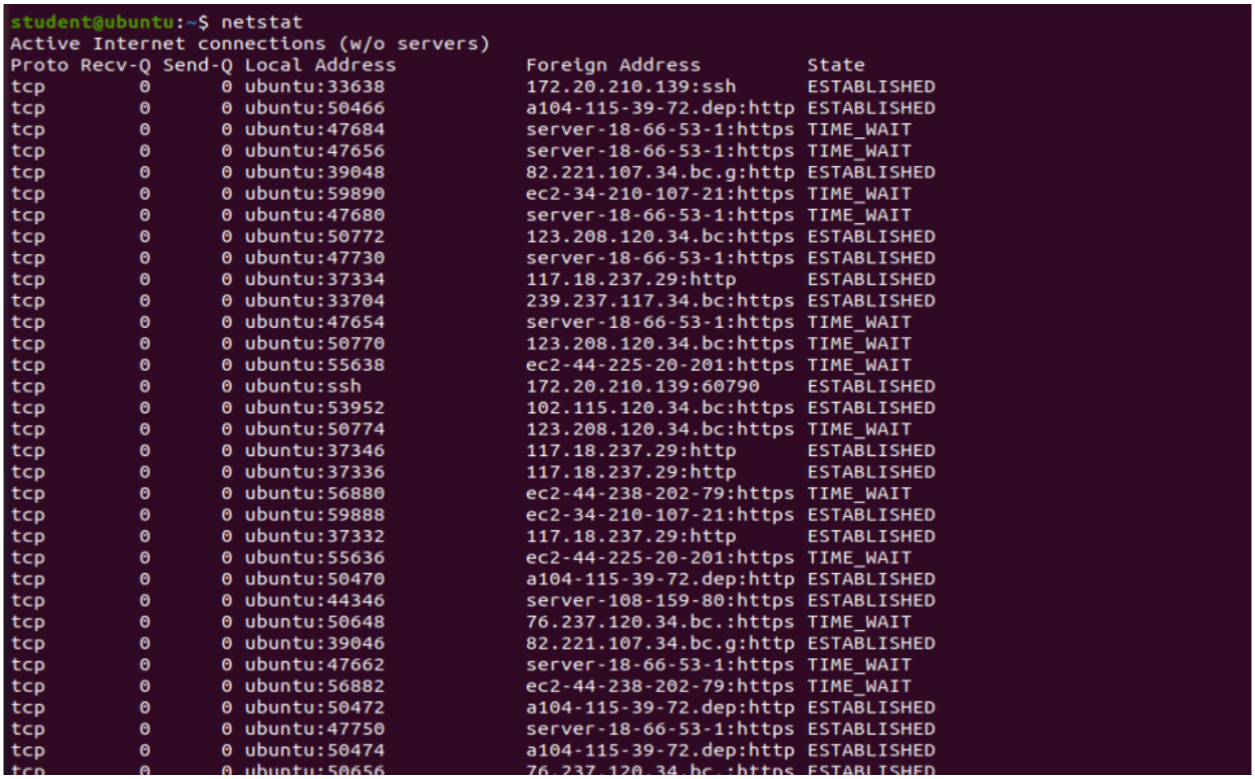
```
student@ubuntu:~$ traceroute www.google.com
traceroute to www.google.com (142.250.192.132), 30 hops max, 60 byte packets
 1  _gateway (172.20.210.1)  0.718 ms  0.689 ms  0.675 ms
 2  * * *
 3  * * *
 4  * * *
 5  * * *
 6  * * *
 7  * * *
 8  * * *
 9  * * *
10  * * *
11  * * *
12  * * *
13  * * *
14  * * *
15  * * *
16  * * *
17  * * *
18  * * *
19  * * *
20  * * *
21  * * *
22  * * *
23  * * *
24  * * *
25  * * *
26  * * *
27  * * *
28  * * *
29  * * *
30  * * *
```



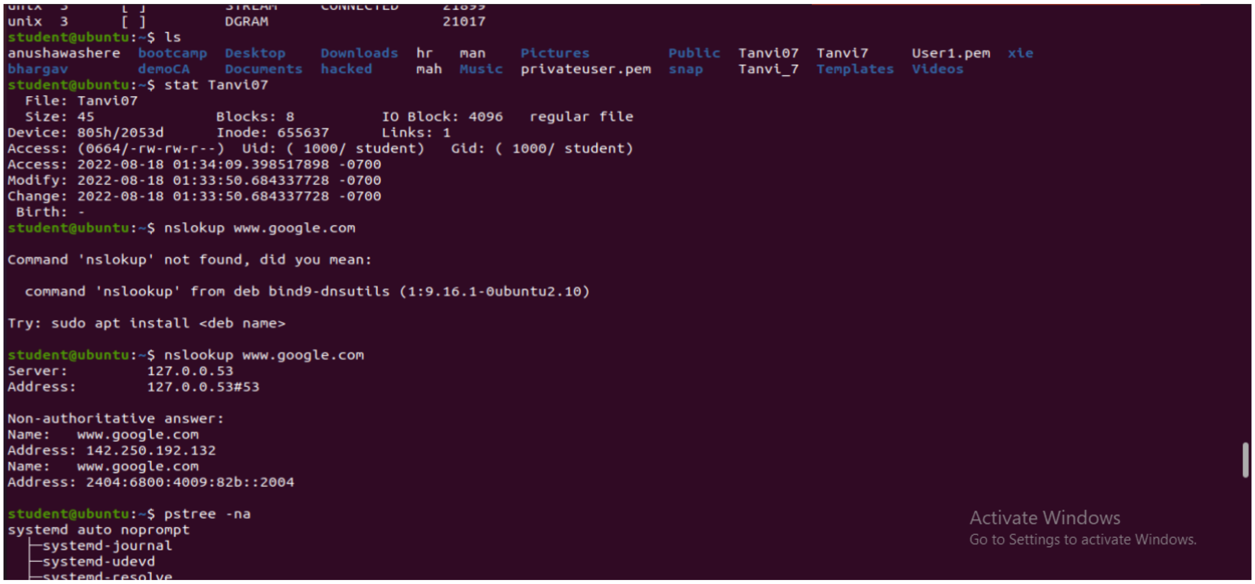
```
28  * * *
29  * * *
30  * * *
student@ubuntu:~$ dig www.wikipedia.org

; <<>> DiG 9.16.1-Ubuntu <<>> www.wikipedia.org
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 33345
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;www.wikipedia.org.             IN      A

;; ANSWER SECTION:
www.wikipedia.org.      17882   IN      CNAME   dyna.wikimedia.org.
dyna.wikimedia.org.     436     IN      A       103.102.166.224

;; Query time: 4 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Sep 15 01:53:16 PDT 2022
;; MSG SIZE  rcvd: 91

student@ubuntu:~$ w
 01:55:26 up 46 min,  2 users,  load average: 0.00, 0.03, 0.06
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
student  :0       :0               01:09   ?xdm?   1:42   0.00s /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu
student  pts/1    172.20.210.139   01:17   30:14   0.07s  0.07s -bash
student@ubuntu:~$ whois
Usage: whois [OPTION]... OBJECT...

-h HOST, --host HOST   connect to server HOST
-p PORT, --port PORT   connect to PORT
-I                     query whois.iana.org and follow its referral
-H                     hide legal disclaimers
```



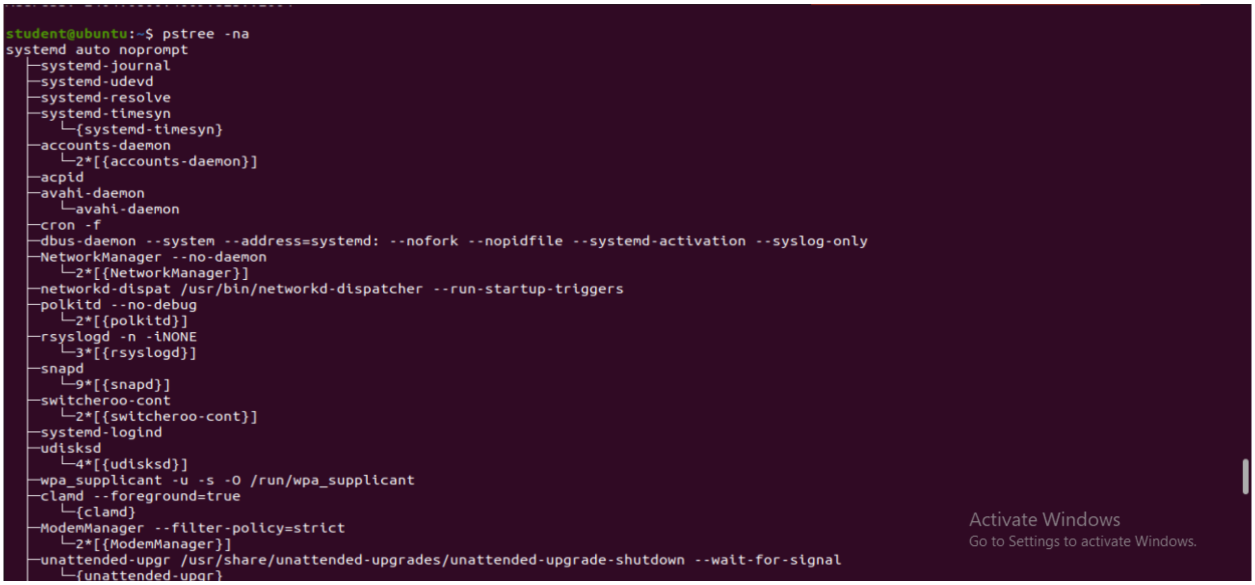
```
^Cinterrupted by signal 2...
student@ubuntu:~$ whois goole.com
connect: Network is unreachable
student@ubuntu:~$ whois google.com
connect: Network is unreachable
student@ubuntu:~$ whois google.com
   Domain Name: GOOGLE.COM
   Registry Domain ID: 2138514_DOMAIN_COM-VRSN
   Registrar WHOIS Server: 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: 2022-09-15T09:00:41Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
```



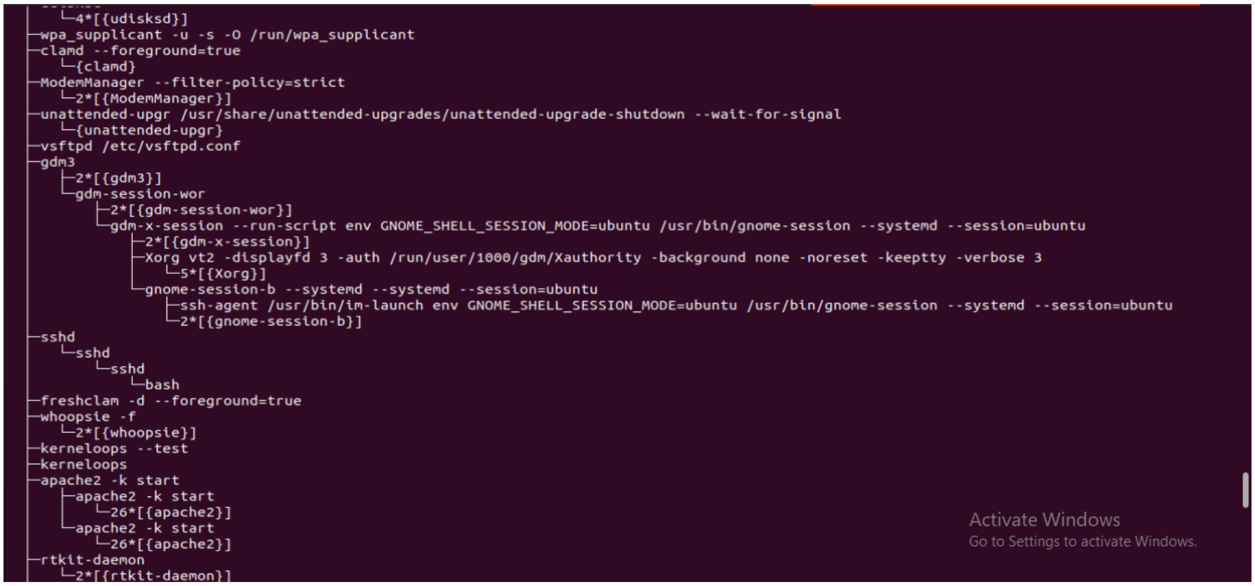
```
student@ubuntu:~$ netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 ubuntu:33638            172.20.210.139:ssh      ESTABLISHED
tcp        0      0 ubuntu:50466            a104-115-39-72.dep:http ESTABLISHED
tcp        0      0 ubuntu:47684            server-18-66-53-1:https TIME_WAIT
tcp        0      0 ubuntu:47656            server-18-66-53-1:https TIME_WAIT
tcp        0      0 ubuntu:39048            82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 ubuntu:59890            ec2-34-210-107-21:https TIME_WAIT
tcp        0      0 ubuntu:47680            server-18-66-53-1:https TIME_WAIT
tcp        0      0 ubuntu:50772            123.208.120.34.bc:https ESTABLISHED
tcp        0      0 ubuntu:47730            server-18-66-53-1:https ESTABLISHED
tcp        0      0 ubuntu:37334            117.18.237.29:http      ESTABLISHED
tcp        0      0 ubuntu:33704            239.237.117.34.bc:https ESTABLISHED
tcp        0      0 ubuntu:47654            server-18-66-53-1:https TIME_WAIT
tcp        0      0 ubuntu:50770            123.208.120.34.bc:https TIME_WAIT
tcp        0      0 ubuntu:55638            ec2-44-225-20-201:https TIME_WAIT
tcp        0      0 ubuntu:ssh              172.20.210.139:60790    ESTABLISHED
tcp        0      0 ubuntu:53952            102.115.120.34.bc:https ESTABLISHED
tcp        0      0 ubuntu:50774            123.208.120.34.bc:https TIME_WAIT
tcp        0      0 ubuntu:37346            117.18.237.29:http      ESTABLISHED
tcp        0      0 ubuntu:37336            117.18.237.29:http      ESTABLISHED
tcp        0      0 ubuntu:56880            ec2-44-238-202-79:https TIME_WAIT
tcp        0      0 ubuntu:59888            ec2-34-210-107-21:https ESTABLISHED
tcp        0      0 ubuntu:37332            117.18.237.29:http      ESTABLISHED
tcp        0      0 ubuntu:55636            ec2-44-225-20-201:https TIME_WAIT
tcp        0      0 ubuntu:50470            a104-115-39-72.dep:http ESTABLISHED
tcp        0      0 ubuntu:44346            server-108-159-80:https ESTABLISHED
tcp        0      0 ubuntu:50648            76.237.120.34.bc.:https TIME_WAIT
tcp        0      0 ubuntu:39046            82.221.107.34.bc.g:http ESTABLISHED
tcp        0      0 ubuntu:47662            server-18-66-53-1:https TIME_WAIT
tcp        0      0 ubuntu:56882            ec2-44-238-202-79:https TIME_WAIT
tcp        0      0 ubuntu:50472            a104-115-39-72.dep:http ESTABLISHED
tcp        0      0 ubuntu:47750            server-18-66-53-1:https ESTABLISHED
tcp        0      0 ubuntu:50474            a104-115-39-72.dep:http ESTABLISHED
tcp        0      0 ubuntu:50656            76.237.120.34.bc.:https ESTABLISHED
```



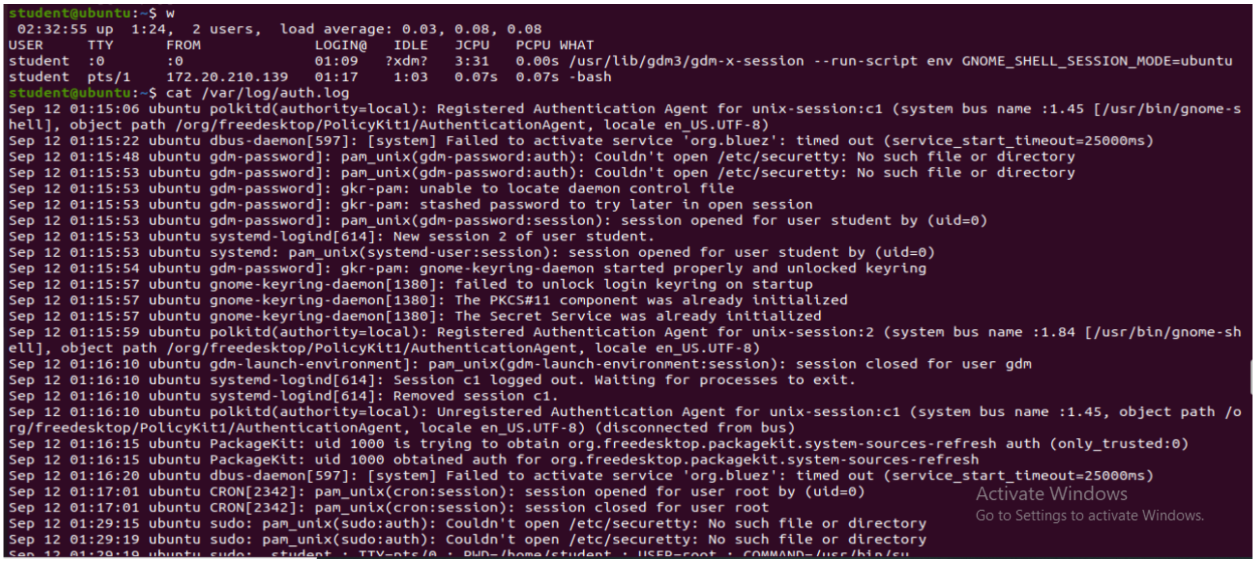
```
unix  3      [ ]         STREAM     CONNECTED     21899
unix  3      [ ]         DGRAM                    21017
student@ubuntu:~$ ls
anushawashere  bootcamp  Desktop    Downloads  hr   man    Pictures          Public  Tanvi07  Tanvi7     User1.pem  xie
bhargav        demoCA    Documents  hacked     mah  Music  privateuser.pem   snap    Tanvi_7  Templates  Videos
student@ubuntu:~$ stat Tanvi07
  File: Tanvi07
  Size: 45              Blocks: 8          IO Block: 4096   regular file
Device: 805h/2053d      Inode: 655637      Links: 1
Access: (0664/-rw-rw-r--)  Uid: ( 1000/ student)   Gid: ( 1000/ student)
Access: 2022-08-18 01:34:09.398517898 -0700
Modify: 2022-08-18 01:33:50.684337728 -0700
Change: 2022-08-18 01:33:50.684337728 -0700
 Birth: -
student@ubuntu:~$ nslokup www.google.com

Command 'nslokup' not found, did you mean:

  command 'nslookup' from deb bind9-dnsutils (1:9.16.1-0ubuntu2.10)

Try: sudo apt install <deb name>

student@ubuntu:~$ nslookup www.google.com
Server:         127.0.0.53
Address:        127.0.0.53#53

Non-authoritative answer:
Name:   www.google.com
Address: 142.250.192.132
Name:   www.google.com
Address: 2404:6800:4009:82b::2004

student@ubuntu:~$ pstree -na
systemd auto noprompt
  ├─systemd-journal
  ├─systemd-udevd
  ├─systemd-resolve
```



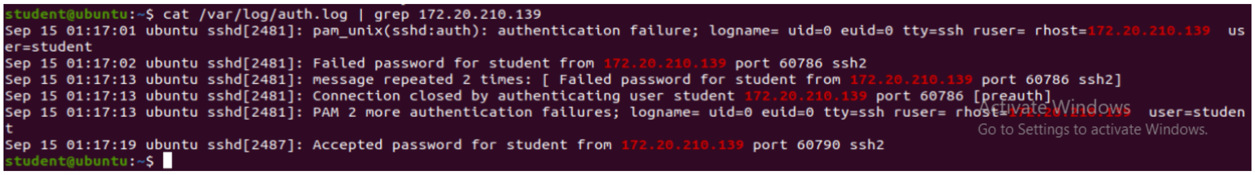
```
student@ubuntu:~$ pstree -na
systemd auto noprompt
  ├─systemd-journal
  ├─systemd-udevd
  ├─systemd-resolve
  ├─systemd-timesyn
  │   └─{systemd-timesyn}
  ├─accounts-daemon
  │   └─2*[{accounts-daemon}]
  ├─acpid
  ├─avahi-daemon
  │   └─avahi-daemon
  ├─cron -f
  ├─dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-activation --syslog-only
  ├─NetworkManager --no-daemon
  │   └─2*[{NetworkManager}]
  ├─networkd-dispat /usr/bin/networkd-dispatcher --run-startup-triggers
  ├─polkitd --no-debug
  │   └─2*[{polkitd}]
  ├─rsyslogd -n -iNONE
  │   └─3*[{rsyslogd}]
  ├─snapd
  │   └─9*[{snapd}]
  ├─switcheroo-cont
  │   └─2*[{switcheroo-cont}]
  ├─systemd-logind
  ├─udisksd
  │   └─4*[{udisksd}]
  ├─wpa_supplicant -u -s -O /run/wpa_supplicant
  ├─clamd --foreground=true
  │   └─{clamd}
  ├─ModemManager --filter-policy=strict
  │   └─2*[{ModemManager}]
  ├─unattended-upgr /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
  │   └─{unattended-upgr}
```



```
│    └─4*[{udisksd}]
├─wpa_supplicant -u -s -O /run/wpa_supplicant
├─clamd --foreground=true
│    └─{clamd}
├─ModemManager --filter-policy=strict
│    └─2*[{ModemManager}]
├─unattended-upgr /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-signal
│    └─{unattended-upgr}
├─vsftpd /etc/vsftpd.conf
├─gdm3
│    ├─2*[{gdm3}]
│    └─gdm-session-wor
│         ├─2*[{gdm-session-wor}]
│         └─gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu /usr/bin/gnome-session --systemd --session=ubuntu
│              ├─2*[{gdm-x-session}]
│              ├─Xorg vt2 -displayfd 3 -auth /run/user/1000/gdm/Xauthority -background none -noreset -keeptty -verbose 3
│              │    └─5*[{Xorg}]
│              └─gnome-session-b --systemd --systemd --session=ubuntu
│                   ├─ssh-agent /usr/bin/im-launch env GNOME_SHELL_SESSION_MODE=ubuntu /usr/bin/gnome-session --systemd --session=ubuntu
│                   └─2*[{gnome-session-b}]
├─sshd
│    └─sshd
│         └─sshd
│              └─bash
├─freshclam -d --foreground=true
├─whoopsie -f
│    └─2*[{whoopsie}]
├─kerneloops --test
├─kerneloops
├─apache2 -k start
│    ├─apache2 -k start
│    │    └─26*[{apache2}]
│    └─apache2 -k start
│         └─26*[{apache2}]
├─rtkit-daemon
│    └─2*[{rtkit-daemon}]
```

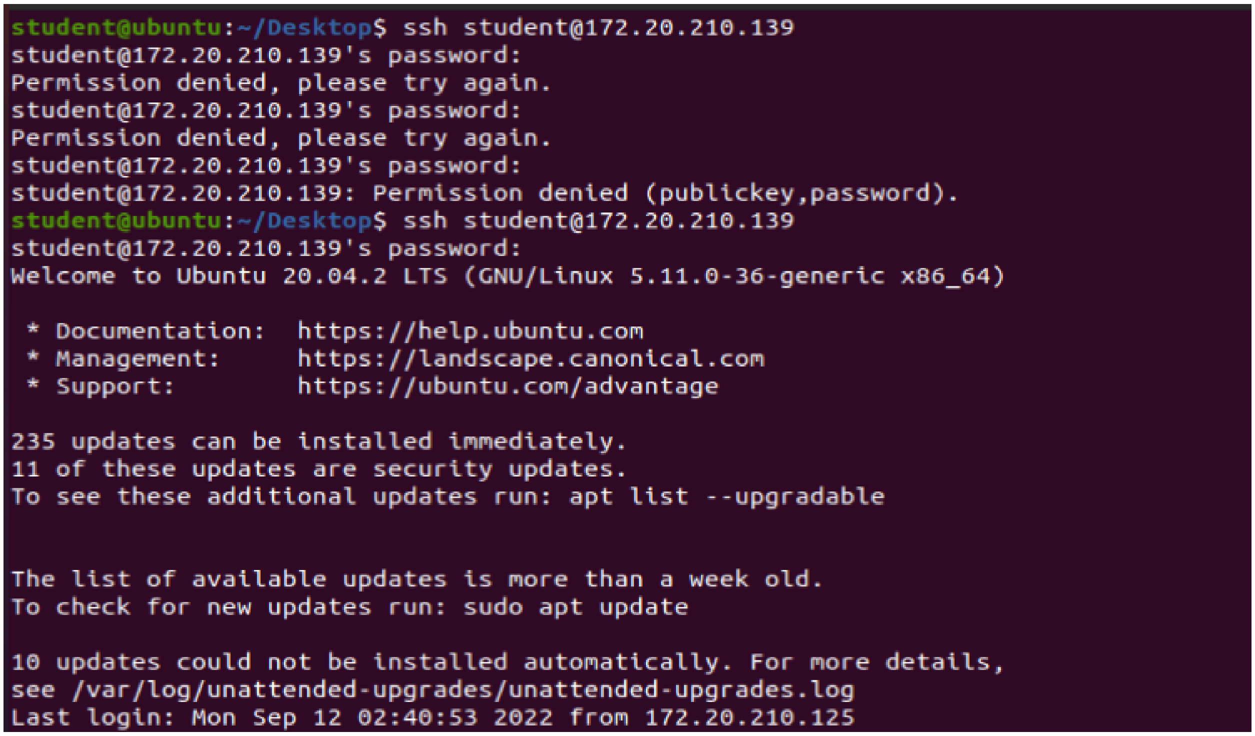


```
student@ubuntu:~$ w
 02:32:55 up  1:24,  2 users,  load average: 0.03, 0.08, 0.08
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
student  :0       :0               01:09   ?xdm?   3:31   0.00s /usr/lib/gdm3/gdm-x-session --run-script env GNOME_SHELL_SESSION_MODE=ubuntu
student  pts/1    172.20.210.139   01:17    1:03   0.07s  0.07s -bash
student@ubuntu:~$ cat /var/log/auth.log
Sep 12 01:15:06 ubuntu polkitd(authority=local): Registered Authentication Agent for unix-session:c1 (system bus name :1.45 [/usr/bin/gnome-s
hell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep 12 01:15:22 ubuntu dbus-daemon[597]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
Sep 12 01:15:48 ubuntu gdm-password]: pam_unix(gdm-password:auth): Couldn't open /etc/securetty: No such file or directory
Sep 12 01:15:53 ubuntu gdm-password]: pam_unix(gdm-password:auth): Couldn't open /etc/securetty: No such file or directory
Sep 12 01:15:53 ubuntu gdm-password]: gkr-pam: unable to locate daemon control file
Sep 12 01:15:53 ubuntu gdm-password]: gkr-pam: stashed password to try later in open session
Sep 12 01:15:53 ubuntu gdm-password]: pam_unix(gdm-password:session): session opened for user student by (uid=0)
Sep 12 01:15:53 ubuntu systemd-logind[614]: New session 2 of user student.
Sep 12 01:15:53 ubuntu systemd: pam_unix(systemd-user:session): session opened for user student by (uid=0)
Sep 12 01:15:54 ubuntu gdm-password]: gkr-pam: gnome-keyring-daemon started properly and unlocked keyring
Sep 12 01:15:57 ubuntu gnome-keyring-daemon[1380]: failed to unlock login keyring on startup
Sep 12 01:15:57 ubuntu gnome-keyring-daemon[1380]: The PKCS#11 component was already initialized
Sep 12 01:15:57 ubuntu gnome-keyring-daemon[1380]: The Secret Service was already initialized
Sep 12 01:15:59 ubuntu polkitd(authority=local): Registered Authentication Agent for unix-session:2 (system bus name :1.84 [/usr/bin/gnome-sh
ell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Sep 12 01:16:10 ubuntu gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session closed for user gdm
Sep 12 01:16:10 ubuntu systemd-logind[614]: Session c1 logged out. Waiting for processes to exit.
Sep 12 01:16:10 ubuntu systemd-logind[614]: Removed session c1.
Sep 12 01:16:10 ubuntu polkitd(authority=local): Unregistered Authentication Agent for unix-session:c1 (system bus name :1.45, object path /o
rg/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Sep 12 01:16:15 ubuntu PackageKit: uid 1000 is trying to obtain org.freedesktop.packagekit.system-sources-refresh auth (only_trusted:0)
Sep 12 01:16:15 ubuntu PackageKit: uid 1000 obtained auth for org.freedesktop.packagekit.system-sources-refresh
Sep 12 01:16:20 ubuntu dbus-daemon[597]: [system] Failed to activate service 'org.bluez': timed out (service_start_timeout=25000ms)
Sep 12 01:17:01 ubuntu CRON[2342]: pam_unix(cron:session): session opened for user root by (uid=0)
Sep 12 01:17:01 ubuntu CRON[2342]: pam_unix(cron:session): session closed for user root
Sep 12 01:29:15 ubuntu sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Sep 12 01:29:19 ubuntu sudo: pam_unix(sudo:auth): Couldn't open /etc/securetty: No such file or directory
Sep 12 01:29:19 ubuntu sudo:  student : TTY=pts/0 ; PWD=/home/student ; USER=root ; COMMAND=/usr/bin/su
```

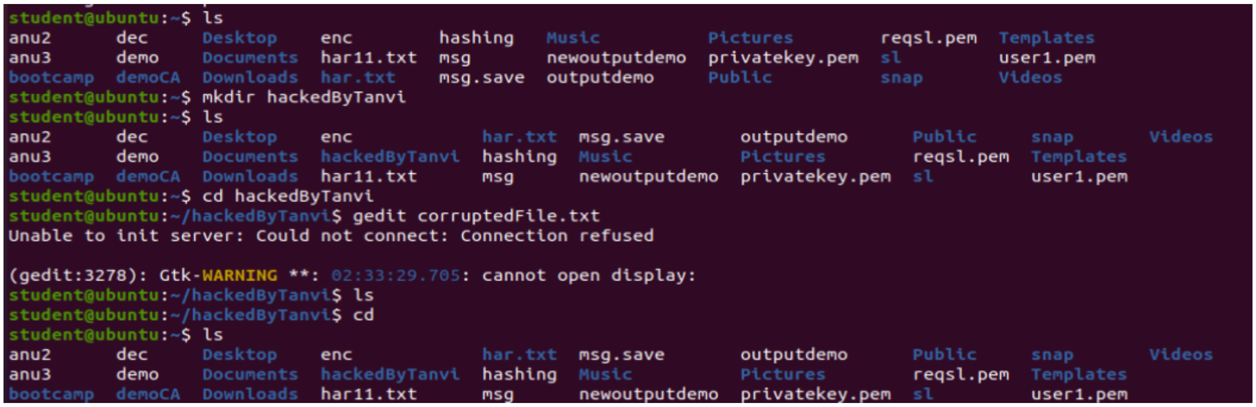


```
student@ubuntu:~$ cat /var/log/auth.log | grep 172.20.210.139
Sep 15 01:17:01 ubuntu sshd[2481]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.210.139  us
er=student
Sep 15 01:17:02 ubuntu sshd[2481]: Failed password for student from 172.20.210.139 port 60786 ssh2
Sep 15 01:17:13 ubuntu sshd[2481]: message repeated 2 times: [ Failed password for student from 172.20.210.139 port 60786 ssh2]
Sep 15 01:17:13 ubuntu sshd[2481]: Connection closed by authenticating user student 172.20.210.139 port 60786 [preauth]
Sep 15 01:17:13 ubuntu sshd[2481]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=172.20.210.139  user=studen
t
Sep 15 01:17:19 ubuntu sshd[2487]: Accepted password for student from 172.20.210.139 port 60790 ssh2
student@ubuntu:~$
```

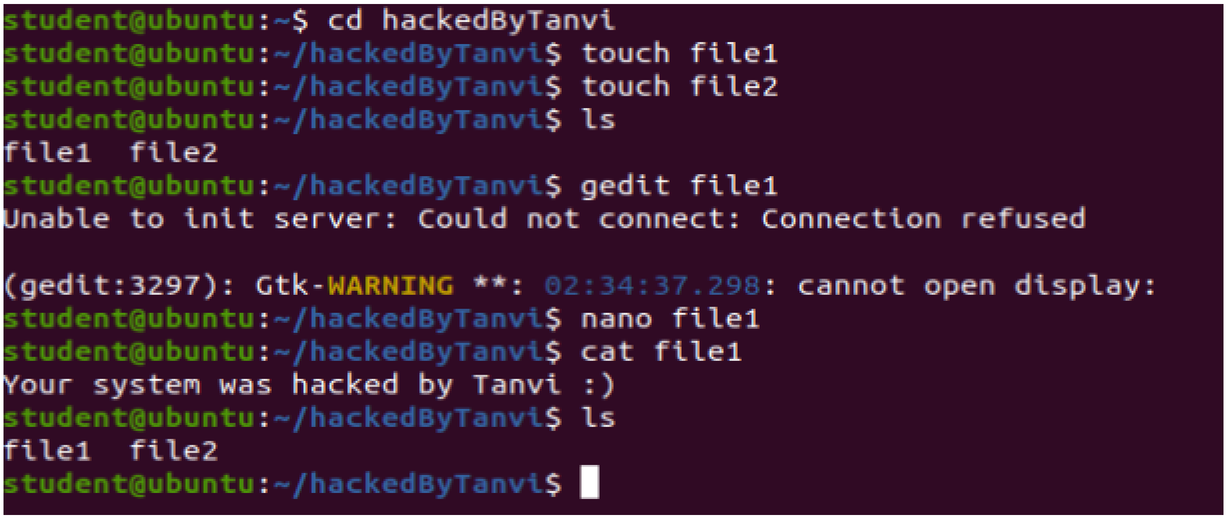
Hacking :



```
student@ubuntu:~/Desktop$ ssh student@172.20.210.139
student@172.20.210.139's password:
Permission denied, please try again.
student@172.20.210.139's password:
Permission denied, please try again.
student@172.20.210.139's password:
student@172.20.210.139: Permission denied (publickey,password).
student@ubuntu:~/Desktop$ ssh student@172.20.210.139
student@172.20.210.139'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


The list of available updates is more than a week old.
To check for new updates run: sudo apt update

10 updates could not be installed automatically. For more details,
see /var/log/unattended-upgrades/unattended-upgrades.log
Last login: Mon Sep 12 02:40:53 2022 from 172.20.210.125
```



```
student@ubuntu:~$ ls
anu2      dec     Desktop    enc        hashing  Music          Pictures        reqsl.pem  Templates
anu3      demo    Documents  har11.txt  msg      newoutputdemo  privatekey.pem  sl         user1.pem
bootcamp  demoCA  Downloads  har.txt    msg.save outputdemo     Public          snap       Videos
student@ubuntu:~$ mkdir hackedByTanvi
student@ubuntu:~$ ls
anu2      dec     Desktop    enc            har.txt  msg.save       outputdemo      Public     snap       Videos
anu3      demo    Documents  hackedByTanvi  hashing  Music          Pictures        reqsl.pem  Templates
bootcamp  demoCA  Downloads  har11.txt      msg      newoutputdemo  privatekey.pem  sl         user1.pem
student@ubuntu:~$ cd hackedByTanvi
student@ubuntu:~/hackedByTanvi$ gedit corruptedFile.txt
Unable to init server: Could not connect: Connection refused

(gedit:3278): Gtk-WARNING **: 02:33:29.705: cannot open display:
student@ubuntu:~/hackedByTanvi$ ls
student@ubuntu:~/hackedByTanvi$ cd
student@ubuntu:~$ ls
anu2      dec     Desktop    enc            har.txt  msg.save       outputdemo      Public     snap       Videos
anu3      demo    Documents  hackedByTanvi  hashing  Music          Pictures        reqsl.pem  Templates
bootcamp  demoCA  Downloads  har11.txt      msg      newoutputdemo  privatekey.pem  sl         user1.pem
```



```
student@ubuntu:~$ cd hackedByTanvi
student@ubuntu:~/hackedByTanvi$ touch file1
student@ubuntu:~/hackedByTanvi$ touch file2
student@ubuntu:~/hackedByTanvi$ ls
file1  file2
student@ubuntu:~/hackedByTanvi$ gedit file1
Unable to init server: Could not connect: Connection refused

(gedit:3297): Gtk-WARNING **: 02:34:37.298: cannot open display:
student@ubuntu:~/hackedByTanvi$ nano file1
student@ubuntu:~/hackedByTanvi$ cat file1
Your system was hacked by Tanvi :)
student@ubuntu:~/hackedByTanvi$ ls
file1  file2
student@ubuntu:~/hackedByTanvi$ 
```