Assignment 1: TCP/IP methods and Attack Methods

Deadline: Friday 25/9 17:00

By: Carl Englund, caren083

1. Why is the IP protocol unreliable?

It does not guarantee the delivery of a sent package to its destination. It relies on other protocols such as TCP for this. It also checks for errors but does not correct them if found. The package is simply dropped.

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

TCP requires a guarantee that the sent package has been delivered before continuing with the next one.

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

Splits the datagram up into smaller quantities.

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

Minimum is 20 bytes and Maximum is 60 bytes or 128/160 bits.

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

Because the last 4 digits in the binary representation are incorrect. These represent the size which has a minimum of 20. In our case they have the value 3.

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

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

TCP provides for reliable communications.

8. What is the purpose of host scanning?

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

9. How does ping scanning work?

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

10. Why are ping scans often not effective?

Often there is a firewall blocking the scan.

11. Why are SYN/ACK scans done?

SYN/ACK scans are done to determine what ports are open on the server.

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

It depends on the OS. Linux for example will block the request. (https://www.juniper.net/techpubs/software/junos-es/junos-es93/junos-es-swconfig-security/tcp-headers-with-syn-and-fin-flags-set.html)

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. In example, what servers your are sent to during a request. It works by sending packets while gradually increasing the TTL value. Starting with a value of one.

14. Why do attackers use Traceroute?

Hackers can watch what way the signal travels through the network and then focus their attacks on certain computers.

15. Why is port scanning done?

It is done to see what ports are open to see what server services can be performed. It can be done to for security reasons to see if something should be closed. Or from attackers to see a port of entry.

16. How does TCP port scanning work?

When scanning for open TCP ports on servers the client sends SYN segments to particular port numbers. Then they observe the SYN/ACK or RST responses for information.

17. How does UDP port scanning work?

The client sends 0 byte UDP packets to each port. If ICMP port is unreachable the port is closed. If there is no reply we don't know.

18. 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 ports.

19. What is fingerprinting?

A way of learning the victims operating system. Can be useful since most exploits works on specific and particular operation systems.

20. Distinguish between active and passive fingerprinting.

Active fingerprinting sends odd messages and observe the replies. Uses messages such as TCP, IP or ICMP. The way this works is that most operating systems answers differently depending on the message sent. Passive fingerprinting reads packets and look at parameters such as TTL, window size and such.

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

Its easy to get caught. It can also trigger invasion detection systems on the server.

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

By sending a SYN request and analysing the response the attacker can see if the port is open or closed.

23. Describe SYN flooding attack.

The attacker sends several SYN messages to the server. When the server responds with the typical SYN-ACK message the attacker simply does not respons back with the typical ACK message. This will bind the server with half-open connections since it will wait for the ACK response from the client. This basically denies normal clients to connect to the server since all the resources will be closed if enough SYN messages are sent from the attacker.

24. Why is the SYN flooding attack effective?

A SYN flooding attack is effective since it's hard for the server to seperate connections from an attacker and an actual client.

25. Describe the Smurf attack.

A large number of ICMP packets with the victims spoofed ip adress are sent to a server. The server will respond to the victims ip adress. If enough packets are sent the victims computer will be flooded with answers and this will lead to slowing down the victims network.

26. Describe DDoS attacks.

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

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

Its easy to scale the method if the victim is holding up well the attacker can increase the amount of attacks and that way crash the victim. It should also be easier to hide who is the attacker since there is a large amount of requests and hard to filter who is the real attacker.

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

Attacks where you want to gather information about a certain client is not a great use of IP spoofing since you want the information to return to your own network.

29. List types for which it will be attractive.

Attacks where you want to perform Denial of Service of a server for example since you can both hide behind the spoofed ip adress as well as some attacks use spoofing to redirect the attacks back to the client.

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

By adding rules to block incoming ports when the threshold expressed in SYN and ACK messages is in one second intervals. Also to check when the period of time in seconds of the SYN:ACK messages have a ratio of 2:1. When this happens the the attacks is deemed to have finished.

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

204800 packets.

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

SYN cookies works such that 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 the certain client. This way it does not have to keep an open connection against the client whilst waiting for the ACK response. When the client returns the ACK it will simply include the cookie stating that the server should know that it have already been contacted.