Homework 2: Network Security

This homework is due **Tuesday, October 10** at **10 p.m.**. You will have a budget of five late days (24-hour periods) over the course of the semester that you can use to turn assignments in late without penalty and without needing to ask for an extension. You may use a maximum of two late days per assignment. Once your late days are used up, extensions will only be granted in extraordinary circumstances.

We encourage you to discuss the problems and your general approach with other students in the class. However, the answers you turn in must be your own original work, and you must adhere to the Code of Academic Integrity. Solutions should be submitted electronically via Canvas in plain text format by completing the template at the end of this document.

Concisely answer the following questions.

1. **Network Exploration.** The `traceroute` tool can be used to explore networks and debug network problems.

   (a) On a Unix-based system, type `man traceroute`, read about how it works, and then describe how traceroute works in your own words.

   (b) Run `traceroute` with a popular website hostname of your choosing and paste the output below.

   (c) Sometimes traceroute seems to show a placeholder for what looks like an intermediate hop without any more information. Find a hostname where `traceroute` from your current location does not give information on some intermediate hops and paste the output below. Why might this be happening?

   (d) Read the `man` entry for the `ping` command and find the option to set the TTL (time to live) field in the IP header. Set it larger than the number of hops to the host you chose in part (b) above and paste what happens. Set it smaller than the number of hops to this host and paste what happens. What is happening?

2. **TCP Handshake Forgery.** The original functional specification for the TCP protocol, RFC ("Request for Comments") 793, specified that hosts should choose the initial sequence numbers for a new TCP connection based on the clock value at the time of connection, and incremented every 4μs. Common Berkeley implementations once simplified this to incrementing by 250,000 (or 256,000) once per second.

   (a) Given this simplified increment-once-per-second implementation, explain how an attacker Mallory could trick another host Alice into believing she has opened a TCP

connection with a third host, Bob. Assume that Mallory is not positioned to see traffic between Alice and Bob, and that Bob does not respond to SYN+ACK packets that Alice is tricked into sending him.

(b) Assuming that the real round-trip travel (RTT) time can be estimated to within 40 ms, about how many tries would you expect Mallory to take to trick Alice into believing she has opened a TCP connection with Bob using the strategy of part (a) with the unsimplified "increment every 4 μs" TCP implementation?

(c) What countermeasure do modern TCP implementations take against this attack? About how much work would you expect Mallory to do in order to trick Alice into believing she has opened a TCP connection with Bob if both Alice and Bob have implemented this countermeasure?

(d) Let Eve be an attacker who is able to eavesdrop on connections between Alice and Bob. Does the countermeasure you described in part (c) protect against Eve tricking Alice into believing she has opened a connection with Bob? If so, describe why; if not, describe how Eve can carry out such an attack.

3. **Internet Censorship and Circumvention.** The Great Firewall of China is a set of technologies that mainland China uses to block access to parts of the internet to their citizens. Monitoring systems are placed at gateways connecting internal traffic to the rest of the internet. These monitoring systems then examine traffic and block or censor unwanted connections.

(a) One method that can be used to block traffic is using the DNS protocol. Briefly describe how the Great Firewall of China could build a system to block access to selected hosts on the internet using DNS, while letting all other traffic through.

(b) How could someone in China circumvent your DNS-based blocking system to get to a host on the internet?

(c) Describe one way that the Great Firewall could block your circumvention attempt in part (b).

(d) Another method that the Great Firewall uses to block traffic is using TCP resets. Assuming that the firewall can monitor all traffic that passes through the gateway, describe how it could block traffic using a TCP reset.

Submission Template

Submit your homework to Canvas as a plain text submission.

```
# Problem 1:

  1a.

  1b.

  1c.

  1d.

# Problem 2:

  2a.

  2b.

  2c.

  2d.

  # Problem 3:

  3a.

  3b.

  3c.

  3d.
```