Assignment 1: TCP/IP methods and Attack Methods

Deadline: Friday 18/9 17:00

This assignment can be done by at most two persons.

Name1: Anna Furugård, annfu090 ____

Name2: ____

A. TCP/IP protocol and Security

This section contains questions related to the security issues that emerge from the TCP/IP protocol.

1. Why is the IP protocol unreliable?

Answer: The IP does not guarantee that the packet/segment/datagram is delivered to the destination.

2. IP is unreliable, and TCP uses IP. How does TCP provide reliable service to the application layer?

Answer: TCP ensures that all data sent arrives and arrives in correct order.

3. What does TCP do if the message to be sent is larger than what a single datagram can handle?

Answer: It split the datagram into smaller quantities.

4. What are the minimum and maximum header size of IP packets?

Answer: The minimum header size of an IP packet is 20 bytes and the maximum header size is 60 bytes.

5. An IP packet arrives at a router with the first eight bits as 01000011. The router discards the packet. Why?

Answer: The packet is discarded because its inaccurate. The minimum of an IP header is 20 bytes and the last four bits shows that the header length is only 12 bytes!

6. Why is it necessary to have both IP address and port number in a packet?

Answer: That is because the IP address identifies the host computer and the port number identifies the running process in the host computer.

7. Which of the protocols TCP, UDP and IP provides for reliable communication?

Answer: TCP provides for reliable communications.

B. Scanning Attacks

A scanning attack is a common type of attack based on the TCP/IP protocol. The following questions aim at understanding how these attacks can be done.

8. What is the purpose of host scanning?

Answer: The purpose of host scanning is to identify possible victims.

9. How does ping scanning work?

Answer: The intruder first finds out which hosts that are “live” by doing a ping sweep. In the ping sweep, you see which computers that respond by sending out ICMP packets to a network of machines. The hosts that are live will respond. When the intruder finds out which hosts that are “live”, he can focus on those machines to continue the attack.

10. Why are ping scans often not effective?

Answer: Firewalls on todays machines are configured to stop pings (the ICMP echo messages).

11. Why are SYN/ACK scans done?

Answer: To determine which ports that are open on the server.

12. How may hosts respond to SYN/FIN messages?

Answer: It depends which OS that is in use. If, for example, Linux is use it will block the reqest.

13. How does Traceroute (or Tracert) work?

Answer: Traceroute (or Tracert) is used to map a target networking by describe the path from the client to the remote host. The purpose (for the attacker) is to not only trace packet path but also to give information on the topology of the target network.

14. Why is port scanning done?

Answer: The attacker gains information about which services are running, what users own those services, if anonymous logins are available, and if certain network services require authentication.

15. How does TCP port scanning work?

Answer: In TCP port scanning the attacker scan servers for open TCP ports by sending SYN segments to a specified TCP port number. Then the attacker can observe the SYN/ACK or RST response.

16. Why is sending a long stream of scanning messages dangerous for attackers?

Answer: It can trigger an invasion detection system on the server. It is also easier for the attacker to get caught.

17 How do attackers use stealth scanning to reduce danger in the previous question?

Answer: The attacker sends a SYN request and analyzes the response. The response shows if the port is open or closed.

18. What rules would you add to the firewall to prevent the SYN/ACK attack?

Answer: We can check the period in seconds of a SYN/ACK message, if it have the ratio of 2:1 then the attack is deemed to have finished.

19. How many packets would be sent by an attacker to port scan 100 hosts for all well-known ports?

Answer: 204800 packets.

C. Attack Methods Based on TCP/IP Protocol

Besides scanning attacks there is a large variety of attacks based on the TCP/IP protocol. This section aims at understanding some of the most popular, the technique used and the consequences of the attack.

20. What is fingerprinting?

Answer: A fingerprint is a group of information that is used to detect a user's software, operating system, network protocols and hardware.

21. Distinguish between active and passive fingerprinting.

Answer: In active fingerprinting you are sending packets to the target and analyzes the result. You never send anything in passive fingerprinting, only analyzes packets with, for example, a sniffer.

22. Describe SYN flooding attack.

Answer: Firstly, an attacker sends multiple SYN messages to the server. The server responds with a SYN-ACK message and the attacker does not respond with a ACK message. The server will then have half-open connections since it will wait for the ACK response. This will lead to other clients being denied connecting to the server.

23. Which measures can be deployed to avoid a SYN flooding attack?

Answer: I would set the firewall to act as a proxy between client and server, this leads to the firewall responding to the SYN packets. The firewall will only allow a connection to the server if it receives an ACK packet from the client.

24. Describe how SYN cookies can be used to stop a SYN flooding attack.

Answer: SYN cookies is used to protect a server SYN queue to fill up during a SYN flood attack. The server replies to a TCP SYN request with SYN-ACKS, without adding a new record in the SYN Queue. Only if the client replies to the response, a new record is inserted.

25. Describe the Smurf attack.

Answer: Multiple ICMP packets with the victims ip-address (spoofed) are sent to the server. The server will then respond to the victims ip-adress. The victim's computer will be flooded with answers if there are enough packets sent. The result of a smurf attack is that the victim's network will be slowed down.

26. Describe DDoS attacks.

Answer: DDos is a denial of service attack from a network of IP addresses. The victims will get flooded with attacks from many attackers.

27. List some of the attacks that do use IP address spoofing.

Answer: Ping flooding (ICMP flooding) and SYN flooding.

28. List some of the attacks that do not use IP address spoofing.

Answer: Session Hijacking and Man-in-the-middle attack.