CPSC 526 Assignment 2

Danny Tran - 30027536

Question 1

Test cases for question 1, starting with an empty passwords.txt file.

Test cases are to be done in order.

1. Testing enroll.py for: no password or username in enroll.py, returns is rejected.
2. Testing enroll.py for: no username with password and no password with username, both returns rejected.
3. Testing enroll.py for [word] password: username = danny, password = word, returns rejected.
4. Testing enroll.py for [num] password: username = danny, password = 1, returns rejected.
5. Testing enroll.py for [word+num] password: username = danny, password = word1, returns rejected.
6. Testing enroll.py for [num+word] password: username = danny, password = 1word, returns rejected.
7. Testing enroll.py for normal use: username = danny, password = sevenducks, returns accepted
8. Testing enroll.py for already existing username: username = danny, password = eightducks, returns rejected
9. Testing authenticate.py for normal use: username = danny, password = sevenducks, returns access granted
10. Testing authenticate.py with missing username or password: returns access denied

Question 2

1. The long-term secrets are, the key generated from Alice’s password, the key of the TGS, and the key of Bob.
2. The short-term secrets are, the session key between Alice and the TGS, and the session key between Bob and Alice.
   1. If the Alice’s key is leaked, the passive adversary could learn the session key between the TGS and Alice and address of the TGS.
   2. If the key of the TGS is leaked, the passive adversary could learn the session key between Alice and Bob.
   3. If the Bob’s key is leaked, the passive adversary could learn the session key between Alice and Bob.
   4. If the session key between Alice and the TGS is leaked, the passive adversary could learn the destination Alice is trying to connect to and when the key expires.
   5. If the session key between Alice and Bob is leaked, the passive adversary could learn the address of Alice, her user id and when the session expires.
3. Kerberos does not have forward secrecy because if one of the private keys is compromised, the session key of Alice and Bob is compromised. The only key needed to compromise Kerberos is Bobs key. This is because Alice sends Bob the session key encrypted with Bob’s key, so if an adversary has Bob’s key, they can get the session key between Alice and Bob.
4. We add a step after the TGS gets the session key between the TGS and Alice, that key gets sent to Bob. When the message with the session key between Alice and Bob is sent to Alice, it is encrypted with the session key between Alice and the TGS. Then when that message is forwarded to Bob, along with a message encrypted with the session key of Alice and Bob. Bob is able to decrypt the session key of Alice and Bob with the session key between Alice and the TGS. If either of Bob or Alice’s key is compromised, the adversary is unable to get Alice and Bob’s session key just from monitoring communications between Alice and Bob.