Computer Security Fall 2023
Network Security Homework

Srdjan Matic, Juan Caballero
IMDEA Software Institute

Guidelines

This homework is due by **Thursday, November 16, 2023 23:59:59 GMT+1**.

Please send your solutions in PDF format to `srdjan.matic@imdea.org`.

No collaboration is permitted on this assignment. Any cheating (e.g., submitting another person's work as your own, or permitting your work to be copied) will automatically result in a failing grade.

Problem 1: Initial Sequence Number Guessing *(14 points)*

Which of the following ISN selection methods used by a server are secure? If you believe that a method is not secure, explain the reason.

a. The server uses as ISN a constant value selected at random at boot time. *(2 points)*

d. The server generates its ISNs by using the 32 least significant bits of a known secure hashing (i.e., SHA256) calculated over a constant value selected at random at boot time. *(2 points)*

c. The server chooses a random ISN for each connection. *(2 points)*

d. The server generates its ISNs by performing a XOR among the following four variables: source IP, source port, destination IP, destination port. *(2 points)*

e. The server generates its ISNs by using the 32 least significant bits of a known secure hashing (i.e., SHA256) calculated over the concatenation of the following four variables: source IP, source port, destination IP, destination port. *(2 points)*

f. The server generates its ISNs by performing a XOR among the following five variables: source IP, source port, destination IP, destination port, current time. *(2 points)*

g. The server generates its ISNs by performing a XOR among client ISN and a random value selected at boot. *(2 points)*

Problem 2: SYN Flooding *(18 points)*

SYN Cookies and Client Puzzles are two techniques developed for defending against SYN flooding attacks.

1. Describe the idea behind SYN cookies. *(4 points)*
2. Describe the idea behind client puzzles. *(3 points).*
3. Flooding of a target can be performed in multiple ways: (a) packets can be sent from the IP address of the attacker, (b) the attacker can spoof the source of each packet, or (c) the attacker might leverage a large network of compromised machines (i.e., a botnet) to send packets. Explain in which of those three scenarios SYN cookies and client puzzles are an effective solution against flooding attacks. *(3 points)*
4. Can UDP be affected by a similar attack? *(2 points)*
5. What would be the problem if the attacker manages to guess the value of the SYN cookie or the solution to a client puzzle? *(2 points)* Can you think of any network scenario where this would happen? *(2 points)*
6. Are SYN cookies and client puzzles useful also in presence of *link flooding*? *(2 points)*

Problem 3: Scanning *(10 points)*

A security researcher has identified the IP address of a command-and-control (C&C) server and wants to gather information about the botnet controlled through this server. To this end, the researcher performs a scan of the services running on the server. After sending several probes, the researcher observes a "RST" packet being returned from port 194.

1. Which protocol typically runs on port 194? *(2 points)*
2. Which transport layer protocol did the research use in his probe packet to trigger this response? *(2 points)*
3. What can the researcher infer about the port status? Is the port "open", "closed" or "filtered" (i.e. , is the server is behind a firewall)? *(6 points)*

Problem 4: Denial-of-Service Amplification *(18 points)*

1. Describe one *network layer* amplification attack that we discussed in the class. *(4 points)*

2. Describe two reflector attacks with amplification that do not use the DNS or the NTP protocol. Detail (*i*) all the involved parties, (*ii*) the type of requests and responses sent by each party, and (*iii*) the packet amplification and bandwidth amplification factors achieved by the attacker. *(14 points)*
   (*Hint*: There are several attacks in the NDSS'14 paper by Rossow, but I want you to provide the details of the requests involved.)

Problem 5: HTTPS *(12 points)*

A security researcher executes a piece of malware inside a Virtual Machine (VM) to study its network communication. The malware uses HTTPS to communicate with a remote command-and-control (C&C) server.

1. Since the C&C communication uses HTTPS, can the researcher recover the domain name and the IP address of the C&C server by monitoring the traffic that the malware generates? Justify your answer. *(4 points)*

2. Explain how the researcher could set up a Man-in-The-Middle HTTPS proxy to decrypt and log the communication between the malware running in the VM and the C&C server. *(4 points)*

3. Explain how the malware developer could protect against such MiTM interception. *(4 points)*

Problem 6: Certificates *(28 points)*

Check the HTTPS certificate for `https://software.imdea.org` and answer the following questions. For each question, you need to provide a textual answer and a screenshot where the answer is visible.

1. How many certificates are there in the certificate chain? *(3 points)*

2. What is the name of the Certification Authority that produced the leaf certificate? *(3 points)*

3. What is the organization name of the Certification Authority that produced the root certificate in the trusted store? *(3 points)*

4. What is the validity period of the intermediate certificate? *(3 points)*

5. How many domains (*i.e., fully qualified domain names*) is the leaf certificate valid for? List the domains alphabetically *(4 points)*

6. What hash algorithm is used by the intermediate certificate? *(3 points)*

7. For the leaf certificate, what are the URLs of the OCSP server and the certificate revocation list (CRL)? *(3 points)*

8. Download the certificate revocation list from the above URL. How many revoked certificates are there in the file? Note that how to view the contents of the CRL file varies depending on your OS and could require you to install a tool. Please provide the command used and the human-readable content of the CRL file in the answer. *(6 points)*