Date: 15-04-2022

CSS Assignment 2

Q1) Write a short note on TCP/IP Vulnerabilities (layer wise).

Identifying Possible Network Interface Layer Attacks

At the Network Interface layer, the packet of information that is placed on the wire is known as a frame. The packet is comprised of three areas: the header, the payload, and the FCS. Because the Network Interface layer is used for communications on a local network, the attacks that occur at this level would be carried out on local networks. Some of the ways the network layer can be exploited to compromise the C-I-A triad include the following:

- MAC address spoofing: The header contains the MAC address of the source and destination computers and is required to successfully send a directed message from a source computer to a destination computer. Attackers can easily spoof the MAC address of another computer. Any security mechanism based on MAC addresses is vulnerable to this type of attack.
- Denial of service (DoS): A DoS attack overloads a single system so that it cannot provide the service it is configured to provide. An ARP protocol attack could be launched against a computer to overwhelm it, which would make it unavailable to support the C-I-A triad.
- ARP cache poisoning: The ARP cache stores MAC addresses of computers on the local network that have been contacted within a certain amount of time in memory. If incorrect, or spoofed, entries were added to the ARP cache, then the computer is not able to send information to the correct destination.

Identifying Possible Internet Layer Attacks

At the Internet layer, IP datagrams are formed. The packet is comprised of two areas: the header and the payload. Some of the ways the Internet layer can be exploited to compromise the C-I-A triad include the following:

- IP address spoofing: If the IP header fields and lengths are known, the IP address in the IP datagram can be easily discovered and spoofed. Any security mechanism based on the source IP address is vulnerable to this attack.
- Man-in-the-middle attacks: This attack occurs when a hacker places himself or herself between the source and destination computer in such a way that neither notices his or her existence. Meanwhile, the attacker can modify packets or simply view their contents.
- DoS: With a DoS attack at this level, simple IP-level protocols and utilities can be exploited to overload a computer, thus breaking the C-I-A triad.
- Incorrect reassembly of fragmented datagrams: For fragmented datagrams, the Offset field is used with packet reassembly. If the offset is changed, the datagram is reformed incorrectly. This could allow a datagram that would typically not pass through a firewall to gain access to your internal network, and could disrupt the C-I-A triad.
- Corrupting packets: Because IP datagrams can pass through several computers between the source and destination, the information in the IP header fields is read and sometimes modified, such as when the information reaches a router. If the packet is intercepted, the information in the header can be modified, corrupting the IP datagram. This could cause the datagram to never reach the destination computer, or it could change the protocols and payload information in the datagram.

Identifying Possible Transport Layer Attacks

At the Transport layer, either a UDP header is added to the message or a TCP header is added. The application that is requesting the service determines what protocol will be used. Some of the ways the Transport layer can be exploited to compromise the C-I-A triad include the following:

- Manipulation of the UDP or TCP ports: By knowing the UDP and TCP header fields and lengths, the ports that are used for communications between a source and destination computer can be identified, and that information can be corrupted or exploited.
- DoS: With a DoS attack at this level, simple IP-level protocols and utilities can be exploited to overload a computer, thus breaking the C-I-A triad. For instance, by knowing the steps involved in a three-way TCP handshake, a hacker or cracker might send the packets in the incorrect order and disrupt the availability of one of your servers. An example of this is a SYN flood, where a hacker sends a large number of SYN packets to a server and leaves the session half open. The server leaves these sessions half-open for a prescribed amount of time. If the hacker is successful in opening all available sessions, legitimate traffic will be unable to reach the server.
- Session hijacking: This kind of attack occurs after a source and destination computer have established a communications link. A third computer disables the ability of one the computers to communicate, and then imitates that computer. Because the connection has already been established, the third computer can disrupt your C-I-A triad.

Identifying Possible Application Layer Attacks

Application layer attacks can be some of the most difficult to protect against because they take advantage of vulnerabilities in applications and lack of end-user knowledge of computer security. Some of the ways the Application layer can be exploited to compromise the C-I-A triad include the following:

- E-mail application exploits: Attachments can be added to e-mail messages and delivered to a user's inbox. The user can open the e-mail message and run the application. The attachment might do immediate damage, or might lay dormant and be used later. Similarly, hackers often embed malicious code in Hypertext Markup Language (HTML) formatted messages. Exploits of this nature might take advantage of vulnerability in the client's e-mail application or a lack of user knowledge about e-mail security concerns.

- Web browser exploits: When a client computer uses a Web browser to connect to a Web server and download a Web page, the content of the Web page can be active. That is, the content is not just static information, but can be executable code. If the code is malicious, it can be used to disrupt the C-I-A triad.

- FTP client exploits: File Transfer Protocol (FTP) is used to transfer files from one computer to another. When a client has to provide a user name and password for authentication, that information can be sent across the Internet using plain text. The information can be captured at any point along the way. If the client uses the same user name and password as they use to attach to your corporate servers, that information could be obtained by a hacker or cracker and used to access your company's information.

Q2) Write a short note on firewall and its types.

A firewall is a network security perimeter device that inspects traffic entering and leaving the network. Depending on the security rules assigned specifically to it, the firewall either permits safe traffic or denies traffic it deems as dangerous.

A firewall's main objective is to establish a barrier (or "wall") that separates an internal network from incoming external traffic (such as the internet) for the purpose of blocking malicious network packets like malware and hacking.

How does firewall technology work?

Firewalls carefully analyze incoming traffic arriving on a computer's entry point, called a port, which determines how external devices communicate with each other and exchange information.

Firewalls operate using specific firewall rules. A firewall rule will typically include a source address, a protocol, a port number and a destination address.

Here's an analogy to explain the components of a firewall rule. Instead of protecting a network, think of a giant castle. The source address represents a person wishing to enter the castle. The port represents a room in the castle. The protocol represents a mode of transportation, and the destination address represents the castle.

Only trusted people (source addresses) may enter the castle (destination address) at all. Or perhaps only people that arrive on foot (protocol). Once inside, only people within the house are permitted to enter certain rooms (destination ports), depending on who they are. The king may be allowed in any room (any port), while guests and servants may only access a certain number of rooms (specific ports).

Types of firewalls

First, firewalls are classified by what they are and where they reside. For example, firewalls can either be hardware or software, cloud-based or on-premises.

A software firewall resides on an endpoint (like a computer or mobile device) and regulates traffic directly from that device. Hardware firewalls are physical pieces of equipment that reside between your gateway and network. Cloud-based firewalls, also known as Firewall-as-a-service (FaaS), act like any other internet-based SaaS solutions, performing their work in the cloud.

The most common firewall types based on methods of operation are:

- Packet-filtering firewalls
- Proxy firewalls
- NAT firewalls
- Web application firewalls
- Next-gen firewalls (NGFW)

Packet-filtering firewalls

Packet-filtering firewalls, the most basic firewall type, examine packets and prevent them from moving on if the specific security rule is not met. This firewall's function is to perform a simple check of all data packets arriving from the network router and inspecting the specifics like source and destination IP address, port number, protocol, and other surface-level data.

Packet filtering firewalls don’t open data packets to inspect their contents. Any data packet that fails the simple inspection is dropped.

These firewalls are not resource-intensive and have a low impact on system performance. Their main drawback is that they provide only basic protection and are therefore more vulnerable to being bypassed.

Packet-filtering firewalls can either be stateful and stateless. Stateless firewalls only analyze each packet individually, whereas stateful firewalls — the more secure option — take previously inspected packets into consideration.

Proxy firewalls

Proxy firewalls, also known as application-level firewalls, filter network traffic at the application layer of the OSI network model. As an intermediary between two systems, proxy firewalls monitor traffic at the application layer (protocols at this layer include HTTP and FTP). To detect malicious traffic, both stateful and deep packet inspection are leveraged.

Proxy firewalls typically operate in the cloud or through another proxy device. Instead of allowing traffic to connect directly, a connection to the traffic's source is established and the data packet is inspected.

Speed can be a key weakness of proxy firewalls, as the transfer process creates extra steps that may slow things down.

NAT firewalls

Network address translation (NAT) firewalls work by assigning a public address to a group of devices inside a private network. With NAT, individual IP addresses are hidden. Therefore, attackers scanning for IP addresses on a network are prevented from discovering specific details.

NAT firewalls and proxy firewalls both act as a go-between connecting groups of devices with outside traffic.

Web application firewalls

Web application firewalls (WAF) are responsible for filtering, monitoring, and blocking data packets as they travel in and out of websites or web applications. A WAF can either reside on the network, at the host or in the cloud and is typically placed in front of one or many websites or applications. WAFs are available as server plugins, cloud services, or network appliances.

A WAF is most similar to the proxy firewall, but has a more specific focus on defending against application layer web-based attackers.

NGFW firewalls

As the threat landscape intensifies, the Next-generation firewall (NGFW) is the most popular firewall type available today.

Thanks to the major improvements in storage space, memory, and processing speeds, NGFWs build upon traditional firewalls' features and add other critical security functions like intrusion prevention, VPN, anti-malware, and even encrypted traffic inspection. NGFW’s ability to handle deep packet inspection means that the firewall can unpack the packet's data to prevent any packets with malicious data from moving forward.

Q3) A and B decide to use Diffie Hellman algorithm to share a key. They chose $p = 23$ and $g = 5$ as the public parameters. Their secret keys are 6 and 15 respectively. Compute the secret key that they share.

Solution:

$prime\ number = \ p = 23, \qquad Genrater = \ g = 5$

$Secret\ key\ of\ A = \ \ X_A = 6, \qquad Secret\ key\ of\ B = X_B = 15$

$Public\ key\ of\ A = \ R_A = g^{X_A}(mod p) \ = 5^6(mod 23) = \ (5^2)^3(mod 23)$

$R_A = \ 2^3(mod 23) = 8$ Send to B

$Public\ key\ of\ B = \ R_B = g^{X_B}(mod p) \ = 5^{15}(mod 23) = \ (5^2)^7 \times 5(mod 23)$

$R_B = 2^7 \times 5(mod 23) = 13 \times 5(mod 23) = 72\ (mod 23) = 19$ Send to A

$Secret\ Key\ calculated\ by\ A = key = \ (R_B)^{X_A} = 19^6(mod 23) = 2$

$Secret\ Key\ calculated\ by\ B = key = \ (R_A)^{X_B} = 8^{15}(mod 23) = 2$