Name: Anthony Redamontt Section: 01

CSE 644 – Network Security

Final Exam

Monday, March 27, 2023

Instructions:

- Electronic devices are NOT allowed.
- The maximum number of points is 100, as indicated.
- Please answer questions in the spaces provided; if space is insufficient, please use the back of the pages.

#1 (20)	**#2** *(20)*	**#3** *(20)*	**#4** (20)	**#5(20)**	**Total** *(100)*

Q1 [20 points]

a) What is DNS cache poisoning attack? What are the fundamental problems of the DNS protocol that makes DNS vulnerable to DNS cache poisoning attacks?

b) When a DNS reply is received by a local server, what are the four parts of the reply. Which of these parts will be cached and which will not be cached?

a) a DNS cache poisoning attack is when an attacker sends a spoofed reply ~~to~~ the DNS server acting as the root authority. The spoofed message will contain the attacker's domain as an authority of the server in the query. The attacker specifies how long the entry stays in the DNS cache. Whenever a client requests the authority of a specific domain, the DNS server will provide the attacker's domain. The attacker could also spoof the client's DNS query directly, but this would only poison the DNS cache of the client (not the DNS server). The fundamental problem with DNS is that it is a UDP packet ~~ut~~ wrapped in an IP packet, so it is a connectionless protocol.

b) ~~Cert~~ ① Certificate Authority IP / ② Port Number

CA

~~Certific~~ Root IP / Port Number

~~ADDit~~ ③ ④

There is also an additional section for other trusted authorities of the domain are listed.

The certificate authority (CA) and additional section will be cached. The root authority information will not be cached.

Q2 [20 points]

a) If a CA's private key is stolen by an attacker, what damages can the attacker achieve?

b) Before issuing the certificate, the CA needs to do a verification regarding the subject field. Please describe what this verification is, and why it is necessary

a) The attacker can then generate their own self-signed certificate and become a root CA!! (NOT GOOD!) Then they can generate legal certificates for their malicious domains!

b) The certificate authority needs to verify that the domain name is truely the owner of the certificate. ~~It will use the certificate in combination with a passed key to verify ask~~

CA ~~It~~ will ask the root authority if the domain name is owner of certificate. Root server will verify legitimacy of certificate ownership.

Q3 [20 points]

a) A program wants to send many pieces of data to a server, each piece will be sent via a separate call. The server needs to know the boundaries among these pieces. (1) If the program uses UDP, how does the server know where the boundaries are? (2) What if the program uses TCP?

b) Explain what is an SYN flooding attack. Can we launch an SYN flooding attack from a computer without using the root privilege? Why or why not?

a) UDP has a length field and a checksum to calculate the boundaries between packets. TCP/IP has a sequence number and an offsets (used for IP fragmentation) to determine the boundaries.

b) a SYN flooding attack is when an attacker initiates a TCP/IP handshake with the victim but has no intension of completing the connection (doesn't send SYN+ACK). The attacker keeps sending SYN message after SYN message until the victim's half-open connection queue is full. The victim will not be able to accepts any new connections (Denial-of-service attack).

We must use root privelege to open a RAW socket. Then the attacker can write custom fields in the spoofed TCP/IP packet. OS will not tamper or modify with packets.

Q4 [20 points]

a) What is a TCP Reset attack. Is it effective against encrypted connections like SSH. Is UDP connection subject to Reset attacks.

b) What is a TCP session highjacking attack. Will it succeed against an SSH connection

a) A TCP/IP reset attack is when the attacker spoofs a TCP/IP packet with the ~~correct~~ RST bit set and correct destination port number and sequence number. The victim will close their side of the connection, leaving the other end (hanging up on other machine). If the data in the connection is encrypted, the RST ~~attack~~ would still work because the RST bit is contained in the header of the TCP packets. (not encrypted). ~~It~~ UDP is not subject to reset attacks because it is a connectionless protocol.

b) TCP/IP session hijacking attack is when the attacker injects ~~on~~ a TCP packet with the correct sequence number(+1) and destination port/IP. The victim will be kicked out of the connection because they are using an incorrect sequence ~~sub~~ number. Yes, it can still succeed against the SSH connection. The header is not encrypted.

Q5 [20 points]

a) A developer writes the following in a post: "I am writing a login for a forum, and I would like to hash the password at the client side in JavaScript before sending it to the server. If the hash matches with the one stored on the server, the user will be allowed to log in." The developer believes that by sending the hash of the password, instead of sending the password directly, can improve the security. Do you agree or not, why?

b) Why is the hash function f(x) = x mod 10000 not a good one-way hash function?

a) Yes, sending the hash is more secure because there is no way ~~to~~ to decrypt a hash value. Typically, clients will send encrypted hash values for even more security. Hash values are also unique (collision-free).

b) Because there would be many collisions!

$f(1) = 1 \bmod 10000 = 1$

$f(10{,}001) = 10{,}001 \bmod 10000 = 1$

Hash functions must produce unique values.