CS419
homework 3

1. Network Packet Analysis
   a. HTTP traffic
      1. amazon.com
         bing.com
         google.com
      2. adventures in stochastic processes
         madison map in bing
         chicago metro in bing

   b. FTP traffic
      1. username: shiningmoon
         password : public
      2. In active FTP, the server connects to the client; in passive FTP the client connects to the server
         active ftp
            In active mode FTP the client connects from a random unprivileged port (N > 1023) to the FTP server's command port. Then, the client starts listening and sends the FTP command to the FTP server. The server will then connect back to the client's specified data port from its local data port
         passive ftp
            In order to resolve the issue of the server initiating the connection to the client a different method for FTP connections was developed. This was known as passive mode
      3. there are no active connections
      4. 30-46
         75-99
         110-126
         146-176
         180-200
         217-233

243-263

5. L2Switch.java
   ARP.java
   dragon.zip

c. Traceroute (ICMP)
   1. 192.168.0.1
   2. 74.125.255.46
   3. 192.168.0.100
      10.131.180.1
      96.34.20.20
      96.34.17.95
      96.34.16.112
      96.34.16.77
      96.34.2.4
      96.34.0.7
      96.34.0.9
      96.34.3.9
      96.34.152.30
      209.85.254.120
      209.85.254.28
      74.125.225.46

d. POP
   1. user: cs155@dummymail.com
      password: whitehat
   2. 5
   3. date: fri 23 apr 2010 08:20:52
      Subject: foobar
      from: cs155@dummymail.com
      to: cs155@dummymail.com

      date: fri 23 apr 2010 08:23:25
      Subject: can you see this subject?
      from: cs155@dummymail.com
      to: cs155@dummymail.com

date: fri 23 apr 2010 10:25:00
Subject: test message
from: harinym@stanford.edu
to: cs155@dummymail.com

date: fri 23 apr 2010 08:22:28
subject: geogology rocks
from: harinym@stanford.edu
to: cs155@dummymail.com

date: fri 23 apr 2010 08:21:51
Subject: wassup
from: harinym@stanford.edu
to: cs155@dummymail.com

2. Network-based Denial-of-Service

by reading the live packets and storing them to a file there could be a lot of things wrong happening to this proposal
such as

A.

-attackers can do DDOS attack with a large botnet

-buffer overflow, -length of buffer is according to packet ,and it can be specified by sender, & the sender can be malicious or errbuff could be overwritten
-format string vulnerability , write something else instead of what the program asks for
-change privilege in fopen
-forge position of payload

B.

-after finding out youre under attack start ignoring connections from certain IPs

-create packets that counter a buffer overflow
-canaries, or encrypt addresses

4. SSL
    a. there are certificates which don't let this happen because of signatures from CA
    b. encryption in SSL does not let passwords or any raw data to be sniffed
    c. there exist a private key and public key in SSL so this cant be done
    d. IP hijacking cant be done because of SSL session keys
    e. cannot be dealt by SSL but can be done with SYN cookie
    f. nonces prevent replay attacks
    g. longer bits (length), larger key space so they cant use brute force

5. Web Security
    a.
        a website that is vulnerable to XSS can be compromised by an attacker to steal web cookies by forcing a target's browser to issue some sort of GET request to a server controlled by the attacker which accepts the target's cookie as a parameter and processes it in some way
        cookie stealing is when you insert a script into the page so that everyone that views the modified page inadvertently sends you their session cookie
    b.
        exploits the trust a site has in a user's browser. Include a link or script in a page that accesses a site to which the user is known to have authenticated.
        the link or script can reference an action on user's bank account , if the bank keeps authentication information in a cookie (can also query passwords and such information)and hasn't expired
        Solution: same origin policy,additional authentication(
                repeat user authentication before security critical operation), or CAPTCHA

c. -XSRF is an example of a confused deputy attack because it uses a web browser to perform sensitive actions against a web application
   -the confused deputy in the bank example is the user's web browser which is confused into missing the user's authority at the attacker's direction
   -the principles on behalf of which the deputy acts is the user
d. for the additional authentication , it gives all entities all and only the capabilities they will actually need and thats what a capability based solution is
e. because the setuid binaries can be exploited using a shell script or by providing false data and an attacker can get permission to run programs (temporary elevated privileges). confuses system that it has permissions when it really doesn't