ITIS 6200/8200 Principles of Information Security and Privacy

Homework 4

Please **briefly** explain your answer.

**Question 1. ARP Attack (15 points)**

ARP, the Address Resolution Protocol, translates Layer 3 IP addresses into Layer 2 MAC addresses. Assume that Alice wants to communicate with Bob, whose computer is on the same LAN network. Alice knows Bob’s IP address but wants to learn his MAC address.

An attacker, Mallory, wants to convince Alice that your MAC address (and not Bob’s) corresponds to Bob’s IP address, causing messages intended for Bob to be sent to you instead. Mallory, Alice, and Bob are part of the same LAN network. Assume that Mallory computer has IP address 1.2.3.4 and Mallory’s MAC address is 66:66:66:66:66:66, Alice’s IP address is 1.2.3.77 and her MAC address is 77:77:77:77:77:77, and Bob’s IP address is 1.2.3.8 and his MAC address is 88:88:88:88:88:88. The network LAN router’s IP address is 1.2.3.5.

Q 1.1: Alice broadcasts to everyone else on the LAN: “What is the MAC address of 1.2.3.8 (Bob)?" What values for the IP and MAC address can Mallory include in her response to Alice to cause her messages intended for Bob to be sent to you instead?

Q 1.2: How would your spoofed response to Alice change if Bob was outside the LAN that Mallory and Alice are both part of?

Q 1.3: A network switch is deployed to prevent further ARP spoof attacks. What would the switch do in the following two cases: (1) the switch knows Bob’s IP to MAC address mapping and (2) the switch does not know Bob’s IP to MAC address mapping. Explain in one sentence why that helps with ARP spoof attacks.

**Question 2. TCP Spoofing (25 points)**

The left diagram below shows how TCP handshake works. The right diagram some initial data have been transferred between the Client and the Server.



***TCP handshake*** ***Initial data transfer after handshake***

Q 2.1: Assume that the next transmission will be some data sent from Client to Server. What are the sequence number and ACK for this packet?

Q 2.2: Consider a on-path attacker Eve who can observe the traffic but cannot modify it. Can Eve hijack the TCP connection between the Client and the Server? What can she do?

Q 2.3: Consider a off-path attacker David who cannot observe and modify the traffic. Can David do anything malicious to the connection? If so, what can he do?

Q 2.4: The Client wants to send a message M to the Server. Consider a modified version of TCP where the Server no longer sends an ACK to the Client for messages the Server receives. If the client sends a message M using this modified version of TCP and M was dropped during delivery, can the Server know that M is lost? Would the message M be resent by the client?

Q 2.5: The Client wants to send a message M to the Server. Consider a modified version of TCP where the Client no longer sends an ACK to the Server for messages the Client receives. If the client sends a message M using this modified version of TCP and M was dropped during delivery, can the Server know that M is lost? Would the message M be resent by the Client?

**Question 3. Denial of Service Attack and Firewalls (20 points)**

SYN flooding attack is a DoS attack that attacks a server by sending a large amount of SYN requests to the server.

Q 3.1: Explain in two sentences how this DoS attack works. (What resources are being consumed at the server?)

Q 3.2: The server wants to defend against SYN flooding attack by SYN cookies: it encodes the state needed for each SYN request as the sequence number of the SYN-ACK message sent back from the server. Assume the server needs to track the following information for each SYN request: (a) Source IP, (b) Source Port, (c) Destination IP, and (d) Destination Port. Design a scheme to generate a sequence number from the information. Explain how to validate the connection if with such a sequence number.

Q 3.3: Assume we want to use stateful packet filter to help with SYN flooding. Write a rule that allows inbound connections to IP address 1.2.3.4 with port 8080.

Q 3.4: Reconsider Q 3.2 about encoding the state needed for a SYN request with a sequence number. Can you design a scheme that generates sequence numbers that helps with packet filtering? In particular, the sequence numbers can help

**Question 4. Intrusion Detection (25 points)**

Q 4.1: Explain the difference between specification-based detection and anomaly-based detection.

Q 4.2: When the script **hack.js** runs, what origin does it has?

Q 4.3: Can we use XSS to steal information in Cookies? If yes, how can we defend against that?

Q 4.4: Design a GET request that can launch a CSRF attack shown in Question 3, i.e., a CSRF attack to *bank.com* than can transfer $1000 to Mallory.

**Question 5. Memory Vulnerability (20 points)**

A

Q 5.1: Design an