Cybersecurity Definitions

1. Hacker

A hacker is anyone who attempts to gain unauthorized access to systems, networks, or data. Hackers can have varying intentions, ranging from curiosity to malicious intent.

2. Types of Users

- **Normal User**: A user who interacts with systems and applications in a standard, non-harmful manner.
- **Malicious User**: A user who intentionally uses systems or applications in an aggressive or harmful way to cause damage or gain unauthorized access.

3. Types of Attacks

- **Local Attack**: An attack that occurs within a local network, targeting devices or systems within that network.
- **Remote Attack**: An attack that occurs over the internet, targeting systems or networks from anywhere in the world.

4. Vulnerability

A weakness or flaw in a system, network, or application that can be exploited to cause harm or malfunction.

5. Exploit

The act of taking advantage of a vulnerability to gain unauthorized access or cause harm to a system.

6. Payload

The malicious component of a virus or malware that performs the harmful action, such as stealing data or damaging files.

7. Session

The period during which a virus or malware remains active on a compromised system.

8. Zero-Day Vulnerability

A vulnerability that is discovered and exploited by attackers before the software developer has had a chance to release a patch or fix.

9. Security Through Obscurity

A security approach that relies on hiding or obscuring data, systems, or processes to prevent unauthorized access. This method is often considered weak if used alone.

10. Authentication

The process of verifying a user's identity, typically through a username and password, to grant access to a system.

11. Authorization

The process of granting or restricting access to specific resources or data based on a user's permissions and role.

12. Script vs. Normal Program

- **Script**: A set of instructions executed through a command-line interface (CLI) or terminal.
- **Normal Program**: A software application with a graphical user interface (GUI) designed for user interaction.

13. Administrator

The highest-level user in a Windows system with full control over the system's settings and resources.

14. Root

The highest-level user in a Linux system with unrestricted access to all commands and files.

15. User

A standard user with limited permissions, typically restricted from making system-wide changes.

16. Permissions

Rules that determine what actions a user can perform on a system or resource, such as reading, writing, or executing files.

17. Privilege

The level of access or authority granted to a user to perform specific tasks or access certain data.

18. Eavesdropping

The unauthorized interception of data or communications as they travel across a network.

19. Denial of Service (DoS) Attack

An attack that floods a server or network with excessive traffic from a single device, overwhelming it and causing it to become unavailable.

20. Distributed Denial of Service (DDoS) Attack

An attack that floods a server or network with excessive traffic from multiple devices, making it even more difficult to mitigate and causing widespread disruption.

21. Server

A centralized system or device that stores and manages data, resources, or services for other devices or users.

22. Port

A virtual entry point on a server or device that allows communication between systems. Each port is associated with a specific service or protocol.

23. Service

A specific function or resource provided by a server, such as file sharing, email, or web hosting.

24. Protocol

A set of rules and standards that govern how data is transmitted and communicated over a network (e.g., HTTP, HTTPS, FTP).

25. HTTP (Hypertext Transfer Protocol)

A protocol used to transfer data over the web. It is not secure, as data is transmitted in plain text.

26. HTTPS (Hypertext Transfer Protocol Secure)

A secure version of HTTP that encrypts data during transmission to protect it from interception or tampering.

27. Status Codes

Numeric codes that indicate the status of a web request:

- **200**: The request was successful.

- **3xx**: Redirection (the requested data has moved).
- **4xx**: Client error (e.g., 404 - Not Found).
- **5xx**: Server error (e.g., 500 - Internal Server Error).

28. Shellcode

A piece of code used in exploits to execute malicious actions on a compromised system.

29. Hashing Techniques

- **Salt**: A random string of characters added to a password before hashing to enhance security.
- **Pepper**: A secret value added to a password before hashing, typically stored separately for added security.

30. Sniffing

The process of capturing and analyzing network traffic to monitor or intercept data. Tools include:

- **Wireshark**: A GUI-based network analysis tool.
- **TCP Dump**: A command-line tool for capturing network traffic.

31. Malware

Malicious software designed to harm, exploit, or gain unauthorized access to systems or data.

32. Worm

A type of malware that spreads across networks, infecting multiple devices without user interaction.

33. Virus

A type of malware that infects a single computer or device, often requiring user interaction to spread.

34. Backdoor

A hidden method of bypassing security mechanisms to gain unauthorized access to a system or network.

35. Bypass

The act of circumventing security measures or protections to gain unauthorized access.

36. Active Directory

A directory service used in Windows environments to manage and connect computers, users, and resources within a network.

Extra Definitions

1. **Ransomware**: A type of malware that encrypts a victim's data and demands payment (ransom) in exchange for decryption.
2. **Firewall**: A network security device that monitors and controls incoming and outgoing traffic based on predefined security rules.
3. **VPN (Virtual Private Network)**: A service that encrypts internet traffic and masks the user's IP address to ensure privacy and security.
4. **Botnet**: A network of compromised devices controlled by an attacker to perform malicious activities, such as DDoS attacks.
5. **Intrusion Detection System (IDS)**: A tool that monitors networks or systems for suspicious activity and alerts administrators.
6. **Data Breach**: An incident where sensitive or confidential data is accessed, stolen, or exposed without authorization.
7. **Patch Management**: The process of updating software to fix vulnerabilities, improve functionality, or enhance security.
8. **Identity and Access Management (IAM)**: A framework for managing user identities and controlling access to resources based on roles and permissions.
9. **Cloud Security**: Measures and technologies designed to protect data, applications, and infrastructure in cloud environments.
10. **Threat Intelligence**: Information about potential or current cyber threats, used to proactively defend against attacks.