Assignment 1: TCP/IP methods and Attack Methods

Deadline: Friday 17/9 17:00

This assignment can be done by at most two persons.

Name1: Linn Storesund_____

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?

IP protocol is connectionless, meaning that each packet is sent independently from other packets. The sender will send a packet without asking the receiver if the receiver is ready or active. There is no acknowledgment from the receiver that the packet is delivered. The packets could be lost without the sender knowing.

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

TCP provides a reliable service since it makes sure the delivery of data using a data field known as checksum. The protocol itself makes sure that all that was sent is eventually delivered to the receiver. TCP can make sure of this even if packets were lost since it allows for the retransmission of said packages.

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

If the message is larger than what a single datagram can handle it is fragmented into several pieces to later be reconstructed.

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

The IP header has 4 bits that specify the number of 32-bit words in the header. The minimum field is 5 and therefore the minimum size is 5*32 bits = 160 bits = 20 bytes. The maximum value is 15 and the maximum size is 15*32 = 480 bits = 60 bytes.

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

This packet has an error, even though the 4 left-most bits (0100) show the version which is correct the next 4 bits (0011) show the header length which is 3 * 4 = 12 where the minimum number of bytes in the header must be 20 and therefore the router discards the package.

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

The port number is associated with the application layer and indicates the service to be used.

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

TCP

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?

Identify and use vulnerabilities in the operating system, applications and programs.

9. How does ping scanning work?

With the ping scanning it sweeps and discover all the host IP addresses in a network. It is an Internet Control Message Protocol, ICMP which from echo request replies if the target is alive.

10. Why are ping scans often not effective?

It is easy for a user to block pings on the firewall or on the router.

11. Why are SYN/ACK scans done?

To gain information on the firewall to be able to better use the system. From the scan it can for example allow one to analyze if the firewall is stateful or non-stateful.

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

SYN/FIN messages never occur in regular traffic and may indicate that a DoS attack or some sort of probing scan is underway. The most reasonable would be for the host to simply shun the source of the message.

13. How does Traceroute (or Tracert) work?

It traces the paths data packets from the source to the destination, allowing administrators to better resolve connectivity issues.

14. Why is port scanning done?

To determine and get information of what ports a system may be listening on and what services are running on the system.

15. How does TCP port scanning work?

TCP scanning is used for finding open TCP ports and works by sending SYN segments to port numbers and observing the SYN/ACK or RST response. An SYN/ACK response means that the port is possibly open, and an RST response means that the port is closed but that there is an alive device here. No response means the SYN filtered by the network.

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

They risk being detected. Most systems have some form of IDS (Intruder detection systems) installed and they are very good at detecting such long streams of scanning messages.

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

They scan the ports in a longer period to avoid being detected

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

A firewall that simply only allow the client to connect to the server after it has received an ACK packet, eliminating half-open connections to server/client.

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

0 to 1023 are known as the "well-known ports" which means that 204 800 packets (1024*2*100 UDP ports and TCP ports) would need to be sent to port 100 hosts.

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?

A method that uses ICMP to determine the underlying OS since every OS has different methods of handling network traffic.

21. Distinguish between active and passive fingerprinting.

Active – an active technique to determine a serves role. This could be techniques such as simply calling or emailing or more technical such as scanning. The scanning may be done by sending traffic to a system and analysing the response. This may be done only in the purpose of monitoring traffic.

Passive – use some sort of sniffer to capture sent traffic from a system. The fingerprinting technique analyses the traffic to find out what the server is up to and collects only traffic, meaning the sniffer needs to be installed in the network.

22. Describe SYN flooding attack.

It is a DDoS attack of sort. By sending a slew of SYN requests to a target's system it aims to consume enough of the servers' recourses to render the system unable to handle legitimate traffic.

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

There are several methods that can be used to defense these types of attacks, For example are to increase the backing queue and to reduce the SYN received timer.

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

SYN cookies is a technical attack mitigation technique whereby the server replies to TCP SYN requests with crafted SYN-ACKs, without inserting a new record to its SYN Queue. Only when the client replies this crafted response a new record is added. This technique is used to protect the server SYN Queue from filling up under TCP SYN floods.

25. Describe the Smurf attack.

It's a DDoS attack where many ICMP echo request packets with the victims spoofed source IP are broadcasted to a computer network using an IP broadcast address. This prompts, by default, a response from most devices on a network to the source IP address. This response, if large enough will flood the source IP address to the point that it may render the victim's computer useless.

26. Describe DDoS attacks.

DDoS stands for distributed denial-of-service attack and is when several systems flood the bandwidth of a certain system. This is usually done to unison of web servers using a notnet by flooding it with traffic. When a server is bombarded with connections it can no longer establish any new ones.

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

- SYN flooding
- PING flooding
- Smurf attack

28. List some of the attacks that do <u>not</u> use IP address spoofing.

- SQL injection
- Malware