ISA562-Homework-3

Srilatha Maddineni

G01421250

1.A DNS Poisoning:

DNS Poisoning, also known as DNS cache poisoning, is an attack where a malicious party manipulates the DNS cache of a DNS server to redirect the traffic to a malicious website or to intercept sensitive information. DNS is critical service in the system which translates the human readable domain names into the corresponding numerical IP addresses which can be used by computers to communicate over network.

Example:

Normal DNS Resolution: When a client wants to visit the website named 'www.fictional.com', it sends a DNS query to its DNS server asking for IP address associated with 'www.fictional.com'.

Legitimate DNS Response:

- The DNS server checks it cache and if it did not have the IP address for 'www.fictional.com', It forwards the query to authoritative DNS server which is responsible for the 'fictional.com' domain.
- The authoritative DNS server replies with the legitimate IP address of 'www.fictional.com'
- Now, the DNS server caches the response and sends back to the client.
- As the client knows the IP address, it connects to the IP address to access the website.

Malicious DNS Response:(DNS Poisoning)

- An attacker is trying to conduct a DNS poisoning attack. He sends a fake DNS response to the DNS server, claiming to be the authoritative server for example.com.
- In this fake response, the attacker provides a malicious IP address (203.0.113.1) instead of the legitimate one.
- DNS server caches this malicious IP address and sends it back to the client.
- Now, the client connects to this malicious IP address to access the website which leads to a fake site created by the attacker.
- As a result, attackers can carry out various malicious activities such as accessing login credentials.

OSI Layer: DNS Poisoning targets the Application layer which is layer 7 of the OSI model
Mitigation:

- **DNSSEC (DNS Security Extensions):** Implement DNSSEC to provide cryptographic authentication of DNS data, ensuring the integrity of DNS responses.

- **Cache Expiration and Refreshing:** Regularly flush or refresh the DNS cache to remove poisoned entries and replace them with accurate information.
- **Regular Security Audits and Updates:** Review and update security configurations and keep DNS servers patched and up to date to protect against vulnerabilities.

B. Syn Flood: A SYN flood attack is a type of denial-of-service (DoS) attack where an attacker sends a large number of TCP connection requests with forged source IP addresses, overwhelming the target server's resources and causing it to become unresponsive to legitimate requests. Specifically, it targets the three-way handshake process used by the Transmission Control Protocol (TCP) to establish a connection between a client and a server.

OSI Layer: Syn Flood attack targets the Transport Layer of the OSI model.

Mitigation:

- **SYN Cookies:** Enable SYN cookies on servers. SYN cookies are a technique that allows a server to handle incoming connection requests during a SYN flood attack without maintaining a complete connection state table.
- **Keep Systems Updated**: Regularly update and patch server operating systems and network equipment to ensure they are protected against known vulnerabilities that could be exploited in a SYN flood attack.
- **Rate Limiting**: Implement rate limiting for incoming SYN requests. This can be done at the network level, using firewalls or specialized network equipment, to limit the rate at which new connections are accepted.

2. What is DNSSEC used for?

B. Cryptographic authentication of DNS zones.

3. Which of the following configurations is not a good security practice for a single domain name system (DNS) name server to perform? (5 Points)

A. Both authoritative name server and recursive name server

4. Domain name system (DNS) is a part of which of the following TCP/IP layers?

A. Applications layer

5. Which of the following is not a security goal of a domain name system (DNS)?

B. Confidentiality

6. Which of the following is a primary software component of a domain name system (DNS)?

D. Resolver

7. Which of the following does not use encryption?

D. Telnet

8. Which of the following provides a dynamic mapping of an Internet Protocol (IP) address to a physical hardware address?

B.ARP

9. Which of the following is not one of the actions taken by a firewall on a packet?

D. Destroy

10. Network address translation (NAT) protocol operates at what layer of the ISO/OSI reference model?

B. Network Layer 3

11. Spoofing in a local-area network (LAN) occurs with which of the following?

A. Internet Protocol (IP) addresses and Media access control (MAC) addresses

12. Packet sniffers are commonly used to capture network traffic data for which of the following purposes?

A. Troubleshooting purposes

13. Identify the true statement.

B. Stateful packet filtering considers the TCP connection state.

14. Which of the following is not a primary component or aspect of firewall systems?

D. Packet switching

15. Identify the true statement

A. An IPS is in the direct path of network traffic flow.