Assignment 1: TCP/IP methods and Attack Methods

Deadline: Friday 16/9 17:00

This assignment can be done by at most two persons.

Name1: ___Uma Eriksson, umaer178_____

Name2: ___Hugo Dahl, hugda958_____

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?

   The IP protocol does not verify if the source adress in the headers are the correct one. It is done by the transfer protocol which take advantage of the IP protocol.

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

   The TCP first confirms a connection between two hosts before any “real” communication takes place. This confirmation is called the Three Way Handshake.

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

   It’s split in to smaller pieces (fragmentation)

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

   The minimum is 20 bytes and the maximum is 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 is to small. The minimum header size is 20 bytes. The first 4 bits represent the version and the last four represents the header size. 0011 represents the decimal 3, which means this package is of the size 3 * 4 = 12 bytes, i.e. to small.

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

   Port numbers are the address to a specific service or application on a system whilst the IP address is the destination for the system.

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?

   To identify possible victims

9. How does ping scanning work?

   An ICMP echo request is sent to a target IP adress (usually multiple targets in a network), if the response is an ICMP reply you know the target is alive.

10. Why are ping scans often not effective?

    Usually blocked by firewalls

11. Why are SYN/ACK scans done?

    To find victims for attacks without them knowing (usually no connection will be logged with this attack)

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

    The host who starts the termination of a connection with the FIN flag should get a response with the ACK and FIN flag, then the host responds with a ACK flag and the connection is terminated.

13. How does Traceroute (or Tracert) work?

    Traceroute is used to track how the network traffic is routed. It works by sending ICMP packets, every router involved in this transfer gets these packets. The packets contain information about how efficiently a router transfer the data during the transmission.

14. Why is port scanning done?

    It is done to identify network services running on a host and could be used to find possible vulnerabilities.

15. How does TCP port scanning work?

    It will test an IP address for any common ports.

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

    You can easily be detected. You can trigger invasion detection systems that are on the server.

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

Stealth scans uses certain packet flags that will cause the system to respond without having a fully established connection.

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

    Enable the firewall to detect and filter the SYN packets. Firewalls can remove strange options and fragmented packets before they reach the OS.

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

    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?

    Fingerprinting is used to find out the operating system of a certain target.

21. Distinguish between active and passive fingerprinting.

    Active fingerprinting is sending odd messages to gain a response and then observing the response. Because most OS and application programs respond differently and you can use this to your advantage.

    Passive fingerprinting relies on sniffing techniques meaning only to observe and not actively sending requests to gain information.

22. Describe SYN flooding attack.

    It is a DDoS attack that attempts a system with request to consume resources and ultimately leads to the system being overwhelmed and maybe crash.

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

    It can be prevented by using a firewall as a proxy between the server and client. The firewall will only allow connections to server after it receives an ACK packet, this process will eradicate the possibilities of server/client half-open connections.

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

    The server replies to the TCP SYN requests with a crafted SYN-ACK, without creating new TCBs for the TCP connection. This TCB is only created for the TCP connection when the client replies to it

25. Describe the Smurf attack.

It is a type of DDoS attack that will render the computers networks inoperable. It will accomplice this by exploitation of the IP and ICMP vulnerabilities. First the malware will use a technique called spoofing (creating a network packet attached to a fake IP address) Inside the packet is an ICMP ping message which asks for the network node that will receive the packet for a response. These replies are then sent back to the IP address again, which now sets up into an infinite loop.

26. Describe DDoS attacks.

DDoS (Distributed Denial of Service) will try to use up all the server resources by sending a bunch of requests to overwhelm the server, therefore rending it unusable.

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

SYN Flooding

Smurf Flooding

And other DDoS attacks where you want to hide behind the spoofed IP.

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

Man in the Middle

Session hijacking

And other attacks where you want to gather data, since you want to redirect the gathered data back to yourself (your own IP).