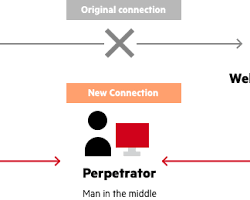
**Lab Practical #01:**

Study of passive and active attacks on computer systems.

* **Active Attacks**

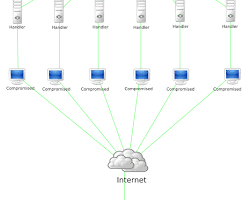
1. **Man-in-the-Middle (MitM) Attacks:**

A MitM attack is a cyberattack where an attacker secretly inserts themselves into the communication between two parties, essentially becoming the "middle man." The attacker can then eavesdrop on the conversation, steal data, or even modify the data before it reaches its intended recipient.



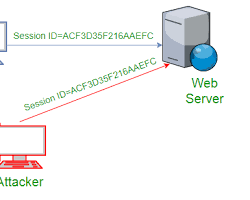
1. **Denial-of-Service (DoS) Attacks:**

A Denial-of-Service (DoS) attack aims to overwhelm a system or network with a flood of traffic, making it unavailable to legitimate users. Imagine a crowded waiting room with so many people that no one can get served. A DoS attack disrupts normal operations by creating a similar situation in the digital world.



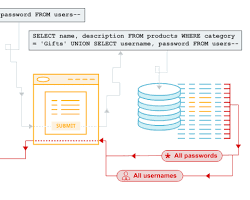
1. **Session Hijacking:**

Session hijacking is a cyberattack where an attacker takes over a legitimate user's session on a server. This allows the attacker to access the user's account, steal data, or even impersonate the user. Imagine someone stealing your car keys while you're momentarily distracted. Session hijacking works in a similar way, where an attacker steals your "session key" to impersonate you online.



1. **SQL Injection:**

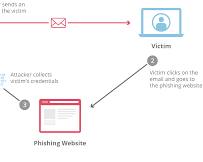
SQL injection (SQLi) is a cyberattack that exploits vulnerabilities in how websites and applications interact with databases. Attackers can inject malicious SQL code into user input fields to manipulate the database queries and potentially gain unauthorized access to sensitive information. Imagine someone tampering with a library's search function to access restricted sections of the catalog database. SQL injection works in a similar way, manipulating website functions to access unauthorized data.



1. **Phishing Attacks:**

A phishing attack is a cyberattack that deceives users into revealing sensitive information, such as usernames, passwords, credit card details, or other personal data. Phishing attempts typically involve masquerading as a trusted entity like a bank, credit card company, social media platform, or even a colleague.

Imagine receiving a seemingly legitimate email from your bank, urging you to verify your account details. Clicking a link in the email might take you to a fake website that looks real, designed to steal your login credentials. Phishing attacks are prevalent because they prey on human trust and inattentiveness.

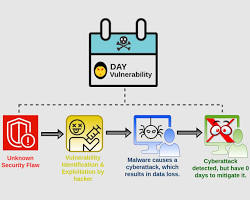


1. **Malware Attacks:**

Malware, short for **malicious software**, refers to any program or code designed to harm a computer system, network, or device. Malware attacks are a significant threat in information and network security, aiming to disrupt operations, steal data, or gain unauthorized access to systems.

1. **Zero-Day Attacks:**

A zero-day attack is a cyberattack that exploits a previously unknown vulnerability in software or hardware. Because the vulnerability is new and there's no patch available, these attacks are particularly dangerous. Imagine a thief discovering a new way to break into houses, and using it to rob homes before anyone knows about the vulnerability. Zero-day attacks operate in a similar fashion, targeting weaknesses before software developers have a chance to fix them.



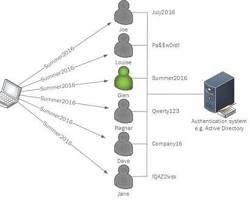
1. **Watering Hole Attacks:**

A watering hole attack is a targeted cyberattack strategy that exploits frequented online locations visited by a specific group of users. Imagine a predator lurking near a watering hole in the wild, waiting to ambush unsuspecting animals. In the digital world, attackers target websites or online resources that a particular group of users (like employees of a company or visitors to a specific forum) are known to frequent. Once the target website is compromised, attackers can infect devices with malware or steal data when users visit the compromised site.



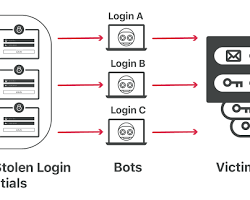
1. **Password Spraying Attacks:**

A password spraying attack is a brute-force technique that attempts to gain unauthorized access to multiple accounts by trying a single common password against a large list of usernames. Imagine a thief trying the same skeleton key on multiple doors in a building, hoping one will open. Password spraying works similarly, trying a common password on many accounts to exploit weak password practices.



1. **Credential Stuffing Attacks:**

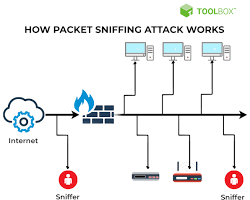
Credential stuffing is a cyberattack technique that exploits stolen login credentials (usernames and passwords) from one source to gain unauthorized access to accounts on other websites or services. Imagine a thief finding a lost wallet with multiple credit cards inside. The thief might try those same cards at different stores, hoping one will work. Credential stuffing works similarly, trying stolen credentials across various platforms to see if they unlock any accounts.



* **Passive Attack**

1. **Traffic Sniffing:**

Traffic sniffing, also known as packet sniffing, is a technique used to capture data packets traveling across a computer network. Imagine a wiretap on a telephone conversation, but instead of intercepting voice calls, traffic sniffing intercepts digital communication flowing through a network. This captured data can include sensitive information like usernames, passwords, emails, and even financial data if not properly encrypted.



1. **Shoulder Surfing:**

Shoulder surfing is a social engineering technique where attackers steal confidential information by simply looking over someone's shoulder. Imagine someone peering over your shoulder while you're counting cash at an ATM. In the digital world, shoulder surfing targets people entering sensitive data like passwords or PINs on their devices in public places.

1. **Eavesdropping:**

Eavesdropping, in the context of information and network security, refers to the unauthorized interception of private communication. Imagine someone listening in on a phone conversation they're not part of. In the digital world, eavesdropping targets electronic communications, including data transmissions over networks, phone calls, or even video conferencing sessions.

1. **Piggybacking:**

Piggybacking, in information and network security, refers to the unauthorized use of a legitimate user's connection to access a computer network. Imagine someone sneaking onto a crowded train without a ticket by following a paying passenger. In the digital world, piggybacking exploits weaknesses in network security to gain unauthorized access.

1. **WLAN (Wireless Local Area Network) eavesdropping:**

WLAN eavesdropping, also known as Wi-Fi eavesdropping, refers to the unauthorized interception of data transmitted over wireless local area networks (WLANs). Imagine someone listening in on a phone conversation, but instead of voices, they're intercepting digital information flowing through the air. In WLAN eavesdropping, attackers exploit weaknesses in Wi-Fi security to steal sensitive data or spy on network activity.



1. **Dumpster Diving:**

Dumpster diving, in the cybersecurity realm, refers to the act of searching through discarded physical materials for sensitive information that can be used to compromise computer systems or steal data. Imagine a real-life dumpster diver searching through trash for recyclables, but instead of cans and bottles, they're looking for confidential documents or electronic devices.

1. **Steganography Detection:**

Steganography, as we discussed earlier, is the art of hiding secret messages within seemingly harmless media like images, audio, or video files. Unlike cryptography, which scrambles the message itself, steganography attempts to conceal the very existence of the hidden data.

1. **Zero-Knowledge Proofs:**

Zero-knowledge proofs (ZKPs) are a powerful cryptographic technique that allows one party (the prover) to convince another party (the verifier) that they possess a certain piece of information (the secret) without actually revealing the information itself. Imagine proving you're over 21 to enter a bar without showing your ID – the bouncer (verifier) is convinced you meet the age requirement (secret) through some verification process without actually seeing your birthdate.