Assignment 1: TCP/IP methods and Attack Methods

Deadline: Friday 16/9 17:00

This assignment can be done by at most two persons.

Name: Daniel Böök

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?

   The IP protocol does not guarantee the delivery of packets. They can be lost, reordered, corrupted or duplicated.

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

   TCP breaks down the data into packets and relies on IP to send them. It attaches a sequence number to preserve the delivery order of packets. Lost packets are re-sent.

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

   It splits the datagram into smaller quantities.

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

   Min: 20 bytes, Max: 60 bytes.

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

   The last 4 digits in the packet are incorrect. These should specify the size, and the result is 3. The minimum size of a packet is 20 bytes therefore it is discarded.

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

   To find the right application on the right computer.

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

   TCP provide for reliable communication.

Scanning Attacks

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

8. What is the purpose of host scanning?

   To identify possible victims. By pinging a large amount of IP addresses a chance of finding an entry point is larger.

9. How does ping scanning work?

   A scan is done to check which IP addresses are mapped to live hosts.

10. Why are ping scans often not effective?

    Because a firewall often blocks the scan.

11. Why are SYN/ACK scans done?

    To find possible open ports on the server.

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

    That depends on the operating system. For example, Linux will block the request.

13. How does Traceroute (or Tracert) work?

    A traceroute is a network diagnostic tool for displaying the route a certain request takes when connecting to an internet protocol. For example which servers you are sent to during a request. Packets are sent while gradually increasing the TTL value starting with a value of one.

14. Why do attackers use Traceroute?

    Attackers can which way the signal travel through the network. Then they can focus their attack on certain computers.

15. Why is port scanning done?

    The see which ports are open and what server services can be performed. It can also be utilized for security reasons, to check if some ports should be closed. An attacker could benefit this, to check for a port of entry.

16. How does TCP port scanning work?

    The client sends SYN segments to scan for open TCP ports. After this, the client can observe the SYN/ACK or RST responses.

17. How does UDP port scanning work?

    0 byte UDP packets is sent by the client to each port. If ICMP port is unreachable the port is closed.

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

This makes the attacker more vulnerable to getting caught. It can trigger invasion detection on the server they are attacking.

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

They send SYN requests and analyzes the responses. The attacker can then see if the port is open or closed.

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

You add rules to block incoming ports when the threshold expressed in SYN and ACK messages is in one second intervals. Another rule is to check that the period of time between the SYN:ACK messages have a ratio of 2:1.

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

2048*100 = 204800 packets.

22. If both TCP and UDP port scanning are done against a host, how many ports need to be scanned to test all well-known ports?

1024.

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.

23. What is fingerprinting?

A way to find out what operating system the victim is using. Is pretty effective since most attacks are targeted to specific operating systems.

24. Distinguish between active and passive fingerprinting.

Active fingerprinting is sending odd messages and observing the results. These messages can be TCP, IP or ICMP. Different operating system answers differently depending on the message sent.

Passive fingerprinting reads packets and looks at parameters such as window size, TTL etc.

25. Describe SYN flooding attack.

The attacker sends many SYN messages to the server. The server will respond with the SYN/ACK message, but the attacker does not respond with the ACK message. This creates half-open connections since the server waits for the ACK message. If enough SYN messages are sent from the attacker, the server will deny normal clients to connect to the server, since all the resources are tied up waiting for the ACK messages from the attacker.

26. Why is the SYN flooding attack effective?

It is hard for the server to separate the connections of an attacker to an actual client. Therefore it is effective.

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

When the server receives a SYN packet from a client, the server will return the SYN and a cookie saying that it has received a request from that specific client. The client returns the ACK with the included cookie and the server now knows that the specific client before has contacted it. This keeps the server from waiting for an ACK response from the client with its connections open.

28. Describe the Smurf attack.

A large number of ICMP packets with the victims spoofed IP address are sent to a server. The server will then respond to the victims IP address. If enough packets are sent, the victims computer is flooded with answers to that will lead to slowing down the victims network.

29. Describe DDoS attacks.

It is a denial of service attack from a distributed network of IP addresses where the victim gets flooded with attacks from a large amount of attackers.

30. Why do attackers use DDoS attacks instead of simpler attacks?

Because it is easy to scale the method. If the victim is holding up against the attacks, the attacker can simply increase the amount of attacks and crash the victim's computer. It is also easier to hide since it is hard to filter through the large amount of requests.

31. List types of attacks for which IP address spoofing will be unattractive.

Attacks where you want to gather information about a certain client. In these attacks you want the information to return to your own network, and not somewhere else.

32. List types for which it will be attractive.

Denial of service for instance. You can both hide behind the spoofed IP as well as redirect some attacks back to the client.