سيـــــســـــــــــــــ ٢ ـــــــــــــــــكــو

1.why Passwords are poor security mechanisms ?

- Users typically choose passwords that are **easy to remember** and easy to guess
- **Randomly** generated passwords are **hard to remember**;
- Passwords are **easily shared**, written down, and forgotten.
- Passwords **can be stolen** through many means, including observation,
- Passwords are often **transmitted in clear text** or with easily broken encryption
- Password **databases are often stored in publicly** accessible online locations.
- **Short passwords** can be discovered quickly in **brute-force attacks**.

2. ***what is Challenge-response tokens*** ?

generate passwords or responses based on instructions from the authentication system. The authentication system displays a challenge, usually in the form of a code. This challenge is entered into the token device. The token responds to the challenge, and then that response is entered into the system for authentication.

Using token authentication systems offers much stronger security than using password authentication alone. In addition to username, password, PIN, code, and so on.

➔ 3. What are Methods of Attack

classes of attacks or attack methodologies:

methods of network-based attacks:

- Brute-force and dictionary attacks
- Denial-of-service attacks
- Spoofing
- Man-in-the-middle attacks
- Spamming
- Sniffers

الشـــــــــــــــــــــــرح

Brute-Force and Dictionary Attacks

brute-force and dictionary attacks together because they are against : passwords.

brute-force attack

is an attempt to discover passwords for user accounts by systematically attempting every possible combination of letters, numbers, and symbols.

With enough time, all passwords can be discovered using a brute-force attack method. Most passwords of 14 characters or less can be discovered within 7 days on a fast system using a brute-force attack program against a stolen password database file

In theory, this window can be exploited in a time-memory trade-off known as *rainbow tables.*

The longer the password, the more costly and time-consuming a brute-force attack.

dictionary attack

is an attempt to discover passwords by attempting to use every possible password from a predefined list of common or expected passwords.

This type of attack is named such because you were using the entire dictionary one word at a time to discover passwords.

Password attacks employ a specific cryptographic attack method known as the *Birthday attack*
This attack is also called *reverse hash matching* or the *exploitation of collision*

attack exploits the fact that if two messages are hashed and the hash values are the same, then the two messages are probably the same.

$$H(M)=H(M').$$

Denial-of-Service Attacks

Denial-of-service (DoS) attacks are attacks that prevent the system from processing or responding to legitimate traffic or requests for resources and objects.

The most common form of denial-of- service attacks is transmitting so many data packets to a server that it cannot process them all.

Other forms of denial-of-service attacks focus on the exploitation of a known fault or vulnerability in an operating system, service, or application. Exploiting the fault often results in system crash or 100 percent CPU utilization.

denial-of-service attacks based on *flooding* (that is, sending sufficient traffic to a victim to cause a DoS) are a way of life on the Internet.

Another form of attack is called the ***distributed denial of service*** **(DDoS)**. Distributed denial of service occurs when the attacker compromises several systems and uses them as launching platforms against one or more victims.

are often called *slaves* or *zombies*.

A more recent form of DoS, called a *distributed reflective denial of service* (DRDoS)
DRDoS attacks take advantage of the normal operation mechanisms of key Internet services, such as DNS and router update protocols. DRDoS attacks function by sending numerous update, session, or control packets to various Internet service servers or routers with a spoofed source address of the intended victim. Usually these servers or routers are part of the high-speed, high-volume Internet backbone trunks.

This type of attack is called a *reflective attack* because the high-speed backbone systems reflect the attack to the victim.

SYN Flood Attack

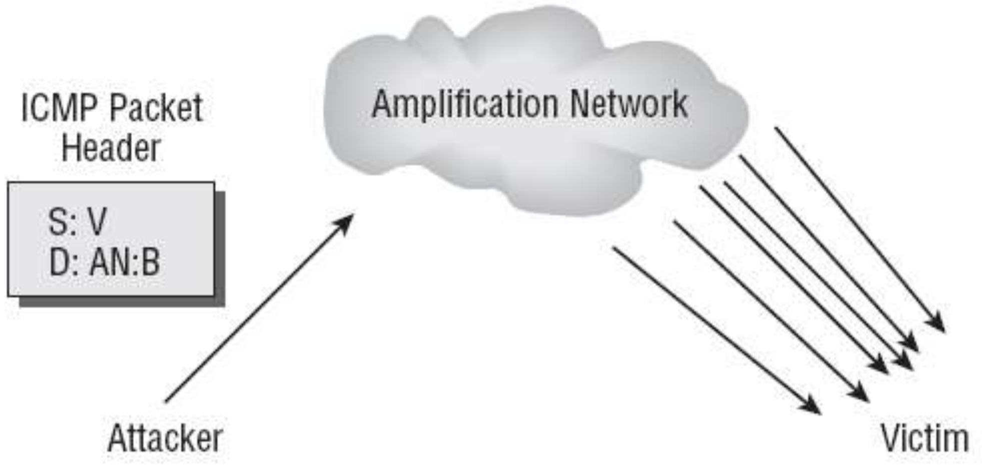
SYN flood attacks are waged by breaking the standard three-way handshake used by TCP/IP to initiate communication sessions. Normally, a client sends a SYN packet to a server, the server responds with a SYN/ACK packet to the client, and the client then responds with an ACK packet back to the server.

This three-way handshake establishes a communication session that is used for data transfer until the session is terminated (using a three-way handshake with FIN and ACK packets).

A SYN flood occurs when numerous SYN packets are sent to a server but the sender never replies to the server's SYN/ACK packets with the final ACK.

Smurf Attack

A *smurf* attack occurs when an amplifying server or network is used to flood a victim with useless data. An amplifying server or network is any system that generates multiple response packets, such as ICMP echo packets or special UDP packets, from a single submitted packet.



One common attack is to send a message to the broadcast of a subnet or network so that every node on the network produces one or more response packets. The attacker sends information request packets with the victim's spoofed source address to the amplification system. Thus, all the response packets are sent to the victim.

with a source address spoofed as the victim (V) and a destination address that is the same as the broadcast address of the amplification network (AN:B). The amplification network responds with multiplied volumes of echo packets to the victim, thus fully consuming the victim's connection bandwidth.

Another DoS attack similar to smurf is called *fraggle*. Fraggle attacks employ spoofed UDP packets rather than ICMP packets

Ping-of-Death, WinNuke, Stream, Teardrop, and Land Attacks

ping-of-death attack employs an oversized ping packet. Using special tools, an attacker can send numerous oversized ping packets to a victim. In many cases, when the victimized system attempts to process the packets, an error occurs, causing the system to freeze, crash, or
reboot. The ping of death is more of a buffer-overflow attack, but because it often results in a downed server, it is considered a DoS attack.
Countermeasures to the ping-of-death attack include keeping up-to-date with OS

A *WinNuke* attack is a specialized assault against Windows 95 systems causes the OS to freeze. Countermeasures for this attack consist of updating Windows 95 with the appropriate patch or changing to a different OS.

A *stream* attack occurs when a large number of packets are sent to numerous ports on the victim system using random source and sequence numbers. The processing performed by the victim system attempting to make sense of the data will result in a DoS. **Countermeasures include patching the system and using an IDS for dynamic blocking.**

A *teardrop* attack occurs when an attacker exploits a bug in operating systems. The bug exists in the routines used to reassemble (that is, resequence) fragmented packets. An attacker sends numerous specially formatted fragmented packets to the victim, which causes the system to freeze or crash. Countermeasures for this attack include patching the OS and deploying an IDS for detection and dynamic blocking.

A *land* attack occurs when the attacker sends numerous SYN packets to a victim and the SYN packets have been spoofed to use the same source and destination IP address and port number as the victim. This causes the system to think it sent a TCP/IP session opening packet to itself, which causes a system failure and usually results in a system freeze, crash, or reboot. Countermeasures for this attack include patching the OS and deploying an IDS for detection and dynamic blocking.

Spoofing Attacks

Spoofing is the art of pretending to be something other than what you are. Spoofing attacks consist of replacing the valid source and/or destination IP address and node numbers with false ones.
Spoofing is when an intruder uses a stolen username and password to gain entry

Two specific types of spoofing attacks are *impersonation* and *masquerading*.
these attacks are the same: someone is able to gain access to a secured system by pretending to be someone else.

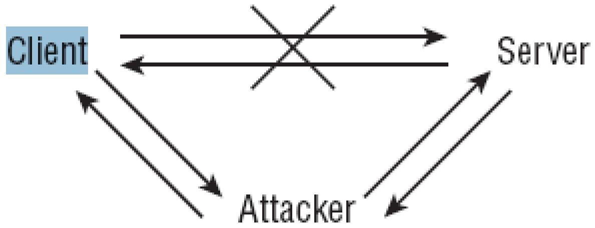
Masquerading is considered a more passive attack because the attacker uses previously stolen account credentials to log on to a secured system.

Countermeasures to spoofing attacks include patching the OS and software, enabling source/destination verification on routers, and employing an IDS to detect and block attacks.

Man-in-the-Middle Attacks

A *man-in-the-middle* attack occurs when a malicious user is able to gain a position between the two endpoints of an ongoing communication.

There are two types of man-in-the- middle attacks. One involves copying or sniffing the traffic between two parties; this is basically a sniffer attack. The other involves attackers positioning themselves in the line of communication where they act as a store-and-forward or proxy mechanism



A result of a man-in-the-middle attack is known as a *hijack attack*. In this type of attack, a malicious user is positioned between a client and server and then interrupts the session and takes it over.

Another type of attack, a *replay attack* (also known as a *playback attack*), is similar to hijacking. A malicious user records the traffic between a client and server

Countermeasures to these types of attacks require improvement in the session establishment, identification, and authentication processes.

An IDS cannot usually detect a man-in-the-middle or hijack attack, but it can often detect the abnormal activities.

Sniffer Attacks

A *sniffer* attack (also known as a *snooping* attack) is any activity that results in a malicious user obtaining information about a network or the traffic over that network.

sniffing attacks are invisible to all other entities on the network and often precede spoofing
or hijack attacks. A replay attack is a type of sniffer attack.
Countermeasures to prevent or stop sniffing attacks require improving the physical access
control, actively monitoring for sniffing signatures and using encrypted traffic over internal and external network connections.

Spamming Attacks

Spam is the term describing unwanted email, newsgroup, or discussion forum messages.

Spamming attacks are directed floods of unwanted messages to a victim’s email inbox or other messaging system.

Such attacks cause DoS issues by filling up storage space and preventing legitimate messages from being delivered.

In extreme cases, spamming attacks can cause system freezes or crashes .

countermeasures include using email filters, email proxies, and IDSs to detect, track, and terminate spam flood attempts.