Assignment 1

Different Types Of Cyber Attacks

**Malware:** Malware is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software. Once inside the system, malware can do the following:

* Blocks access to key components of the network (ransomware)
* Installs malware or additional harmful software
* Covertly obtains information by transmitting data from the hard drive (spyware)
* Disrupts certain components and renders the system inoperable

**Phishing:** Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine. Phishing is an increasingly common cyberthreat.

Man-in-the-middle attack: Man-in-the-middle (MitM) attacks, also known as eavesdropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Two common points of entry for MitM attacks:

1. On unsecure public Wi-Fi, attackers can insert themselves between a visitor’s device and the network. Without knowing, the visitor passes all information through the attacker.

2. Once malware has breached a device, an attacker can install software to process all of the victim’s information.

**Denial-of-service attack:** A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack. This is known as a [distributed-denial-of-service (DDoS) attack](https://www.cisco.com/c/en/us/products/security/what-is-a-ddos-attack.html).

**SQL injection:** A Structured Query Language (SQL) injection occurs when an attacker inserts malicious code into a server that uses SQL and forces the server to reveal information it normally would not. An attacker could carry out a SQL injection simply by submitting malicious code into a vulnerable website search box.

**Zero-day exploit:** A zero-day exploit hits after a network vulnerability is announced but before a patch or solution is implemented. Attackers target the disclosed vulnerability during this window of time. [Zero-day vulnerability threat detection](https://www.talosintelligence.com/vulnerability_reports) requires constant awareness.

**DNS Tunneling:** DNS tunneling utilizes the DNS protocol to communicate non-DNS traffic over port 53. It sends HTTP and other protocol traffic over DNS. There are various, legitimate reasons to utilize DNS tunneling. However, there are also malicious reasons to use DNS Tunneling VPN services. They can be used to disguise outbound traffic as DNS, concealing data that is typically shared through an internet connection. For malicious use, DNS requests are manipulated to exfiltrate data from a compromised system to the attacker’s infrastructure. It can also be used for command and control callbacks from the attacker’s infrastructure to a compromised system.

**Session Hijacking**-It is a security attack on a user session over a protected network. Web applications create cookies to store the state and user sessions. By stealing the cookies, an attacker can have access to all of the user data.

**Brute force**-It is a type of attack which uses a trial and error method. This attack generates a large number of guesses and validates them to obtain actual data like user password and personal identification number. This attack may be used by criminals to crack encrypted data, or by security, analysts to test an organization's network security.

**Dictionary attacks**-This type of attack stored the list of a commonly used password and validated them to get original password.

**URL Interpretation**-It is a type of attack where we can change the certain parts of a URL, and one can make a web server to deliver web pages for which he is not authorized to browse.

**File Inclusion attacks**-It is a type of attack that allows an attacker to access unauthorized or essential files which is available on the web server or to execute malicious files on the web server by making use of the include functionality.

**Man in the middle attacks**-It is a type of attack that allows an attacker to intercepts the connection between client and server and acts as a bridge between them. Due to this, an attacker will be able to read, insert and modify the data in the intercepted connection.