John F. Lake, Jr.
CSE 30264
Homework #10

Chapter 8:

17)

a) PuTTY utilizes RSA encryption to handle new servers. When connecting to a new server, PuTTY saves the host public key from the server, and after that point when PuTTY connects to the same server it will compare the public key to the one saved from the first connection. If you are using PuTTY on a server you haven't been to before, you need to utilize a password.

b) After creating a public/private key combination, the client lets the server know what the public key is. Every login after that point, the server will utilize the client's private key for authentication.

c) The client and server need to agree on the type of encryption. In the ssh config file, the server and client can both specify a cipher. If they don't match, a default one is used.

d) Some servers may only have the capability to utilize more rudimentary encryption algorithms. PuTTY utilizes a "warning threshold," which is set by the user, to determine if a cipher is weak or not. PuTTY will inform the user if the server's first cipher method is weak, and the user can decide to connect or not.

e) If a session runs for too long on a specific key, it can become vulnerable to attacks. Because of this, changing the key periodically helps make the connection more secure and protected from threats.

18)

a) Because the telnet uses ports above 1023 for receiving messages back from the server, we cannot block whatever port is chosen for this service. If we do, the outgoing connection will never receive any response from the server.

b) You could have the firewall look at the flags for the ACK bit. If it is set, have the firewall send a UDP message to the client letting them know that the server has received their message. You could also just have the firewall translate the TCP message into UDP.

19)

a) The PORT command works by giving a port number and an IP address for the server to use on the next data transfer. This can be limited to one port, so it is possible for the firewall to block all inbound ports but the one used by the PORT command for future file transfers.

b) PASV is like the PORT command, only it's server side. This command allows the client to know exactly what port to use, so the need for a firewall to direct the traffic is reduced.

Chapter 9:
14)

a) When a client sends a GET request, you can use the HTTP result code of redirection to point the user to the correct server that is closest. Essentially, the client will send a request, and the initial server will reply with a 301 result code telling the client to go to that location.

b) To use DNS in this process, the HTTP request can go through the same way, but the DNS service will take the specific URL supplied and will determine where the closest server with that URL is to give a response.

The DNS one is probably the easier of the two to utilize. You wouldn't need to upgrade the browser, as the DNS service would take care of the rerouting, rather than the browser itself.

22)

ARP doesn't need a very long timeout because it is used for very temporary connections that are going to change quickly. DNS can justify a longer timeout because URL locations won't change as often. If the DNS cache had a longer timeout, it could be possible that a website moved locations but wasn't updated in the cache, so a client would not be able to properly access it.