

# Homework Assignment-3

Kaustav Vats (2016048)

## Part I

1. I created my public and private key using this command - **gpg --full-generate-key** (4096 bits)

```
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1$ gpg --full-generate-key
gpg (GnuPG) 2.2.4; Copyright (C) 2017 Free Software Foundation, Inc.
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

Please select what kind of key you want:
  (1) RSA and RSA (default)
  (2) DSA and Elgamal
  (3) DSA (sign only)
  (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits long.
What keysize do you want? (3072) 4096
Requested keysize is 4096 bits
Please specify how long the key should be valid.
    0 = key does not expire
    <n> = key expires in n days
    <n>w = key expires in n weeks
    <n>m = key expires in n months
    <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y

GnuPG needs to construct a user ID to identify your key.

Real name: Kaustav Vats
Email address: kaustav16048@iiitd.ac.in
Comment: this is for fcs assignment
You selected this USER-ID:
    "Kaustav Vats (this is for fcs assignment) <kaustav16048@iiitd.ac.in>"
```

2. This command can be used for encrypting a file with person email id - **gpg --encrypt --sign --armor -r kaustav16048@iiitd.ac.in file.txt**

Here i encrypted file.txt with my public key and signed it using my private key. --armor converts the file to a pgp encrypted text with same name as the input file, but with an .asc extension. Here -r is the receipts email address. This will encrypt message with person public key and will only be decrypted with associated private key.

```

kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1/EncryptDecrypt$ cat file.txt.asc
-----BEGIN PGP MESSAGE-----

hQIMAZd22kBBUPDPAQ/+ONXVUJhbmuYqG5bRlxTBK/7lorixwzkn09FgdocdDPd4
60/sNeyTzSd81QSLDJKAGNSaKbbVh+KdJBIA+NJpulweTVyxzqhrClB/G9iuguTY
bMg9DQG+ucON/UHnPL7kfubykhxGsRUqDR74sr17FR2ybVtpyHBzXIilQq1+xkf6
X5U2GxmL302olje2BlzAYBn+GCdM4TzRYEmmXkQLGi0Tv4dXqGhusXYupQ1kidW
ekpNSkUevj6fytpRqQASLKD0Hu6uyJB0rLuiGABptdRB9dXJ2xmeP7HiT0kQJFYc
nfEB6bvxDFlxeSh4w+MnJtpexufo0WttDnHnTRSc+fsiotCENFD5ew60ycGaLS8q
U1R6tVatFM0If/JK0gj6YX9TccxYDIyGxK/LhnNkD34d+6srst40VCiT+UzDHJ4I
bqYBpjFDV3ZFF9iIBBLj3dmF5do080Y0F77ktgLq19NPjB7jEtL5jnJvn5/rZt6X
uDoY1dhA/Io+3omBGjsVAoj1vC7znTkaJSBJDPWi07LCD5bvysrKqRZjkcH/LMPy
Aynu2LYuME9vhG32aPmZK+DEmfdLu4mzCNGnTj7RlBazz6vcEvSxq86lcYmN6CH
3KrExkEuVq80RhvjBpbZgFwjG8JCR13YdKIMZwemzNJ/eUkF0FVLx7xqBFHzPQnS
6QFFF1P/SYwLCyNf7W1UfPVv3+H3KBYQGkt2qK74XQbJo9dHkxQCT/1WmZ1Erqy
RJVly530098n1jyk0cwMXFrMy0bfuqBgez2w+7pzThnTpDek14wt8CVYPUshCuE
SyjvaZtZelfd/0Q1pVM24AtFu+N17eMP2Io3Nssvo7wrs5Hp6XCCmsFrVUAaXrGi
+liKPXgTu0fdEeli+h3An2ZooY56G4tFwj1aMkXV0xk7AGECVvFRBdwcilz8J70F
a8fb+IMiPSxmuNxmxaaymSWv8k6sjhvJL04W5YGHZib0phDHnDfB42tGLDGPi05h
43kkNKVbKg94qQ0Y3Qv0Lf94mYeVHtm0FkauJr1LHoxhLkY+dfa6a2G0UZHsk0uL
uLWLYyHI7yx09NaHAI0Cur72Cs22+h1QrCRP3InCsrTHDIDFEPd2jP/LidSxupRh
269AQBIYIQLXPNxe8Hbk3IRU+v4YzWnVYZt4TnSNMvVGqe0Shqwb8GhM6qSz8C+G
9BpZqBSWzPcz68RS8SXlj4fgPlye01vp+kQJCrL08XZndkFSqBrA/Kn7T44w5qm2
ANrLQEiGSmTWRzkrVCRqNxMDW0LjSpL8LR7uaKu4/Wm8PMhr6TnuQwJWWy2FRY0Y
wReALrt/mk0Pjpdot+o8frxD4uUpqSK8ibxybhCSYJJFrJptgrIK9RA3g+k9Q183
ATjLXIVZd0MBQUITWZu0JW21lcYHje8Xmig+3pXnAMlsRdi8hHgIDCH4YL8LGZP3
0CJUyY6XnktboWJutus8BkaW0YdLaYML5fgcaC9L7IEEUDMsHs/Fjk+LYmW6cyaf
27Xb/e6KoFwsQb1K14My8B1S1A2T7dsbqoSmfHcbp5vUGFJuc6W8MbsNNIN0tptR
YqJ28PVvFN+ndT56AJE=
=RdYJ
-----END PGP MESSAGE-----

```

```

kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1$ gpg --encrypt --sign --armor -r kaust
av16048@iiitd.ac.in file.txt
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1$ ls
EncryptDecrypt file.txt file.txt.asc mypgg.key
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1$ mv file.txt.asc EncryptDecrypt/
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1$ cd EncryptDecrypt/
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1/EncryptDecrypt$ gpg file.txt.asc
gpg: WARNING: no command supplied. Trying to guess what you mean ...
gpg: encrypted with 4096-bit RSA key, ID 3776DA404150F0CF, created 2018-11-13
"Kaustav Vats (this is for fcs assignment) <kaustav16048@iiitd.ac.in>"
gpg: Signature made Tue 13 Nov 2018 09:14:16 PM +0545
gpg: using RSA key A0C1271FC2957ECB00D4FEDE5CE98C060894345A
gpg: Good signature from "Kaustav Vats (this is my key for fcs assignment) <kausta
v16048@iiitd.ac.in>" [ultimate]
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1/EncryptDecrypt$ ls
file.txt file.txt.asc
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1/EncryptDecrypt$ cat file.txt
Hello

Test file for FCS Q1.

Yo
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1/EncryptDecrypt$

```



3. Using this command one can decrypt message if it was encrypted with his/her public key.

**gpg file.txt.asc**

Since i encrypted file.txt with my own public key, because of this i'm able to decrypt it with my private key and read the content of the file.

If i've encrypted with different recipients public key, then only that person can decrypt using his/her private key.

```
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1/EncryptDecrypt$ gpg file.txt.asc
gpg: WARNING: no command supplied. Trying to guess what you mean ...
gpg: encrypted with 4096-bit RSA key, ID 3776DA404150F0CF, created 2018-11-13
    "Kaustav Vats (this is for fcs assignment) <kaustav16048@iiitd.ac.in>"
File 'file.txt' exists. Overwrite? (y/N) y
gpg: Signature made Tue 13 Nov 2018 09:14:16 PM +0545
gpg:                using RSA key A0C1271FC2957ECB00D4FEDE5CE98C060894345A
gpg: Good signature from "Kaustav Vats (this is my key for fcs assignment) <kausta
v16048@iiitd.ac.in>" [ultimate]
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1/EncryptDecrypt$ cat file.txt
Hello

Test file for FCS Q1.

Yo
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q1/EncryptDecrypt$
```

## Part II

1. Hash with time shown in below image. Commands shown in image. Tested on pycharm tar file.

```

kvats@alienware-ubuntu:~/Downloads$ time md5sum pycharm-professional-2018.2.2.tar.gz
43fad5dd231cd278501c81f8c783b689  pycharm-professional-2018.2.2.tar.gz

real    0m1.136s
user    0m1.046s
sys     0m0.084s
kvats@alienware-ubuntu:~/Downloads$ time sha1sum pycharm-professional-2018.2.2.tar.gz
43aa1358ca95740e324122741d6d6e3074427435  pycharm-professional-2018.2.2.tar.gz

real    0m1.292s
user    0m1.232s
sys     0m0.056s
kvats@alienware-ubuntu:~/Downloads$ time sha224sum pycharm-professional-2018.2.2.tar.gz
4cc472e63fd7ca50c5dc492b4d61643c426df715e505f2201cc2f028  pycharm-professional-2018.2.2.tar.gz

real    0m3.130s
user    0m3.031s
sys     0m0.092s
kvats@alienware-ubuntu:~/Downloads$ time sha256sum pycharm-professional-2018.2.2.tar.gz
e7ce851728c411ff2112b82bfabbcb8d20d0433a8d7ce06887588cb278f8c8b1  pycharm-professional-2018.2.2.tar.gz

real    0m3.096s
user    0m3.013s
sys     0m0.080s
kvats@alienware-ubuntu:~/Downloads$ time sha384sum pycharm-professional-2018.2.2.tar.gz
b560cc90ff046d102670971ee1ee3894382cccd6e624fa8e516fa79d661e5218914f00257dbc0ee0434df49ce48  pycharm-professional-2018.2.2.tar.gz

real    0m1.999s
user    0m1.916s
sys     0m0.072s
kvats@alienware-ubuntu:~/Downloads$ time sha512sum pycharm-professional-2018.2.2.tar.gz
1ed7156434d3b5891547b0579732f276dfb1415765eebf2d90a6c14f687d063562676881fe73a0c6d2a3d8557eaed20d5a8c1fcef04612f45dd9659e74b7  pycharm-professional-2018.2.2.tar.gz

real    0m1.987s
user    0m1.927s
sys     0m0.057s
kvats@alienware-ubuntu:~/Downloads$ time sha3sum pycharm-professional-2018.2.2.tar.gz
3aaa563c7f0bc34b2cb265bc5d1341044fe287cce559331e34a8df85  pycharm-professional-2018.2.2.tar.gz

real    0m2.760s
user    0m2.679s
sys     0m0.076s

```

2. I used md5 hash to calculate checksum using below steps:

a. Steps to identify files modified by third party.

- Place the original files and tampered files in different folder.
- Calculate md5 checksum of the original file and save it in a file.  
Using this command - **md5sum file1.txt file2.txt > csum.md5**
- Copy paste this file csum.md5 to tampered file folder.

- Calculate checksum of tampered file and compare with csum.md5 using this command - **md5sum -c csum.md5**

```
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q2/checksum/driveFiles$  
ls  
100west.txt 13chil.txt 14.lws 16.lws 17.lws csum.md5  
kvats@alienware-ubuntu:~/Desktop/HW3_FCS/Q2/checksum/driveFiles$  
md5sum -c csum.md5  
100west.txt: FAILED  
13chil.txt: OK  
14.lws: OK  
16.lws: FAILED  
17.lws: OK
```

2 File were modified.

100west.txt and 16.lws

- b. Checksum of file remain same if they are not modified. It's not possible to have a same checksum even after tampering the file. Checksum of a file changes if any of its detail is changed.
- c. MD5 and SHA1 will face issue, since they are both not secure. Various vulnerabilities are found for MD5. Collision occur in MD5. Some of the attacks like chosen prefix collision attack are found for MD5. SH1 is also vulnerable to attacks and is considered insecure, but less vulnerable as compared to SH1, because SHA1 has more rounds than MD5. Each hash is much more mixed than MD5.

### Part III

1. Usage for the program: `./passwd <option> <star>`

Here <option> can be -r, -a and <star> Non zero number to show asterisk.

```

Kaustav@Alienware->Q3$ ./passwd -r 98
Enter Username: kaustav
Enter Password: *****
kaustav
[success] User registered successfully!
Kaustav@Alienware->Q3$ ./passwd -a 0
Enter Username: kaustav
Enter Password:
[success] Authenticated
Kaustav@Alienware->Q3$ ./passwd -a 0
Enter Username: kasdkasd
Enter Password:
[error] User not registered
Kaustav@Alienware->Q3$ ./passwd -a 87
Enter Username: kaustav
Enter Password: *****
[success] Authenticated
Kaustav@Alienware->Q3$ ./passwd -a 84
Enter Username: aasdasdasd
Enter Password: *****
[error] User not registered
Kaustav@Alienware->Q3$

```

Credentials are stored in a file credentials.dat

2. Run BruteForce.c to find credentials for 'kv' user.
3. Earlier password were kept in a file /etc/passwd. That file was world readable to provide user related information other than password, many application require these information to work properly.

```

kvats@alienware-ubuntu:/etc$ ls -l passwd
-rw-r--r-- 1 root root 2447 Oct 14 03:48 passwd

```

We can see that read permission is provided to every group. If we change the permission we will face issue using home directory etc. Due to these reason this file is kept world readable. But a user password cannot be kept in a world readable file for security reasons. So password were needed to be separated from this file and store in another file called shadow.

```

kvats@alienware-ubuntu:/etc$ ls -l shadow
-rw-r----- 1 root shadow 1239 Oct 14 03:48 shadow

```

This file is not world readable thus provide security. The password is stored as a one way hash in shadow file with salt and hashing algorithm used to create the hash of the password. When we enter our password it uses the salt and text entered to generate a new hash and compare it with the stored hash.



4. To prevent from brute force attack we can limit the number of attempts of login for a user. Or ban it for few hours. Or can also give sum custom captcha like sum of two random numbers.
5. Using John the ripper i was able to crack my vm password in no time.

```
kvats@alienware-ubuntu:~/Downloads/john-1.8.0/run$ sudo ./john /etc/shadow
Loaded 1 password hash (md5crypt [MD5 32/64 X2])
Press 'q' or Ctrl-C to abort, almost any other key for status
kvats (kvats)
1g 0:00:00:00 100% 1/3 50.00g/s 100.0p/s 100.0c/s 100.0C/s kvats..kvats99999
Use the "--show" option to display all of the cracked passwords reliably
Session completed
kvats@alienware-ubuntu:~/Downloads/john-1.8.0/run$ sudo ./john /etc/shadow --show
kvats:kvats:17779:0:99999:7:::

1 password hash cracked, 0 left
kvats@alienware-ubuntu:~/Downloads/john-1.8.0/run$
```

Kvats is the username of my VM & kvats is the password for the vm.

## Part IV

### 1. Setting up IPTables

- a. `iptables -I INPUT -p icmp --icmp-type echo-request -j DROP`

Above command can be used to stop reply for ping request made from other servers.

IP - 192.168.150.131

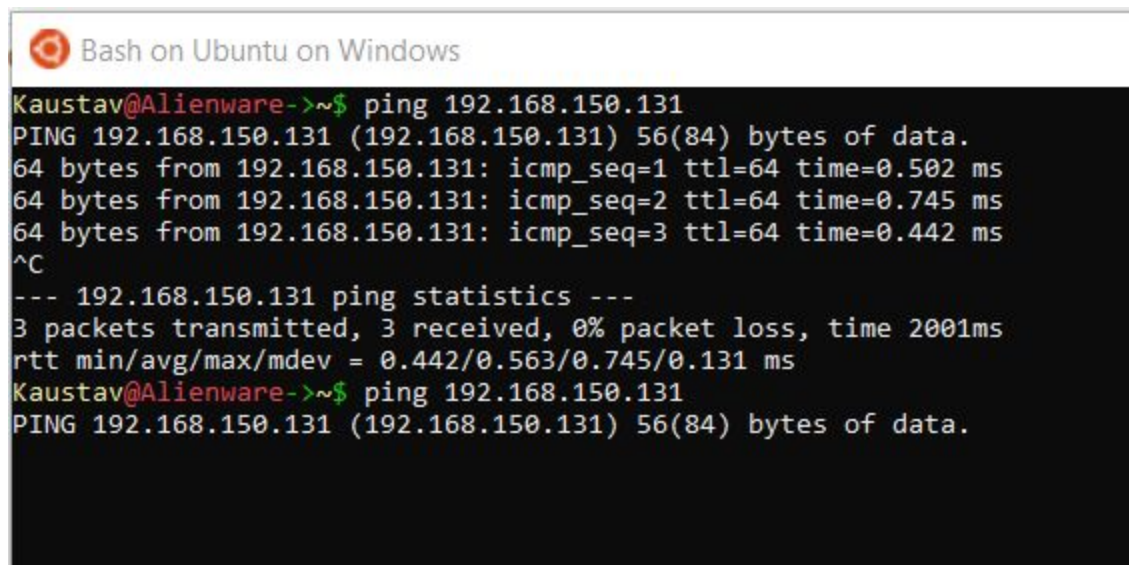
```

kvats@madkv:~$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.150.131 netmask 255.255.255.0 broadcast 192.168.150.255
    inet6 fe80::20c:29ff:feb5:370c prefixlen 64 scopeid 0x20<link>
    ether 00:0c:29:b5:37:0c txqueuelen 1000 (Ethernet)
    RX packets 16889 bytes 20968655 (20.9 MB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 7384 bytes 480689 (480.6 KB)
    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 492 bytes 34990 (34.9 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 492 bytes 34990 (34.9 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

kvats@madkv:~$ sudo iptables -I INPUT -p icmp --icmp-type echo-request -j DROP
kvats@madkv:~$ sudo iptables -L -v
Chain INPUT (policy ACCEPT 5 packets, 575 bytes)
  pkts bytes target     prot opt in     out     source               destination
   25  2100 DROP      icmp  --  any    any     anywhere             anywhere           icmp echo-request
   48  3000 ACCEPT    all  --  lo     any     anywhere             anywhere
    0    0 ACCEPT    tcp  --  any    any     anywhere             anywhere           tcp dpt:ssh
    0    0 ACCEPT    tcp  --  any    any     anywhere             anywhere           tcp dpt:http
    0    0 ACCEPT    tcp  --  any    any     anywhere             anywhere           tcp dpt:44
    0    0 ACCEPT    tcp  --  any    any     anywhere             anywhere           tcp dpt:https

```



```

Kaustav@Alienware-~>$ ping 192.168.150.131
PING 192.168.150.131 (192.168.150.131) 56(84) bytes of data.
64 bytes from 192.168.150.131: icmp_seq=1 ttl=64 time=0.502 ms
64 bytes from 192.168.150.131: icmp_seq=2 ttl=64 time=0.745 ms
64 bytes from 192.168.150.131: icmp_seq=3 ttl=64 time=0.442 ms
^C
--- 192.168.150.131 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 0.442/0.563/0.745/0.131 ms
Kaustav@Alienware-~>$ ping 192.168.150.131
PING 192.168.150.131 (192.168.150.131) 56(84) bytes of data.

```

First ping is when server was accepting ping request. Second ping request was generated after disabling echo reply for ping.

Below image shows that i was able to ping to my main machine from ubuntu server after disabling echo reply.

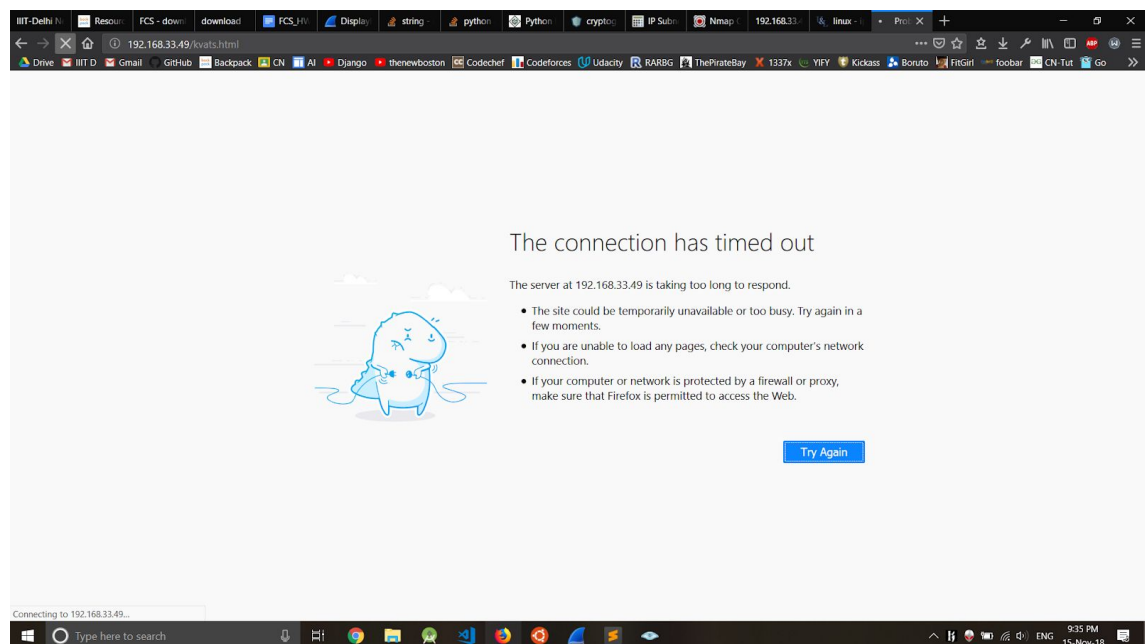


```

kvats@madkv:~$ ping 192.168.47.1
PING 192.168.47.1 (192.168.47.1) 56(84) bytes of data.
64 bytes from 192.168.47.1: icmp_seq=1 ttl=128 time=0.806 ms
64 bytes from 192.168.47.1: icmp_seq=2 ttl=128 time=1.18 ms
64 bytes from 192.168.47.1: icmp_seq=3 ttl=128 time=1.22 ms
64 bytes from 192.168.47.1: icmp_seq=4 ttl=128 time=1.06 ms
64 bytes from 192.168.47.1: icmp_seq=5 ttl=128 time=1.04 ms
64 bytes from 192.168.47.1: icmp_seq=6 ttl=128 time=1.04 ms
64 bytes from 192.168.47.1: icmp_seq=7 ttl=128 time=0.990 ms
64 bytes from 192.168.47.1: icmp_seq=8 ttl=128 time=1.06 ms
64 bytes from 192.168.47.1: icmp_seq=9 ttl=128 time=0.950 ms
64 bytes from 192.168.47.1: icmp_seq=10 ttl=128 time=1.01 ms
64 bytes from 192.168.47.1: icmp_seq=11 ttl=128 time=0.993 ms
64 bytes from 192.168.47.1: icmp_seq=12 ttl=128 time=1.02 ms
64 bytes from 192.168.47.1: icmp_seq=13 ttl=128 time=0.948 ms
64 bytes from 192.168.47.1: icmp_seq=14 ttl=128 time=1.05 ms
64 bytes from 192.168.47.1: icmp_seq=15 ttl=128 time=1.07 ms
64 bytes from 192.168.47.1: icmp_seq=16 ttl=128 time=1.02 ms
^C
--- 192.168.47.1 ping statistics ---
16 packets transmitted, 16 received, 0% packet loss, time 77ms
rtt min/avg/max/mdev = 0.806/1.027/1.216/0.096 ms
kvats@madkv:~$

```

- b. On Adding these commands i was able to allow only my Phone to access the website.



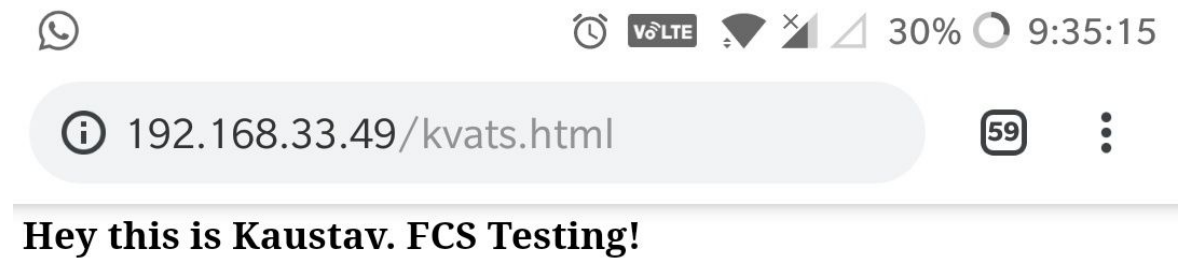
**Sudo iptables -A INPUT -s 192.168.169.32 -j ACCEPT**

**Sudo iptables -A OUTPUT -d 192.168.169.32 -j ACCEPT**

**Sudo iptables -P INPUT DROP**

**Sudo iptables -P OUTPUT DROP**

Above command will only allow entered ip request for the server. All other packets coming from different ip will be dropped.



2. To find open ssh port on a subnet, we can use this command :

**Nmap -p 22 --open 192.168.33.0/20**

```
Nmap scan report for 192.168.41.1
Host is up (0.0014s latency).
PORT      STATE SERVICE
22/tcp    open  ssh

Nmap done: 4096 IP addresses (142 hosts up) scanned in 37.42 seconds
iiiitd@iiiitd-ThinkCentre-M900:~$ ifconfig
eno1      Link encap:Ethernet  HWaddr 4c:cc:6a:3c:3f:7a
          inet addr:192.168.33.48 Bcast:192.168.47.255 Mask:255.255.255
          inet6 addr: fe80::85:6dd4:fc64:4341/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1199510 errors:0 dropped:0 overruns:0 frame:0
          TX packets:100761 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:182864448 (182.8 MB)  TX bytes:11790623 (11.7 MB)
          Interrupt:16 Memory:df000000-df020000
```

I found that 142 hosts provide access to ssh. Ip range: **192.168.32.1 - 192.168.47.254**

OS Fingerprinting was taking too much time. Well the command i was using is for the students subnet. It was unclear that hostel has a separate subnet or not. Some seniors said we are assigned our ip under students subnet. Based on the above assumptions i got around 62% of Windows user and 27% of Linux user. Note these values are not actual values and depend on the number of devices connected.

3. My Phone ip: 192.168.169.32

```

iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 TLS: Initial packet from [AF_INET]192.168.169.32:41
iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 CRL CHECK OK: CN=ChangeMe
iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 VERIFY OK: depth=1, CN=ChangeMe
iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 CRL CHECK OK: CN=fcs
iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 VERIFY OK: depth=0, CN=fcs
iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 Data Channel Encrypt: Cipher 'AES-256-CBC' initiali
iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 Data Channel Encrypt: Using 512 bit message hash 'S
iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 Data Channel Decrypt: Cipher 'AES-256-CBC' initiali
iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 Data Channel Decrypt: Using 512 bit message hash 'S
iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 Control Channel: TLSv1.2, cipher TLSv1/SSLv3 DHE-RS
iitd-ThinkCentre-M900 ovpn-server[15244]: 192.168.169.32:41382 [fcs] Peer Connection Initiated with [AF_INET]192.1
iitd-ThinkCentre-M900 ovpn-server[15244]: MULTI: new connection by client 'fcs' will cause previous active session
uplicate-cn option if you want multiple clients using the same certificate or username to concurrently connect.
iitd-ThinkCentre-M900 ovpn-server[15244]: MULTI_sva: pool returned IPv4=10.8.0.2, IPv6=(Not enabled)
iitd-ThinkCentre-M900 ovpn-server[15244]: MULTI: Learn: 10.8.0.2 -> fcs/192.168.169.32:41382
iitd-ThinkCentre-M900 ovpn-server[15244]: MULTI: primary virtual IP for fcs/192.168.169.32:41382: 10.8.0.2
iitd-ThinkCentre-M900 ovpn-server[15244]: fcs/192.168.169.32:41382 PUSH: Received control message: 'PUSH_REQUEST'
iitd-ThinkCentre-M900 ovpn-server[15244]: fcs/192.168.169.32:41382 send_push_reply(): safe_cap=940
iitd-ThinkCentre-M900 ovpn-server[15244]: fcs/192.168.169.32:41382 SENT CONTROL [fcs]: 'PUSH_REPLY,redirect-gatewa
10.8.0.1,topology subnet,ping 10,ping-restart 120,ifconfig 10.8.0.2 255.255.255.0' (status=1)

```

My Laptop main OS is windows and i run Apache on VM. So i tried using openVPN and connected to a lab pc via vpn and tried to access another lab pc which has a apache server. Fcs.ovpn attached with assignment.

**Status**

**Battery status**  
 Not charging

**Battery level**  
 23%

**SIM status**

**IMEI information**

**IP address**  
 192.168.169.32  
 fe80::b086:9df3:f207:b6e6



## Part V

1.

1. There are 189 unique ip address and 13 unique mac address. File attached with the assignment(ip.txt, mac.txt).

Calculated using wireshark and a shell command.

```
tshark -r log.pcap -T fields -e ip.src -e ip.dst | tr "\t" "\n" | sort | uniq > ip.txt
```

```
tshark -r log.pcap -T fields -e eth.src -e eth.dst | tr "\t" "\n" | sort | uniq > mac.txt
```

2. ISP Backbone. Since all the traffic is going through one IP 10.0.2.3 They have a separate DNS server. All traffic is goes through ISP Block. Many DNS request are also made. Server has also provided some file request. Server accepts request at normal http port 80.
3. DNS Hostname- dl.xs4all.nl (194.109.21.66). FTP is not safe for transferring sensitive data. FTP sends data in clear text. Alternative would be to use HTTPS. Which provide encryption over network layer. All packets send using https protocol are encrypted.
4. Client provided MD5 , SHA1 cipher algorithm. Well both of them are worrisome. Since both of them are cracked or can be break. MD5 consist of multiple collision which make more vulnerable.
5. Attacker can try to install some extension in user browser by some convincing way which might corrupt browser. Attacker can act as a proxy server and install some other CA certificate. Then all communication made by user will be accessible by the attacker. Even the connection is HTTPS. But attacker can still do this and attack the genuine user.