CS 177 Homework 6

1) Since the IP address we have access to from the outside is a broadcast IP address, we can magnify our resources to include the machines in the subnet as a form of “botnet.” The more machines in the subnet, the more powerful our denial of service attack is because more messages will be sent due to there being more machines on the subnet. In order to complete a successful denial of service attack, as attackers we need to have more resources than the target. We can achieve this by combining the computing power of the machines in the subnet. To attack our target, we will need to spoof our source IP address. This will allow us to send packets as if we were the target’s machine. By sending a ping request to the broadcast IP address, we will effectively ping all the machines on the subnet. Since the machines on the vulnerable subnet think the spoofed packet they are receiving is coming from the target, they will send their long responses to the target, effectively overwhelming the targets resources, and denying them service.
2) With the setup described in Task 2, there are multiple safeguards against SYN flooding attacks. The first deterrent is the time counter. Since the counter is mod 32 to fit into five bits, the server could implement an efficient timeout system that drops ACKs that are too out of date. This can be determined by finding the difference between the current time and the packet’s time. In addition to a timeout system, the server implements a message authentication code that stores the IP address, port number, time, and maximum memory for each connection. This protects against SYN flooding because all the necessary information to start a TCP connection is stored in the sequence number. Since the MAC will not be able to be computed without the secret key, which only the server has, attackers will not be able to forge valid ACK packets that would start fake connections. The server will drop packets with invalid MACs when they are received, and not start up a connection, which will prevent memory waste. The only way a connection can be started is if there is an ACK with a sequence number one greater than the SYN/ACK sequence number, the corresponding MAC of this subtracted (SYN-ACK) sequence number is valid (mac recomputed with server’s secret key and compared), and the timer is close enough to have not timed out. This will nullify IP spoofing because if a SYN-ACK packet is sent to a spoofed IP, the spoofed IP will not respond, the connection will not be started, and no memory will be used by the server. This method is not perfect though. If the attacker has control of a botnet, they could create a very large number of legitimate TCP connections from each of the machines in the botnet, which would use up a lot of memory on the server. However, this would not be a SYN flood attack anymore.
3)
   A) The server mitigates the effects of SYN flood attacks because the table T has a fixed number of cells, meaning the cells could never use up the entirety of the system’s memory.

B) The disadvantage of this method is that if enough SYN requests to fill all 2^16 cells of the table are sent to the server as part of the SYN flood attack between the time the server sends a SYN-ACK request to the legitimate client and the time the server receives a legitimate ACK from the legitimate client, then the client's entry in the table will be overwritten. This means that the server will think that the legitimate client's legitimate request is not legitimate, because there is no previous entry for that client's request, as it has been overwritten.

4) There are a couple problems with the NTP protocol. The information about the 600 previous addresses that get returned is actually quite a lot of data (megabytes). A possible attack would be to send packets with a spoofed IP address to this time server which would overwhelm the targeted (spoofed) IP address with data that would cripple the system. In addition to performing these denial of service attacks, the network time protocol would give out a list of 600 legitimate IP addresses that attackers could possibly target.

5)

A)
```
22/tcp open  ssh
80/tcp open  http
```
Port 80 (http) and Port 22 (ssh) are the only two ports open out of all 65,535 ports.

B) The server runs ssh version 2, and http version 2.4.18. The ssh version can be found by searching the /etc/ssh/sshd_config file to find the protocol number. Both the ssh and http versions can be found using the -sV flag when running the nmap command.

C)

1) An example of a scenario when this suggestion is useful is when someone is doing a large, shallow scan of network ports to abuse very insecure machines to create a botnet. The attacker probable would not check all ports for the sake of time and the scale of the attack.

2) An example of a scenario when this suggestion is not useful is if an attacker is specifically targeting John. This is because ports above 1024 do not require root privileges to listen on. Also, if an attacker was specifically targeting John, they would be able to figure out that the ssh port had changed by doing a port scan. The resulting insecurity of the passwords John has chosen will make brute forcing Johns passwords easier than normal, leaving John very vulnerable.