

Name :- Ronak Kumar

Roll No :- 2015080

FCS Assignment 3

Part I

A1)

I created my public and private GPG key pair (4096 bit). The keys are in the Part I Folder.

Commands :-

```
gpg --gen-key
```

```
gpg -a --export ronak15080@iiitd.ac.in > mypubkey.asc
```

```
gpg -a --export ronak15080@iiitd.ac.in > mysecretkey.asc
```

The mypubkey.asc is the public GPG key and the mysecretkey.asc is the private GPG key.

A2)

The files are in the Part I Folder

Commands :-

```
gpg --armor -e -r ronak15080@iiitd.ac.in file.txt
```

```
gpg --sign --default-key ronak15080@iiitd.ac.in file.txt.asc
```

A3)

No, it is not possible to decrypt the file since the file is first encrypted with the GPG public key whose private key I don't know. Also, since the passphrase used during the signature phase is not available, it is not possible to decrypt the file.txt from the signature file.

Part II

A1)

Screenshot :-

```
darkcoder@darkcoder: ~/Desktop/FCS Assignment 3/Part II
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ time md5sum large_file.txt
4a2a907d1321051cf013789a7c000c4  large_file.txt
real    0m0.102s
user    0m0.089s
sys     0m0.014s
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ time sha1sum large_file.txt
1149a2b29a7a1a1fa22d4f72122d179a9a87839e2  large_file.txt
real    0m0.103s
user    0m0.103s
sys     0m0.000s
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ time sha224sum large_file.txt
3bd17115f34bda352b8dd72d4685946a6ffabaff0db1a4466ed3f1e  large_file.txt
real    0m0.210s
user    0m0.201s
sys     0m0.009s
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ time sha256sum large_file.txt
080e26f5b88f2f036a26a2b55654218bf4a960b643f14772f5139b23620159c  large_file.txt
real    0m0.212s
user    0m0.199s
sys     0m0.013s
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ time sha384sum large_file.txt
a50f7071b71a3b3955175255848eef9ee0e1e16a059b06c90d54f6308126accc096a4521be5828f8a78b24d16904  large_file.txt
real    0m0.147s
user    0m0.144s
sys     0m0.002s
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ time sha512sum large_file.txt
43b3f7471337b7c3b9b2527e5b8b76a59f9ba172bb4046351249b3e74036634ff79bf167526373927f363d9e023ec9a183a0beebf50f5aefb398d5d483  large_file.txt
real    0m0.340s
user    0m0.138s
sys     0m0.008s
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$
```

MD5 is the fastest hash algorithm among all the hashing techniques. SHA256 takes the longest time among all of them. SHA1 takes slight more time than MD5. However, this might fluctuate with CPU factors.

A2)

a)

```
darkcoder@darkcoder: ~/Desktop/FCS Assignment 3/Part II
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ md5sum ./drive_stories/100west.txt && md5sum ./website_stories/100west.txt
98c218ef51e4808e0229e05220baef  ./drive_stories/100west.txt
90bc9a284adb01f1ce130587b7c01d0  ./website_stories/100west.txt
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ md5sum ./drive_stories/13chill.txt && md5sum ./website_stories/13chill.txt
e6011247f142af47a8c2d7f0b938c931  ./drive_stories/13chill.txt
e6011247f142af47a8c2d7f0b938c931  ./website_stories/13chill.txt
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ md5sum ./drive_stories/14.lws && md5sum ./website_stories/14.lws
64579883876e742ffe27e2d778783e03  ./drive_stories/14.lws
64579883876e742ffe27e2d778783e03  ./website_stories/14.lws
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ md5sum ./drive_stories/16.lws && md5sum ./website_stories/16.lws
02b56c5c5d5e98327dc0d0e4c4950664  ./drive_stories/16.lws
a1610930df75ab9bc9452aa8faba89  ./website_stories/16.lws
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$ md5sum ./drive_stories/17.lws && md5sum ./website_stories/17.lws
df14fcd0b833e0c98e1bc4c6e0e6bb  ./drive_stories/17.lws
df14fcd0b833e0c98e1bc4c6e0e6bb  ./website_stories/17.lws
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part II$
```

As, in the above screenshot, I computed the MD5 Checksum of the respective files. The files which are having the same checksum are 13chill.txt, 14.lws, 17.lws i.e these are the files that are not tampered. So, the files that were modified by the third party are 100west.txt & 16.lws as their checksum is different.

The MD5 checksum technique is the fast method for finding any tamperness / modification in the data since, if there is any change in the files then the checksums don't match. I used the MD5 approach as it is the fastest and a reliable source for identifying tamperness and verifying the integrity of the files. The large file taken as input is the same given in the previous Homework 2

b)

Yes, it is possible to modify the content of the file without changing the value of the checksum. A good example for this would be the use of MD5 and the SHA1 algorithms. Both the algorithms can remain the same, even if change the content. This is why it is better to move to more secure hash algorithms like SHA-256 as MD5 and SHA1 are considered to be deprecated in terms of verifying the integrity of the file.

c)

The two properties that may get violated in part b are collision resistance and second preimage resistance. This is because even if the two files have different contents in them still the SHA and the MD5 hash turns out to be the same. Hence it becomes easy to find two hashes with the same value thereby violating the collision resistance property. Also, the second property is violated in the same way since it says that it should be hard to find a different input with the same hash value although now it becomes easy to find as seen in the first example.

Part III

A1)

The code is given in the Part III Folder

A2)

The code is given in the Part III Folder

A3)

The permissions for the file /etc/passwd is "-rw-r--r-- 1 root root 2298 Oct 10 11:00". I ran the `ls -l | grep passwd` command in the /etc directory for getting the

permissions. The first section is for the owner or root user, second for group and the third for normal/other users. So, it means that every user is capable of reading this file but only the root user is allowed to modify or write to the file. The password of the username is stored in the /etc/shadow file. The passwords are encrypted using hashing methods like MD5 or by using Secure Hash Algorithm.

A4)

The code is given in the Part III Folder

A5)

Screenshots :-


```
darkcoder@darkcoder: ~/Desktop/FCS Assignment 3/Part III/john-1.8.0
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part III/john-1.8.0$ ls
doc README run src
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part III/john-1.8.0$ sudo unshadow /etc/passwd /etc/shadow > ~/passwd
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part III/john-1.8.0$ ls
doc README run src
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part III/john-1.8.0$ cat ~/passwd
cat: /home/darkcoder/.passwd: no such file or directory
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part III/john-1.8.0$ cat ~/passwd
root::0:0:root:/root:/bin/bash
daemon:*:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:*:2:2:bin:/bin:/usr/sbin/nologin
sys:*:3:3:sys:/dev:/usr/sbin/nologin
sync:*:4:65534:sync:/bin:/bin/sync
games:*:5:60:games:/usr/games:/usr/sbin/nologin
man:*:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:*:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:*:8:8:mail:/var/mail:/usr/sbin/nologin
news:*:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:*:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:*:13:13:proxy:/bin:/usr/sbin/nologin
www-data:*:33:33:www-data:/var/www:/usr/sbin/nologin
backup:*:34:34:backup:/var/backups:/usr/sbin/nologin
list:*:36:36:MailList Manager:/var/list:/usr/sbin/nologin
irc:*:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:*:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:*:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:*:100:102:systemd Time Synchronization,,:/run/systemd:/bin/false
systemd-networkd:*:101:103:systemd Network Management,,:/run/systemd/netif:/bin/false
systemd-resolve:*:102:104:systemd Resolver,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:*:103:105:systemd Bus Proxy,,:/run/systemd:/bin/false
syslog:*:104:106:/home/syslog:/bin/false
apt:*:105:65534:/nonexistent:/bin/false
messagebus:*:106:110:/var/run/dbus:/bin/false
uidmd:*:107:111:/run/uidmd:/bin/false
lightdm:*:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:*:109:117:/nonexistent:/bin/false
avahi-autoipd:*:110:119:Avahi autoip daemon,,:/var/lib/avahi-autoipd:/bin/false
avahi:*:111:120:Avahi mDNS daemon,,:/var/run/avahi-daemon:/bin/false
dnsmasq:*:112:65534:dnsmasq,,:/var/lib/isc:/bin/false
colord:*:113:123:colord colour management daemon,,:/var/lib/colord:/bin/false
speech-dispatcher:*:114:29:Speech Dispatcher,,:/var/run/speech-dispatcher:/bin/false
hplip:*:115:7:HPLIP system user,,:/var/run/hplip:/bin/false
kernoops:*:116:65534:kernoops Oops Tracking daemon,,:/bin/false
pulse:*:117:124:PulseAudio daemon,,:/var/run/pulse:/bin/false
rtkit:*:118:128:RealtimeKit,,:/usr/bin:/bin/false
saned:*:119:127:/var/lib/saned:/bin/false
usbmux:*:120:40:usbmux daemon,,:/var/lib/usbmux:/bin/false
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part III/john-1.8.0$ john --single ~/passwd
Created directory: /home/darkcoder/.john
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort; Almost any other key for status
0g 0:00:00:00 21% 0g/s 299.3p/s 299.3c/s 299.3C/s KRONAKG.dkumar!!
0g 0:00:00:23 57% 0g/s 300.0p/s 300.0c/s 300.0C/s Kumarronak97.Darkcoderkumar04
0g 0:00:00:27 63% 0g/s 300.0p/s 300.0c/s 300.0C/s darkcoderronak1..ronakdarkcodere
0g 0:00:00:31 73% 0g/s 301.0p/s 301.0c/s 301.0C/s darkcoderkumar30..ronakdarkumar36
0g 0:00:00:34 76% 0g/s 301.4p/s 301.4c/s 301.4C/s Kdarkcoder47..Dronak24
0g 0:00:00:39 89% 0g/s 301.5p/s 301.5c/s 300.0C/s darkcoderkumar1970..ronakdarkumar1970
0g 0:00:00:41 92% 0g/s 300.6p/s 300.6c/s 300.6C/s rkumar2008..kronak2024
0g 0:00:00:45 100% 0g/s 300.7p/s 300.7c/s 300.7C/s ronakdarkoder1904..kronak1900
Session completed
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part III/john-1.8.0$ john --show ~/passwd
1 password hashes cracked, 1 left
darkcoder@darkcoder:~/Desktop/FCS Assignment 3/Part III/john-1.8.0$
```

Part IV

A1)

I disabled the echo-reply (pong) on the local lab machine. I have explained the steps in the form of commands in the order in which I executed :-

ifconfig (Got IP Address of my laptop) (Let it be IP1)

ping IP1 (Got responses)

ifconfig (Got IP Address of the Lab Computer) (Let it be IP2)

sudo iptables -L

sudo iptables -A INPUT -s IP2 -j DROP

Now the IP on the lab machine would come in the list in my laptop

Now if I ping my laptop from the machine i.e IP1 it would not show any results as it is now blocked

If I again want to ping, then I would accept the IP using the command

sudo iptables -D INPUT 1

Then I will be able to ping my laptop i.e IP1 from the lab machine

For blocking all the IPs I used the ACCEPT and the DROP command simultaneously

For connecting to the mobile, I used the following commands

In the folder

Screenshots :-

```
darkcoder@darkcoder: ~/Desktop
darkcoder@darkcoder:~/Desktop$ ifconfig
enp2s0    Link encap:Ethernet  HWaddr 18:db:f2:17:57:5c
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:16970 errors:0 dropped:0 overruns:0 frame:0
          TX packets:16970 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1689995 (1.6 MB)  TX bytes:1689995 (1.6 MB)

wlp1s0    Link encap:Ethernet  HWaddr e4:02:9b:80:c1:40
          inet addr:192.168.56.141  Bcast:192.168.63.255  Mask:255.255.240.0
          inet6 addr: fe80::2f08:2932:11b5:b1f1 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:180721 errors:0 dropped:0 overruns:0 frame:0
          TX packets:435135 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:972256294 (972.2 MB)  TX bytes:92875702 (92.8 MB)

darkcoder@darkcoder:~/Desktop$ sudo iptables -A INPUT -s 192.168.32.181 -j DROP
[sudo] password for darkcoder:
darkcoder@darkcoder:~/Desktop$
```

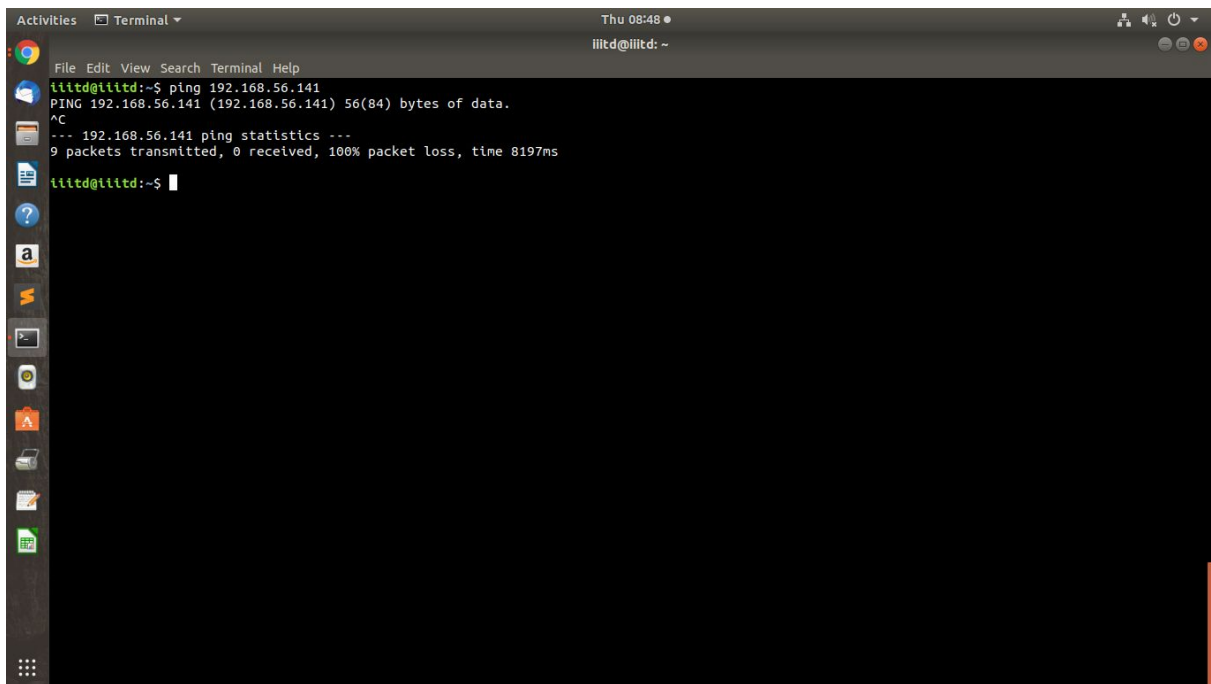
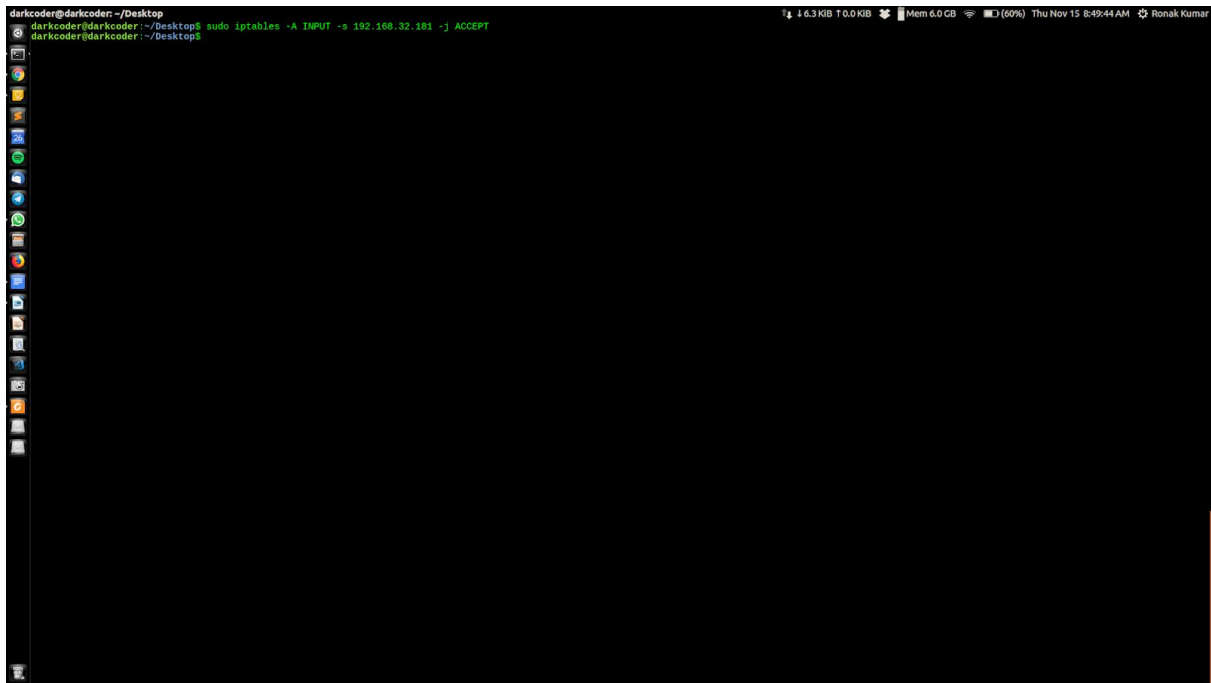
```
Activities  Terminal  Thu 08:48
liltd@liltd: ~

File Edit View Search Terminal Help

liltd@liltd:~$ ping 192.168.56.141
PING 192.168.56.141 (192.168.56.141) 56(84) bytes of data.
64 bytes from 192.168.56.141: icmp_seq=1 ttl=63 time=37.2 ms
64 bytes from 192.168.56.141: icmp_seq=2 ttl=63 time=66.3 ms
64 bytes from 192.168.56.141: icmp_seq=3 ttl=63 time=96.5 ms
64 bytes from 192.168.56.141: icmp_seq=4 ttl=63 time=22.3 ms
64 bytes from 192.168.56.141: icmp_seq=5 ttl=63 time=52.8 ms
64 bytes from 192.168.56.141: icmp_seq=6 ttl=63 time=80.4 ms
^C
--- 192.168.56.141 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 22.345/59.288/96.560/25.109 ms
liltd@liltd:~$ ifconfig
enp1s0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.32.181  netmask 255.255.240.0  broadcast 192.168.47.255
        inet6 fe80::2f08:2932:11b5:b1f1 prefixlen 64 scopeid 0x20<link>
        ether 8c:ec:4b:70:24:7e  txqueuelen 1000  (Ethernet)
        RX packets 11908115  bytes 923029943 (923.0 MB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 243460  bytes 25749065 (25.7 MB)
        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 8430  bytes 698526 (698.5 KB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 8430  bytes 698526 (698.5 KB)
        TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

liltd@liltd:~$
```



A2)

a)

These are the IP addresses of the computers connected to the B-519 subnet and provide access to SSH

Screenshots :-


```
darkcoder@darkcoder: ~/Desktop
darkcoder@darkcoder:~/Desktop$ nmap -p 22 --open -sV 192.168.56.141/20
Starting Nmap 7.01 ( https://nmap.org ) at 2018-11-12 12:02 IST
Nmap scan report for 192.168.49.209
Host is up (0.052s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.50.90
Host is up (0.109s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.50.161
Host is up (0.0079s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.51.32
Host is up (0.052s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)

Nmap scan report for 192.168.51.227
Host is up (0.109s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)

Nmap scan report for 192.168.57.105
Host is up (0.058s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)

Nmap scan report for 192.168.57.121
Host is up (0.0069s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.6 (protocol 2.0)

Nmap scan report for 192.168.57.165
Host is up (0.027s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.58.229
Host is up (0.039s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.9 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.59.80
Host is up (0.109s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.59.193
Host is up (0.094s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)

Nmap scan report for 192.168.50.161
Host is up (0.0079s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.51.32
Host is up (0.052s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)

Nmap scan report for 192.168.51.227
Host is up (0.109s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)

Nmap scan report for 192.168.57.105
Host is up (0.058s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)

Nmap scan report for 192.168.57.121
Host is up (0.0069s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.6 (protocol 2.0)

Nmap scan report for 192.168.57.165
Host is up (0.027s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.58.229
Host is up (0.039s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.5 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.59.80
Host is up (0.109s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.2p2 Ubuntu 4ubuntu2.4 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 192.168.59.193
Host is up (0.094s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.7 (protocol 2.0)

Nmap scan report for 192.168.60.42
Host is up (0.035s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.6 (protocol 2.0)

Nmap scan report for 192.168.61.80
Host is up (0.17s latency).
PORT      STATE SERVICE
22/tcp    open  ssh      OpenSSH 7.6 (protocol 2.0)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 4096 IP addresses (38 hosts up) scanned in 79.47 seconds
darkcoder@darkcoder:~/Desktop$
```

b)

The command used for OS fingerprinting is

nmap -sS -o [IP Address]

A3)

I used the commands given in the screenshot for configuring the VPN in the local lab machine.

Screenshots :-

```
iiitd@iiitd-HP-406-MT: ~/Desktop
Building dependency tree
Reading state information... Done
The following packages were automatically installed and are no longer required:
  libpango1.0-0 libpangox-1.0-0 linux-headers-4.4.0-101-generic linux-headers-4.4.0-101-generic linux-headers-4.4.0-104-generic linux-headers-4.4.0-104-generic
  linux-headers-4.4.0-119-generic linux-headers-4.4.0-119-generic linux-headers-4.4.0-130-generic linux-headers-4.4.0-130-generic linux-image-4.4.0-101-generic
  linux-image-4.4.0-104-generic linux-image-4.4.0-119-generic linux-image-4.4.0-130-generic linux-image-extra-4.4.0-101-generic
  linux-image-extra-4.4.0-104-generic linux-image-extra-4.4.0-119-generic linux-image-extra-4.4.0-130-generic linux-signed-image-4.4.0-101-generic
  linux-signed-image-4.4.0-104-generic linux-signed-image-4.4.0-119-generic linux-signed-image-4.4.0-130-generic ubuntu-core-launcher
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  openvpn
The following NEW packages will be installed:
  network-manager-openvpn network-manager-openvpn-gnome openvpn
0 upgraded, 3 newly installed, 0 to remove and 187 not upgraded.
Need to get 206 kB/627 kB of archives.
After this operation, 2,362 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
Get:1 http://in.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 network-manager-openvpn amd64 1.1.93-1ubuntu1.1 [26.5 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu xenial-updates/universe amd64 network-manager-openvpn-gnome amd64 1.1.93-1ubuntu1.1 [180 kB]
Fetched 206 kB in 2s (73.3 kB/s)
Preconfiguring packages ...
Selecting previously unselected package openvpn.
(Reading database ... 380735 files and directories currently installed.)
Preparing to unpack .../openvpn_2.3.10-1ubuntu2.1_amd64.deb ...
Unpacking openvpn (2.3.10-1ubuntu2.1) ...
Selecting previously unselected package network-manager-openvpn.
Preparing to unpack .../network-manager-openvpn_1.1.93-1ubuntu1.1_amd64.deb ...
Unpacking network-manager-openvpn (1.1.93-1ubuntu1.1) ...
Selecting previously unselected package network-manager-openvpn-gnome.
Preparing to unpack .../network-manager-openvpn-gnome_1.1.93-1ubuntu1.1_amd64.deb ...
Unpacking network-manager-openvpn-gnome (1.1.93-1ubuntu1.1) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
Processing triggers for systemd (229-4ubuntu21.2) ...
Processing triggers for ureadahead (0.100.0-19) ...
Processing triggers for man-db (2.7.5-1) ...
Processing triggers for dbus (1.10.6-1ubuntu3.3) ...
Setting up openvpn (2.3.10-1ubuntu2.1) ...
Setting up network-manager-openvpn (1.1.93-1ubuntu1.1) ...
Setting up network-manager-openvpn-gnome (1.1.93-1ubuntu1.1) ...
Processing triggers for libc-bin (2.23-0ubuntu10) ...
Processing triggers for dbus (1.10.6-1ubuntu3.3) ...
iiitd@iiitd-HP-406-MT:~/Desktop$ sudo apt-get install network-manager-openconnect-gnome network-manager-gnome network-manager-openvpn network-manager-vpnc network
-manager-openconnect network-manager-openvpn-gnome network-manager-vpnc-gnome network-manager-openconnect-gnome network-manager
Reading package lists... Done
Building dependency tree
Reading state information... Done
E: Unable to locate package network-manager
iiitd@iiitd-HP-406-MT:~/Desktop$ service network-manager restart
iiitd@iiitd-HP-406-MT:~/Desktop$
```

```
iiitd@iiitd-HP-406-MT:~/Desktop
Commands after installing packages
iiitd@iiitd-HP-406-MT:~/Desktop$ wget http://www.vpnbook.com/#openvpn^C
iiitd@iiitd-HP-406-MT:~/Desktop$ unzip VPNBook.com-OpenVPN-Euro1.zip^C
iiitd@iiitd-HP-406-MT:~/Desktop$ echo "Sed commands for issuing certificates and keys"
Sed commands for issuing certificates and keys
iiitd@iiitd-HP-406-MT:~/Desktop$ cat vpnbook-euro1-tcp80.ovpn | grep remote^C
iiitd@iiitd-HP-406-MT:~/Desktop$ echo "VPN Server started"
VPN Server started
iiitd@iiitd-HP-406-MT:~/Desktop$
```

Part V

A1

a)

Some of the devices that are connected to the network with their MAC Addresses are :-

IP	MAC
98.139.239.224	8c:a9:82:50:f0:a6
74.125.225.129	00:26:08:e5:66:07

etc..

b)

The network inside the pcap file appears to be an ISP since it involves a lot of private IP addresses. ISP's usually distribute IP's in this manner. Some of the IP's got from Wireshark are 10.0.2.3, 10.0.2.2, 74.125.225.143 etc.

c)

No, in my opinion FTP in basic cannot be regarded as a safe protocol. This is because all of the information that is being transferred is being sent in the form of raw/plain text and can be sniffed. Another version of FTP known as the SFTP involving SSL encryption with FTP can be regarded as secure. Also, we can use HTTPS for encrypting all the data before sending it.

d)

The client tried to connect with "<https://vimeo.com/>". Yes, it is possible that HTTPS Server can protect the information leaking issue in the previous question by encrypting the entire data being send in the request before sending. Through this no one would be able to see the content of the request and the information being sent. A cipher suite is a set of cryptographic algorithms and can be considered as secure however if there is some vulnerability in the algorithm itself then it can become risky for both the cipher suite and TLS/SSL. Then, it may be prone to attacks like Downgrade attack on TLS and cipher suite.

e)

Since, the client has connected Facebook using HTTPS in his browser, but site Vimeo can redirect the user to a fake website by using malicious scripts. This may cause the problem of phishing. Here, the HTTPS does not encourage any security.

A2)

I have attached the python code in the Part V Folder. The IP address that is malicious is given in the output.txt file in the same folder. Ignore the set written that is just the data structure I used.

