CREDIT STATEMENT

Tejas Deshmukh(cs22mtech12005) :

Task 1 :

- ➢ Generated the CSRs of Alice(Client) and Bob(Server) and sent it to the CA to get it signed and verified the certificate.

Task 2 :

- ➢ Had a Discussion with Mahanth on the call flow(TCP, Initial Messages,TLS, Data transfer), how TLS is executed on socket programming, loading the certificates of Alice, Intermediate CA and Root CA in Alice and Bob, verifying the keys and certificates, establishing TLS connection.
- ➢ Coding of the runClient(<sv hostname>).
- ➢ Worked on how to use the gethostbyname() function.
- ➢ Collectively worked with Mahanth on merging the two functions while coding TLS and for Application data exchange between Client and Server.
- ➢ Captured PCAP traces of Alice and Bob's container, documented them and prepared a detailed report for task 2 with appropriate evidence.

Task 3 :

- ➢ Had a Discussion on call flow and how the downgrade attack could be carried out.
- ➢ Coded the initial part of downgrade.c++.
- ➢ Captured PCAP traces on Trudys' container, documented them and prepared a detailed report for task 3 with appropriate evidence.

Task 4 :

- ➢ Had a discussion on the call flow and what different things are to be implemented. Understood how the MITM attack is to be carried out.
- ➢ Coded the initial part of downgrade_task4.++.
- ➢ Helped in debugging the code.
- ➢ Captured PCAP traces on Alice, Bob and Trudys' container, documented them and prepared a detailed report for task 4 with appropriate evidence.

Created MakeFiles for all tasks.

Mahanth Kumar Valluri(cs22mtech11015) :

Task 1 :

- ➢ Generated Intermediate CA and Root CA Certificates. Also, signed the certificates of Alice and Bob and issued Certificates to them.

- Prepared the report with appropriate evidence of commands and the certificates.

Task 2 :

- Had a Discussion with Tejas on the call flow(TCP, Initial Messages,TLS, Data transfer), how TLS is executed on socket programming, loading the certificates of Alice, Intermediate CA and Root CA in Alice and Bob, verifying the keys and certificates, establishing TLS connection.
- Coding of the runServer() function.
- Coded the basic Socket structure for TCP.
- Collectively worked with Tejas on merging the two functions while coding TLS and for Application data exchange between Client and Server.

Task 3 :

- Had a Discussion on call flow and how the downgrade attack could be carried out.
- Completed the downgrade attack code.
- Did the Debugging of the Downgrade code.

Task 4 :

- Had a discussion on the call flow and what different things are to be implemented. Understood how the MITM attack is to be carried out.
- Completed the rest of the code and debugged the code for MITM Attack.
- Helped in completing the report.