Types of Attack

Lecture 2

‘Attack’ in Cyber and Information Security

An attack refers to an intentional or malicious act that aims to compromise the confidentiality, integrity, or availability of information or information systems.

Attacks = Motive (Goal) + Vulnerability+Method

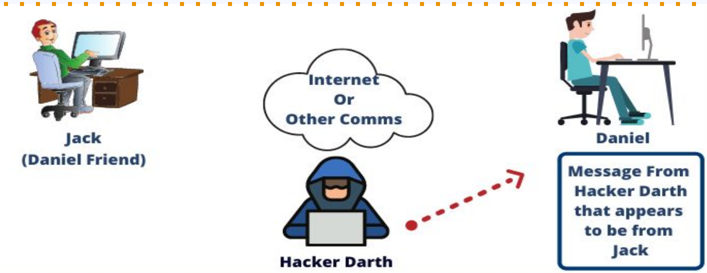
Active Attack

- An Active attack involves direct interference or manipulation of data or systems, such as modifying or deleting data, launching Denial of Service (DoS) attacks, or injecting malware.
- A few common types of Active attacks are:
  - Masquerade
  - Modification of messages
  - Replay
  - Denial of Service

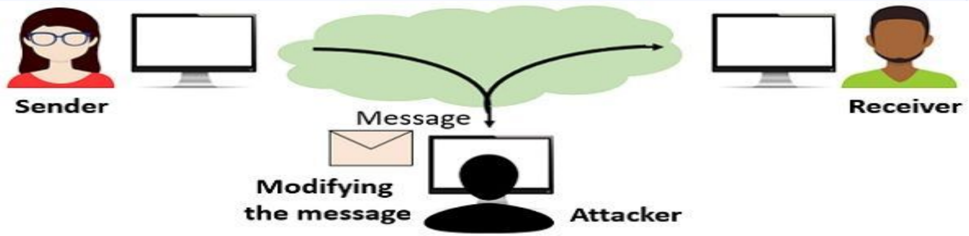
.

Active Attack

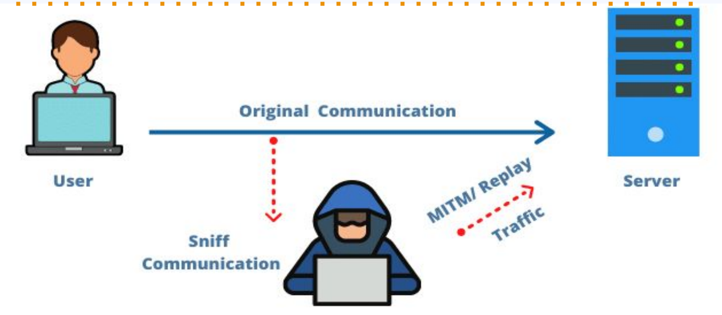
Masquerade



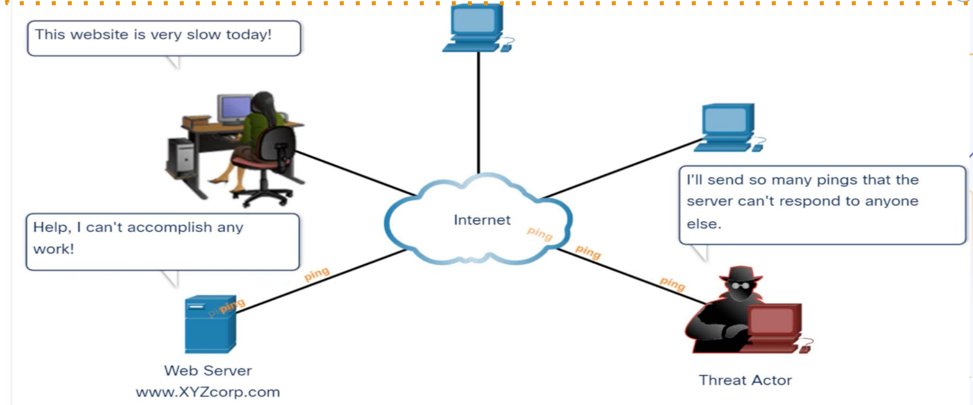
Modification of Message



Replay



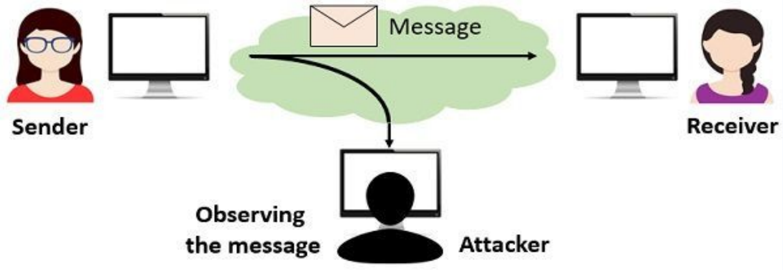
DoS (Denial of Service)


This website is very slow today!
Help, I can't accomplish any work!
Internet
ping
ping
ping
ping
ping
I'll send so many pings that the server can't respond to anyone else.
Web Server
www.XYZcorp.com
Threat Actor

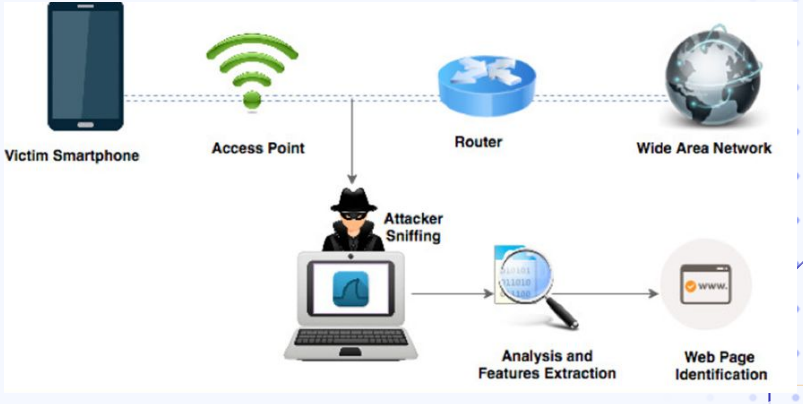
Passive Attack

- **Passive Attack** on the other hand, focus on unauthorized monitoring or capturing of data without altering it, like eavesdropping or sniffing network traffic.
- Types of Passive attacks are as follows:
  - The release of message content
  - Traffic analysis

Release of message content



Traffic analysis



Insider Attack

Insider Attack involve individuals who have authorized access to systems or information but misuse their privileges for malicious purposes.

Compromised insiders

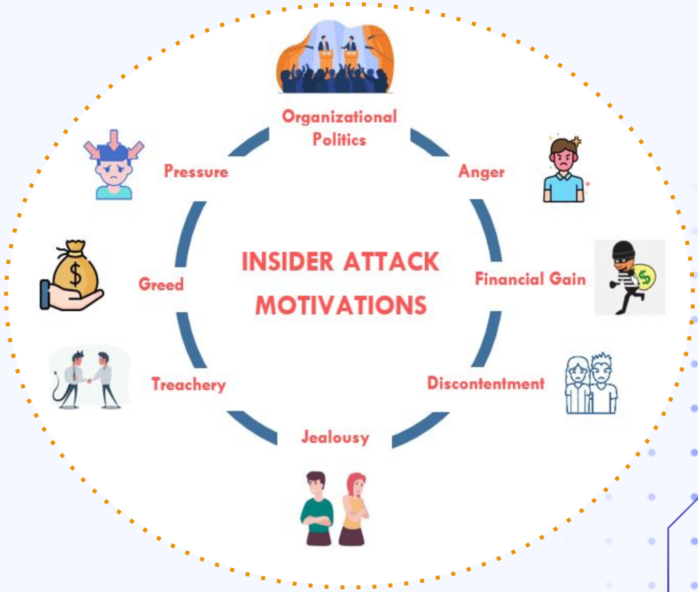
Insiders whose accounts are compromised and used by cyber criminals

Malicious insiders

Intentionally use their access to sensitive data to harm the company

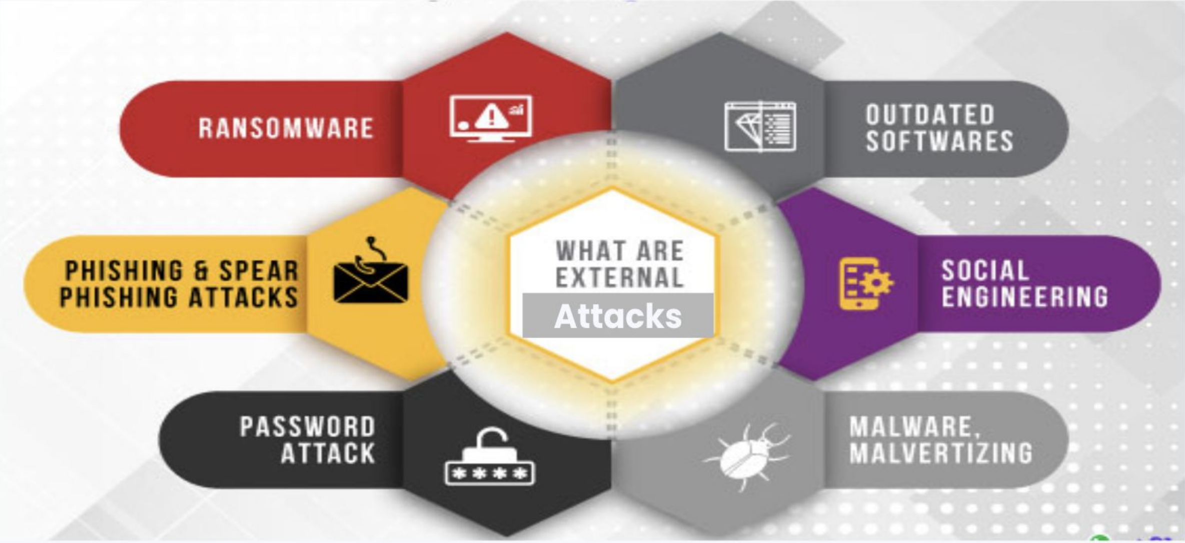
Careless insiders

Pose an unintentional threat due to human error or security policy violations



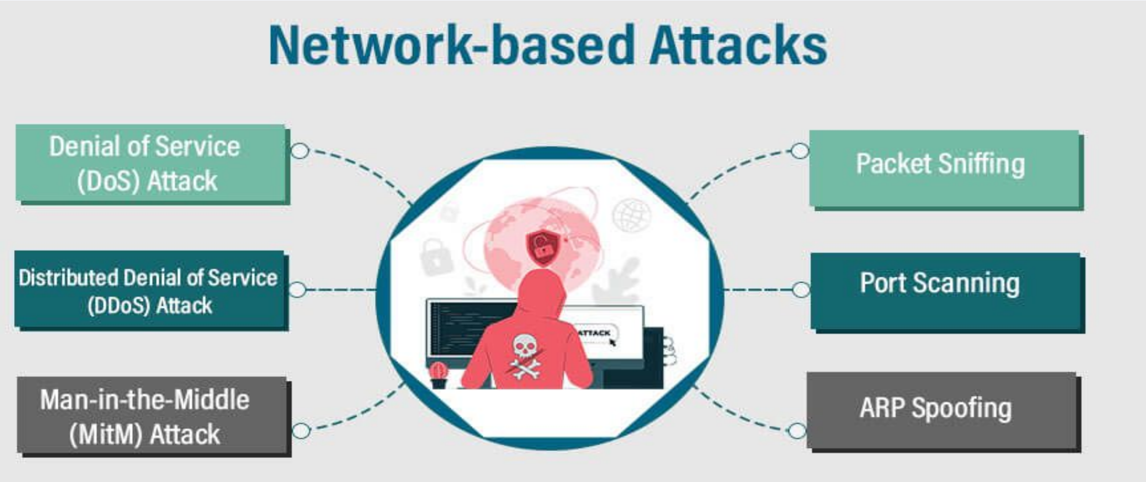
External Attacks

External attacks are conducted by individuals or groups who do not have authorized access and typically target systems from outside the organization's network.



Network-based attacks

Network-based attacks target vulnerabilities in network infrastructure, protocols, or services, aiming to gain unauthorized access, disrupt communication, or intercept data.


Network-based Attacks
Denial of Service (DoS) Attack
Distributed Denial of Service (DDoS) Attack
Man-in-the-Middle (MitM) Attack
ATTACK
Packet Sniffing
Port Scanning
ARP Spoofing

Host-based attacks

Host-based attacks focus on exploiting vulnerabilities in individual computer systems or software applications, attempting to gain control over the host or compromise its data.

Types of Host Based Attacks

- Virus
- Worm
- Trojan Horses
- Back Door
- Trap Door

Symptoms:

- Virus - Freezing, Slow performance, crashing
- Worm - Unexpected restarts, error pop-ups, program malfunctions
- Trojan Horses - Mouse moves by itself, volume goes up and down by itself

Some Other Kinds of Attacks

- **Known attacks** refer to attacks for which security experts and organizations are already aware of the methods or vulnerabilities being exploited. These attacks can be mitigated using established security measures, such as patches, updates, or intrusion detection systems.

- **Zero-day attacks**, on the other hand, exploit previously unknown vulnerabilities that have not been discovered or patched yet. They pose a higher risk as there may be no immediate defense or mitigation available.

- **Web-based Attacks,** This classification focuses specifically on attacks targeting web applications or services. It includes various attacks like SQL injection, Cross-Site Scripting (XSS), session hijacking. These attacks exploit vulnerabilities in web applications to gain unauthorized access, manipulate data, or compromise user accounts.

- **Social engineering attacks** involve manipulating human psychology or behavior to deceive individuals into revealing sensitive information or performing actions that compromise security. Examples include phishing, pretexting, baiting, or tailgating.

Questions

Thanks!