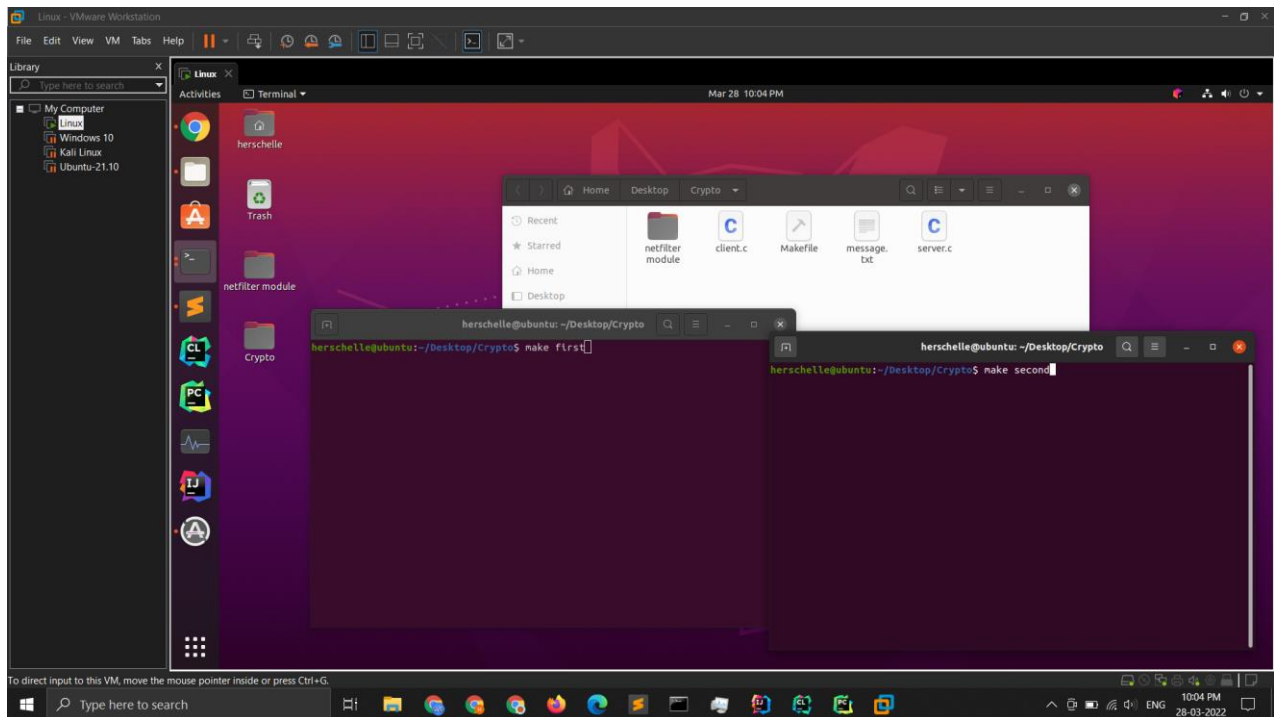
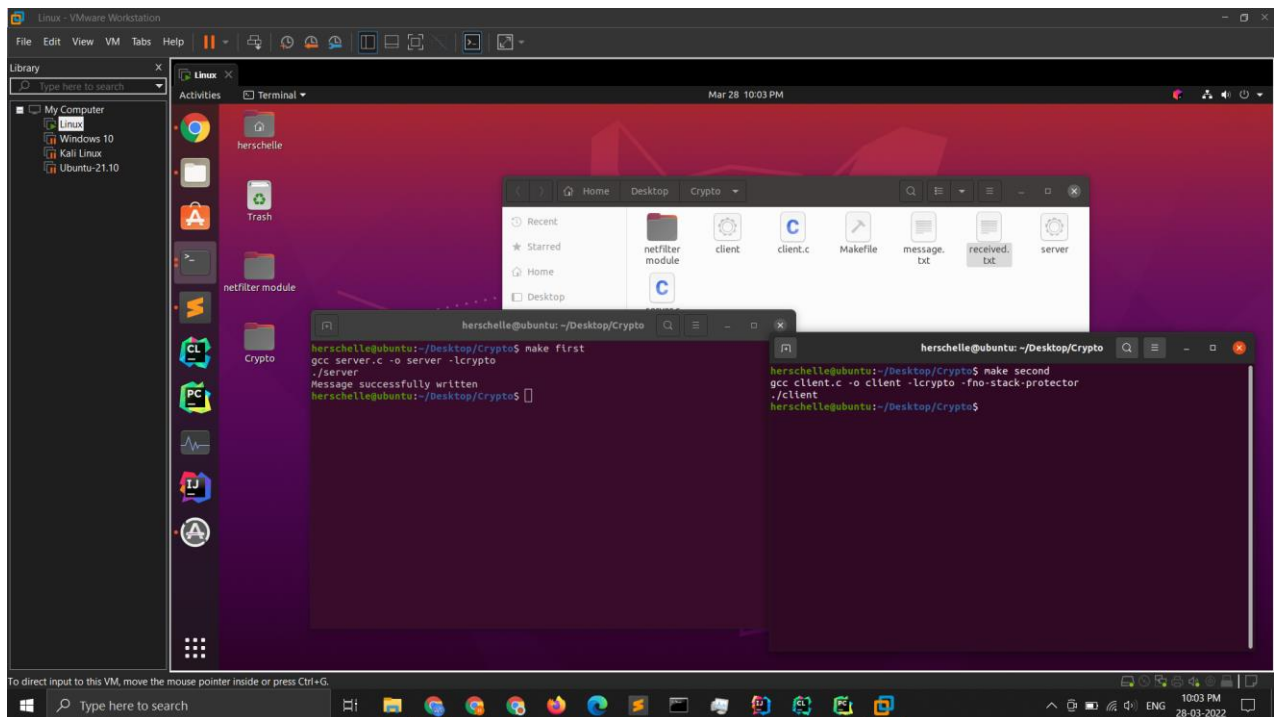


Open two terminals in the folder and type “make first” in one and “make second” in other as shown.

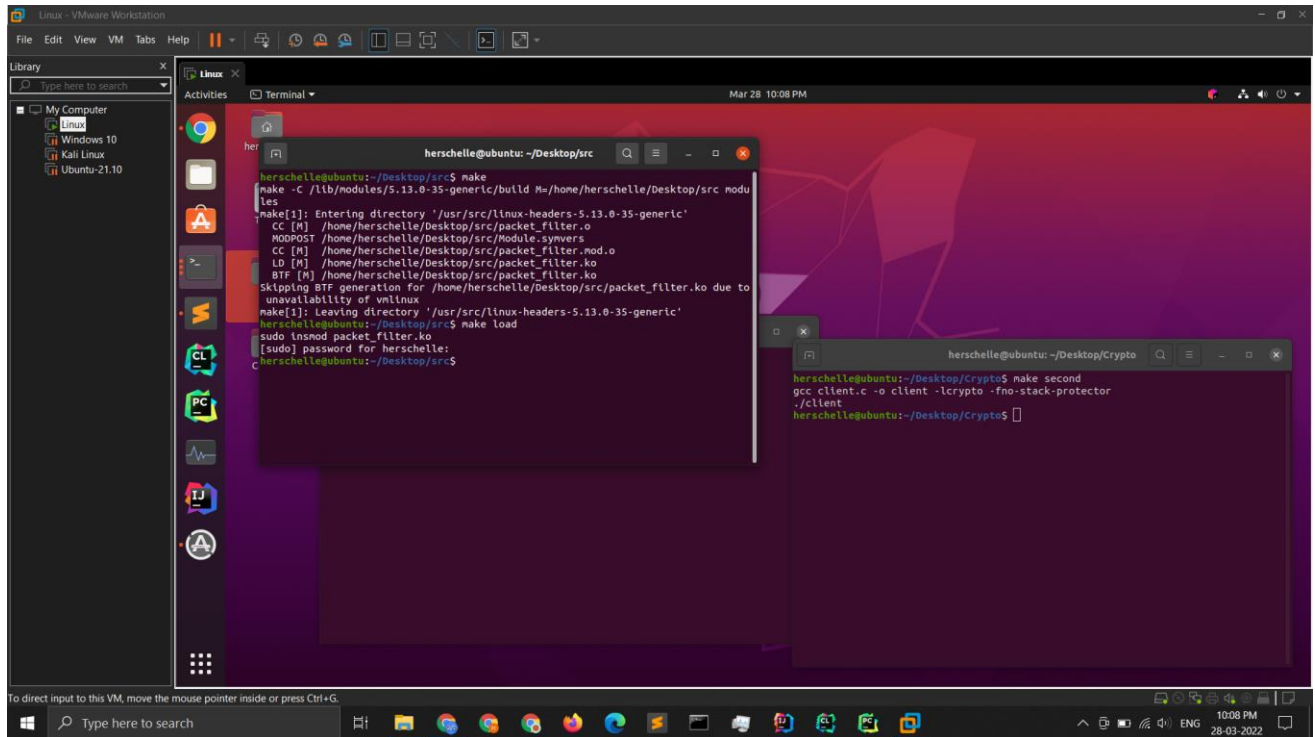


Make sure to run “make first” first as it is the server.



And contents of the message.txt will be transferred to received.txt.

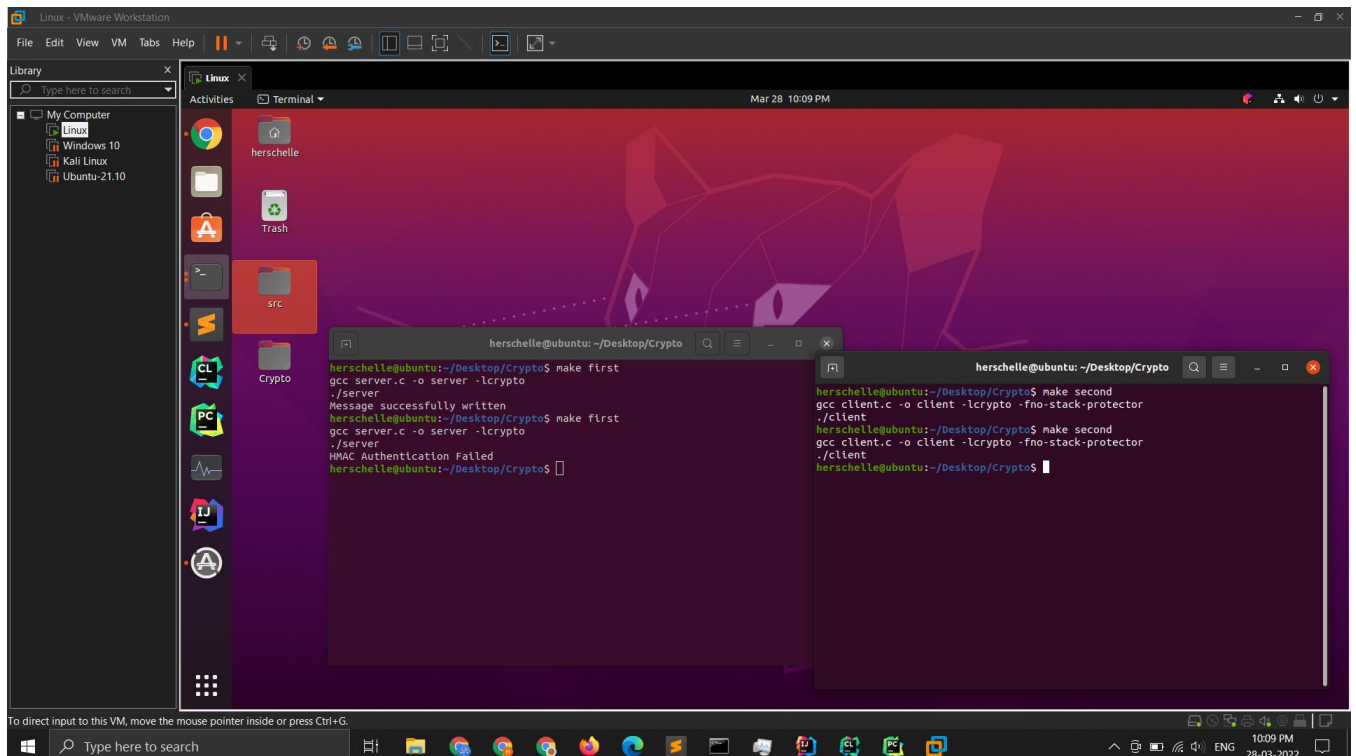
Now we load the netfilter module. Open another terminal in netfilter module directory. Type “make” to compile it and “make load” to load. Incase you already have a module loaded you need to unload it using “make unload” first then load.



```
herschelle@ubuntu: ~/Desktop/src
herschelle@ubuntu:~/Desktop/src$ make
make -C /lib/modules/5.13.0-35-generic/build M=/home/herschelle/Desktop/src modules
make[1]: Entering directory '/usr/src/linux-headers-5.13.0-35-generic'
CC [M] /home/herschelle/Desktop/src/packet_filter.o
MODPOST /home/herschelle/Desktop/src/module.symvers
CC [M] /home/herschelle/Desktop/src/packet_filter.mod.o
LD [M] /home/herschelle/Desktop/src/packet_filter.ko
BTF [M] /home/herschelle/Desktop/src/packet_filter.ko
Skipping BTF generation for /home/herschelle/Desktop/src/packet_filter.ko due to
unavailability of vmlinux
make[1]: Leaving directory '/usr/src/linux-headers-5.13.0-35-generic'
herschelle@ubuntu:~/Desktop/src$ make load
sudo lnmod packet_filter.ko
[sudo] password for herschelle:
herschelle@ubuntu:~/Desktop/src$
```

```
herschelle@ubuntu:~/Desktop/Crypto
herschelle@ubuntu:~/Desktop/Crypto$ make second
gcc client.c -o client -lcrypto -fno-stack-protector
./client
herschelle@ubuntu:~/Desktop/Crypto$
```

Now, we repeat the process and see that HMAC fails.



```
herschelle@ubuntu:~/Desktop/Crypto
herschelle@ubuntu:~/Desktop/Crypto$ make first
gcc server.c -o server -lcrypto
./server
Message successfully written
herschelle@ubuntu:~/Desktop/Crypto$ make first
gcc server.c -o server -lcrypto
./server
HMAC Authentication Failed
herschelle@ubuntu:~/Desktop/Crypto$
```

```
herschelle@ubuntu:~/Desktop/Crypto
herschelle@ubuntu:~/Desktop/Crypto$ make second
gcc client.c -o client -lcrypto -fno-stack-protector
./client
herschelle@ubuntu:~/Desktop/Crypto$ make second
gcc client.c -o client -lcrypto -fno-stack-protector
./client
herschelle@ubuntu:~/Desktop/Crypto$
```

For the netfilter module, all I did was increment the data offset by 1 (tcph->doff). This would change the data, resulting in HMAC authentication failure.

For more info loading netfilter module please refer to Assignment 1.

HMAC code is sent along with msg as msg + separator + hmac\_code. Then separated a the server in the same format.

Assumptions:

I have hard coded key and iv with simple text and placed in the code only. We could generate them reading bits /dev/urandom as mentioned in the question, but this works for testing. In a real-world application, we would store the key and iv safely and place them in environment variables and use them in the code instead.

I have used socket programming instead of netcat program.