Komail Dharsee

QUESTION 1:
Part (a):
1.
205.251.242.54 Amazon.com
173.194.46.70 Google.com
31.13.69.80 Facebook.com
198.105.254.25 Bing.com
180.76.3.151 Baidu.com

2.
Bing: Madison Map
Bing: Chicago Metro
Amazon: adventures in Stochastic Processes

Part (b):
1. username: shiningmoon, password: public

2. In a passive FTP connection, the client is the one initiates the data channel and the command channel. The data channel is initiated based on the response from the server regarding the port number to connect to. In an active FTP connection the client only initiates the command channel, after which the server responds and initiates the data channel. The server connects to the client's specified port for the data channel.

3. Could not find any active connections.

4. Ranges: 30-46, 75-99, 110-126, 180-200, 217-233, 243-263

5.
phase1.html
L2Switch.java
ARP.java
dragon.zip

Part (c):
1. 192.168.0.100

2. 74.125.225.46

3. 192.168.0.100
192.168.0.1
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
209.85.250.28
74.125.225.46

Part (d):
1.
username: cs115@dummymail.com
password: whitehat

2. 5 messages

3.

	Message 1	Message 2	Message 3	Message 4	Message 5
From	cs115@dummymail.com	harinym@stanford.edu	harinym@stanford.edu	cs115@dummymail.com	harinym@stanford.edu
To	cs115@dummymail.com	cs115@dummymail.com	cs115@dummymail.com	cs115@dummymail.com	cs115@dummymail.com
Subject	foobar	wassup	geology rocks!	can you see this subject?	test message
Date	Fri, 23 Apr 2010 08:20:55	Fri, 23 Apr 2010 08:21:50	Fri, 23 Apr 2010 08:22:28	Fri, 23 Apr 2010 08:23:35	Fri, 23 Apr 2010 10:25:00

QUESTION 2:
Part (a):

1. Attackers can perform a Distributed Denial of service attack with a large botnet \

Part(b):

1. implement a blacklisting policy to ignore connections from an ip after a period suspicious traffic.

QUESTION 4:
Part(a):
SSL provides a layer of security allowing parties to communicate with certification with the help of signatures from certification authorities.
Part(b):
SSL encrypts the data allowing secure communication against sniffing of raw sensitive information.
Part(c):
SSL is not attached to specific IP addresses. SSL does not counter this.
Part(d):
With the use of session keys in data encryption, it is difficult for attackers to perform IP Hijacking.
Part(e):
Not countered by SSL

Part(f):
Nonces are incorporated to help prevent replay attacks.
Part(g):
SSL has a large key space with 128 bit keys. The large key space increases the amount of time of dictionary and brute force attacks substantially for success.

QUESTION 5:
Part(a):
Attackers can inject malicious code on the website taking advantage of vulnerabilities like in forms. Users can fall victim by accessing parts of the website with scripts that get invoked by reading comments or filling forms. Attackers may retrieve cookie information this way.

Part(b):
This is where an attacker may take advantage of trusted users on a websites with sensitive information (banking, shopping...). Links may be created by an attacker to perform actions on a currently authenticated user accounts with active cookies to query passwords and other sensitive information. Prevention techniques can include complete mediation in that users will have to authenticate themselves for any request to perform sensitive tasks (like when dealing with money).

Part(c):

I. This attack fools the web service into thinking that the user wanted to perform an action since the user was logged in and opened up a query to perform that action. The web service is doing what it is told without malicious intent, but to the benefit of the attacker.
II. The web service
III. on behalf of the user

Part(d):
It first has the web service uses its capability to check the identity of the user by requesting credentials before performing the actions.

Part(e):
These are setuid programs are vulnerable to being compromised and allowing attackers to run programs and execute code on behalf of the user, while the setuid program is doing what it's told without malicious intent.