README

cs21mtech12002_12005_12007.tar contains the following files & folders :

- Alice
  - alice-rsa.pem
  - alice.pem (alice.crt is changed to alice.pem)
  - ca_cert.pem
- Bob
  - bob-rsa.pem
  - bob.pem (bob.crt is changed to bob.pem)
  - ca_cert.pem
- Trudy
  - fakebob.pem
  - fakebob-rsa.pem
  - fakealice.pem
  - fakealice-rsa.pem
  - ca_cert.pem
  - arp_poison.py
- Root
  - ca_cert.pem
  - ca.pem
- Makefile
- Report
- Readme
- secure_chat_app.py
- secure_chat_interceptor.py
- pcaps
  - task2.pcap
  - task3.pcap
  - task4.pcap
  - bonus.pcap

Procedure

Moving code from local to containers:

1. Run '*make*' in the after extracting cs21mtech12002_12005_12007.tar. This will push all the folders from local to VM at ns@192.168.51.123.

```
supriya@supriya-HP-Laptop-15g-br0xx:~/cs21mtech12002_12005_12007$ make
scp Makefile ns@192.168.51.123:
Makefile                                      100% 1312   266.6KB/s   00:00
scp -r alice/ ns@192.168.51.123:
ca_cert.pem                                   100% 1021     7.8KB/s   00:00
alice-rsa.pem                                 100% 1708    22.1KB/s   00:00
alice.pem                                     100% 1090    34.0KB/s   00:00
alice.csr                                     100% 1216    28.0KB/s   00:00
scp -r bob/ ns@192.168.51.123:
ca_cert.pem                                   100% 1021    13.0KB/s   00:00
bob.pem                                       100% 1029    52.8KB/s   00:00
bob-rsa.pem                                   100% 1708   287.8KB/s   00:00
bob.csr                                       100%  972   215.5KB/s   00:00
scp -r Root/ ns@192.168.51.123:
ca_cert.pem                                   100% 1021    70.6KB/s   00:00
CA.pem                                        100%  361    38.7KB/s   00:00
scp -r trudy/ ns@192.168.51.123:
fakebob.pem                                   100% 1038   168.7KB/s   00:00
fakealice.pem                                 100% 1021   216.8KB/s   00:00
ca_cert.pem                                   100% 1021   229.8KB/s   00:00
attacker.py                                   100% 1433   329.5KB/s   00:00
fakebob-rsa.pem                               100% 1708   353.8KB/s   00:00
secure_chat_interceptor.py                    100%   10KB 362.7KB/s   00:00
CA.pem                                        100%  361     1.7KB/s   00:00
fakealice-rsa.pem                             100% 1704   349.2KB/s   00:00
scp secure_chat_app.py ns@192.168.51.123:
secure_chat_app.py                            100% 9592   817.3KB/s   00:00
scp secure_chat_interceptor.py ns@192.168.51.123:
secure_chat_interceptor.py                    100%   10KB 207.1KB/s   00:00
supriya@supriya-HP-Laptop-15g-br0xx:~/cs21mtech12002_12005_12007$
```

2. Then log in to VM using '*ssh ns@192.168.51.123*'.
3. Run '*make ns13*' . This will transfer all the above-mentioned folders to their respective containers.

```
ns@ns13:~$ make ns13
lxc file push -r alice/ alice1/../
lxc file push -r bob/ bob1/../
lxc file push -r trudy/ trudy1/../
lxc file push Root/ca_cert.pem alice1/../alice/
lxc file push Root/ca_cert.pem bob1/../bob/
lxc file push Root/ca_cert.pem trudy1/../trudy/
lxc file push secure_chat_app.py alice1/../alice/
lxc file push secure_chat_app.py bob1/../bob/
lxc file push secure_chat_interceptor.py trudy1/../trudy/
lxc file push Makefile alice1/../alice/
lxc file push Makefile bob1/../bob/
lxc file push Makefile trudy1/../trudy/
ns@ns13:~$
```

Task 2

1. Enter into Alice's container using '*lxc exec alice1 bash*'. To go to the code directory, run the command '*cd ../alice*'
2. Enter into Bob's container using '*lxc exec bob1 bash*'. To go to the code directory, run the command '*cd ..bob*'
3. Run '*python3 secure_chat_app -s*' in the bob1 container. This will start the program in server mode.
4. Run '*python3 secure_chat_interceptor -c bob1*' in alice1 container. This will start the program in client mode.
5. Enter the message at Bob/Alice's side to continue the conversation. Type CHAT_CLOSE at any end to end the conversation.

Task 3

1. Poison /etc/hosts file of Alice and Bob's containers using '*bash ~/poison-dns-alice1-bob1.sh*'.
2. Enter into Trud's container using 'lxc exec trudy1 bash'. To go to the code directory, run the command 'cd ../trudy'.
3. Remain in the same directory as stated above for Alice and Bob.
4. Run '*python3 secure_chat_app -s*' in the bob1 container. Then run '*python3 secure_chat_interceptor.py -d alice1 bob1*' in trudy1 container. Lastly, run *python3 secure_chat_app -c bob1*' in the alice1 container.

5. Continue the chat by sending messages from alice1 or bob1 container. These messages will be visible on trudy's container as well.
6. Type CHAT_CLOSE at Alice's or Bob's end to end the conversation.
7. Unpoison /etc/hosts using '*bash ~/unpoison-dns-alice1-bob1.sh*'.

Task 4

1. Poison /etc/hosts file of Alice and Bob's containers using 'bash ~/poison-dns-alice1-bob1.sh'.
2. Remain in the same folders as stated above for all three containers.
3. Run '*python3 secure_chat_app -s*' in the bob1 container. Then run '*python3 secure_chat_interceptor.py -m alice1 bob1*' in trudy1 container. Lastly, run *python3 secure_chat_app -c bob1*' in the alice1 container.
4. Continue the chat by sending messages from the alice1 or bob1 container. These messages will be visible on Trudy's container as well. Trudy can also change the messages from alice to bob. To check, send 'I love you' from Alice.
5. Type CHAT_CLOSE at Alice's or Bob's end to end the conversation.
6. Unpoison /etc/hosts using '*bash ~/unpoison-dns-alice1-bob1.sh*'.

Bonus-ARP Poisoning:

1. Enter into Trudy's container using '*lxc exec trudy1 bash*'. To go to the code directory, run the command '*cd ../trudy*'
2. Run the python code arp_poison.py using '*python3 arp_poison.py*'.
3. Enter the hostnames of the containers of bob & alice to start poisoning the ARP caches of alice & bob.
4. Run *secure_chat_interceptor.py* by opening another bash for trudy1 using step 1 for performing the attacks as mentioned in steps of Task3 & Task4.