**Cybersecurity Terminologies Documentation**

1. Access Control:

Access control means the policies and technologies used to regulate who can access information or systems. What people can or cannot do within a system is determined using their roles or credentials.

1. Adware:

Adware is a type of malicious software designed to display unwanted advertisements on a user’s computer or device. It typically generates revenue for its creators by displaying ads, often causing annoyance to the user.

1. Antivirus:

Antivirus software is designed to detect, prevent, and remove malicious software, including viruses, worms, and trojans. It scans files and programs for known threats and protects systems from potential attacks.

1. Authentication:

Authentication is the process of verifying the identity of a user, device, or system. This is often done using credentials such as usernames, passwords, biometrics, or multi-factor authentication (MFA) methods.

1. Authorization:

Authorization refers to granting or denying access to resources as a result of an authenticated identity. Once an account has been authenticated, the system verifies what such a user is allowed to do through their permissions.

1. Backdoor:

A backdoor is a method used to bypass security controls and gain unauthorized access to a system, typically installed by hackers or malware. Backdoors are often used to maintain persistent access to a compromised system.

1. Botnet:

A botnet is a group of hijacked computers or other devices remotely controlled by a hacker. Botnets are employed for massive cyber attacks, such as Distributed Denial of Service attacks.

1. Brute Force Attack:

A brute force attack is a trial-and-error method of cracking passwords or encryption by systematically trying every possible combination until the correct one is found. These attacks are time-consuming and can be prevented by using strong, complex passwords.

1. Cryptography:

Cryptography is the practice of securing communication and information through codes and ciphers. It encompasses encryption, converting plaintext to ciphertext, and decryption, converting ciphertext back to plaintext, to guarantee confidentiality and integrity.

1. DDoS (Distributed Denial of Service):

A DDoS attack is an attempt to overwhelm a system, server, or network by flooding it with an excessive amount of traffic from multiple sources. This causes the target system to become slow or unavailable.

1. Exfiltration:

Exfiltration is the unauthorized transfer of data from a computer or network to an external location. This usually contains sensitive or confidential information, and it is one of the common objectives in cyberattacks.

1. Exploit:

An exploit is a piece of software or code that exploits a vulnerability in a system or application to gain unauthorized access or cause harm.

1. Firewall:

A firewall is a network security device or software that monitors and controls incoming and outgoing network traffic. It establishes a barrier between trusted and untrusted networks, protecting systems from malicious attacks.

1. Hacker:

A hacker is someone who gains unauthorized access to computer systems, networks, or devices, often for malicious purposes. There are different types of hackers (white hat, black hat, gray hat) based on their intentions.

1. Intrusion Detection System (IDS):

An IDS is a security system that monitors network or system activities for signs of malicious activity or violations. It raises alerts when suspicious behavior is detected, allowing for timely responses.

1. Malware:

Malware is malicious software designed to damage, disrupt, or gain unauthorized access to computer systems. Common types of malware include viruses, worms, trojans, ransomware, and spyware.

1. Phishing:

Phishing means social engineering. The attackers just pretend to some legitimate entity who can try their best to hoax individuals into presenting sensitive information: usernames, password, or any credit card-related details. It uses an email the most of its times.

1. Ransomware :

Ransomware is the malware that will encrypt a victim's files, then demand some payment (known as ransom) for the key to decrypt those files. Such attacks can severely cause financial loss and data loss in an individual or organization.

1. Rootkit:

A rootkit is a set of tools used by cybercriminals for gaining privileged access to a system and hiding the presence of that cybercriminal. Rootkits are often difficult to detect and remove because they run at a very low level within the operating system.

1. Social Engineering :

Social engineering is the process of tricking people into revealing confidential information or taking actions that undermine security. Examples include phishing, pretexting, baiting, and tailgating.

1. Spyware:

Spyware is a form of malware that gathers information about a user or organization without their consent, usually by monitoring web browsing patterns or keystrokes. It is typically used to steal sensitive information.

1. SQL Injection:

SQL Injection is the injection of a code to make use of some vulnerability in a web application's database query mechanism. An attacker inserts malicious SQL code into the input fields which then gets executed by the database that may result in data theft or manipulation.

1. Trojan Horse:

A Trojan horse is a type of malware that disguises itself as a legitimate program or file to deceive users into executing it. Once activated, Trojans can perform harmful actions, such as stealing data or creating backdoors.

1. Vulnerability:

A vulnerability is a weakness in a system, application, or network that can be exploited by an attacker in order to gain unauthorized access or to perform malicious actions. Vulnerability assessments regularly help identify and mitigate risks.

1. Zero-Day Attack :

A zero-day attack is an attack where an attacker exploits a previously unknown vulnerability in software or hardware before the vendor can release a patch or fix. These attacks are particularly dangerous because there is no prior defense against them.

* **Conclusion**

Understanding the terminology used in cybersecurity is crucial for anyone entering the field. From technical terms such as “firewalls” and “malware” to more conceptual ones like “social engineering,” being familiar with these terms helps professionals to communicate effectively, identify threats, and implement security measures efficiently. As you progress in your cybersecurity studies, these terms will form the foundation of your knowledge and will be essential in daily practice.