CSCD27 Assignment 2
Derek Lai
laihoche
999035020

1. See email

2. (a) i. Eve does not have enough information to decipher messages between Alice and Bob in the future
   ii. No the scheme is not secure against Mallory, she could modifiy $g \wedge a$ mod p or $g \wedge b$ mod p with values of her own. Alice and Bob would still be able to send and recieve messages between each other but Mallory would be able to read them

   (b) i. Yes, this will be secure enough against Eve despite her being able to see public keys. Public keys along is not enough for her to be able to decipher any messages
   ii. No, Mallory or Eve could insert his/her own public key instead of either Alice or Bob's key. In the event this happenes, his/her own private key would be able to decipher any further messages.

   (c) i. Yes, Eve cannot read the messages between Alice and Bob
   ii. Yes, if Mallory knew their public keys she still wouldn't be able to read messages or create her own.

   (d) i. Yes, Eve cannot read the messages between Alice and Bob
   ii. Yes, Mallory cannot do anything to messages between Alice and Bob
   iii. Yes, in the small chance that Mallory could brute force either Alice's or Bob's private keys in the previous case, he would be able to modify messages between Alice and Bob. This case she would have less than a day to brute force the key and she only would be able to modify messages for one day.

3. Refer to makwill1's submission

4. Refer to makwill1's submission

5.
```
2014-11-09 00:12:44,612 Sending header: content-type : application/
x-www-form-urlencoded
2014-11-09 00:12:44,612 POST Data (www.facebook.com):
lsd=AVq2omPV&email=fakeemail%40hotmail.ca&pass=fakepass&default_persi
stent=0&timezone=&lgnrnd=213321_-VDl&lgnjs=n&locale=en_US
```

   (a) SSL Stripping uses ARP Poision routing to fool a computer into routing traffic through the hackers machine. The user is presented with a view that which pretends to be an HTTPS Browser session but is

not, HTTP. Relying on the fact that no one types "https://" each time when browsing. If the user were to be redirected to an SSL enabled, https, the attacker would intervene and catch and redirect the connection. The attacker would be able to sniff the data then redirect the victims traffic towards the original destination. The HTTPS response from the web server is modified back to HTTP and redirected back to the user.

(b) Users should ensure the sites they browse on are browsing on are HTTPS versions of sites. This exploit targets the transition from non SSL to SSL enabled websites so by being on https in the first place avoids that transition.

(c) Sites can provide positive/visual clues to the user to inform the users that they are now on a SSL connection. Clues such at a yellow bar in the web address or a "lock" on the load bar at the bottom of the browser helps the user see that they are on a secure connection. SSL Stripping removes such cues.

(d) HSTS works by allowing web servers to impose a rule on web browsers so that they only communicate using a secure HTTPS connection and never with HTTP. If there were to be an unsecure http connection, HSTS would modify the request to https.

6. (a) A relatively simple ARP posioning attack against a single computer could involve sending an ARP reply associating the victim's router's IP address with a fake MAC address. In doing so, the victim's computer would believe it is sending packets to the router correctly but in reality it is sending packets to a fake MAC address. This way the victim is cut from the Internet on the en tired network. This is an example of Denial of Service.

(b) Malloy begins by sending Alice an ARP reply with an ip of B, associating it's MAC address m with B. Alice's computer now believes that Malloy's computer is Bob's computer. Then Malloy sends another ARP reply to Bob's computer with an ip of A. This associates MAC address m with IP A. When Alice tries to communicate with Bob, Alice sends traffic to Malloy thinking that it is sending it to Bob and Malloy forwards to message to Bob who thinks it is coming from Alice.

(c) One possible way to avoid ARP posioning is using static IPs on all devices and also a static ARP table. By using static IPs and static ARP table, hackers will be unable to add spoofed ARP entries by broadcasting a reply. The downside to this is that this would be impossible to maintain on a large network due to the vast amount of IPs and MAC addresses to maintain.

(d) MAC address spoofing is simple, so an attacker could broadcast many ARP replies using the victims router IP and many spoof MAC addresses. The tool should detect the rapid change and block the IP

address, which actually was the routers IP, closing off access to the Internet for the victim.

7. (a) No an attacker cannot achieve a DOS attack by flooding the server with ACK request. The server would receive the ACK request and respond to all ACK's with a SYN-ACK. Since the DOS uses fake ip addresses, the SYN-ACK is never received or dealt with, the server does nothing.

   (b) Yes, by reflecting SYN-cookie values or SYN-ACKs from the server, the server would acknowledge the attacker's earlier ACK request and open a connection with at the ip. Since the IP's are fake, they send nothing and the connection is kept alive and the server use's all its resources. This creates a DOS like situation.