Day 6 CYBERSECURITY GLOSSARY AND INTRO TO NETWORKING

Cybersecurity Glossary

A–C

1. **Antivirus** – Software that detects and removes malicious software (malware).
2. **Authentication** – Verifying the identity of a user or system.
3. **Authorization** – Granting access rights to resources or systems.
4. **Backdoor** – Hidden method to bypass normal authentication.
5. **Botnet** – Network of infected devices controlled remotely by hackers.
6. **Brute Force Attack** – Attempting every password combination to gain access.
7. **Cipher** – An algorithm for encrypting and decrypting data.
8. **CIA Triad** – Core principles: Confidentiality, Integrity, Availability.
9. **Clickjacking** – Tricking users into clicking something malicious.

D–H

1. **Data Breach** – Unauthorized access to confidential data.
2. **Dark Web** – Part of the internet that isn't indexed by search engines, often accessed via Tor.
3. **Denial-of-Service (DoS)** – Attack that overwhelms a system to make it unavailable.
4. **Digital Forensics** – Investigating and recovering data from digital devices.
5. **Encryption** – Converting data into unreadable code to protect it.
6. **Exploit** – A method used to take advantage of a vulnerability.

7. **Firewall** – Security system that controls incoming/outgoing traffic.
8. **Hashing** – Converting data into a fixed-length string, typically for verifying integrity.

I–P

1. **Incident Response** – Steps taken after a cybersecurity event.
2. **IP Address** – A unique identifier for a device on a network.
3. **Keylogger** – Malware that records keystrokes.
4. **Malware** – Malicious software designed to harm or exploit.
5. **Multi-Factor Authentication (MFA)** – Using two or more methods to verify identity.
6. **Patch** – A software update that fixes vulnerabilities.
7. **Penetration Testing** – Ethical hacking to find vulnerabilities in a system.
8. **Phishing** – Tricking someone into giving up sensitive information via fake emails or websites.

R–Z

1. **Ransomware** – Malware that encrypts data and demands payment to unlock it.
2. **Rootkit** – Malware designed to hide the presence of other malicious software.
3. **Social Engineering** – Manipulating people into revealing confidential info.
4. **Spoofing** – Disguising a communication from an unknown source as being from a known source.
5. **Spyware** – Software that secretly gathers user info.
6. **Threat Actor** – A person or group behind a cyberattack.
7. **Trojan Horse** – Malware disguised as legitimate software.
8. **Two-Factor Authentication (2FA)** – A subset of MFA using 2 verification methods.
9. **Vulnerability** – A weakness in a system that can be exploited.

10. **Zero-Day** – A vulnerability unknown to the vendor and unpatched.

Networking

- **Definition:** Networking is the process of connecting computers and other devices to share resources and information.
- **Purpose:** Enables communication, file sharing, internet access, and device management.
- **Key Components:** Routers, switches, cables, wireless access points.

What is the Internet?

- **Definition:** A global network of networks that connects millions of devices worldwide.
- **How it works:** Uses protocols like TCP/IP to transmit data between devices.
- **Fun Fact:** The Internet is the biggest example of a Wide Area Network (WAN).

Identifying Devices on a Network

- **Each device (host) has:**
  - An **IP address** (unique identifier).
  - A **MAC address** (hardware identifier).
- Tools like `ipconfig` **(Windows)** or `ifconfig` **(Linux/Mac)** help identify devices.
- Network scanners (like Nmap) can also list connected devices.

Ping (ICMP)

- **Ping:** A tool that sends an **ICMP echo request** to test connectivity between devices.
- **Example:** `ping google.com` checks if your computer can reach Google.
- **Useful for:** Troubleshooting, checking network latency or downtime.

Intro to LAN

- **LAN (Local Area Network):** A network limited to a small area like a home, office, or school.
- **Characteristics:** High speed, low latency, and usually privately managed.
- **Devices in LAN:** Computers, printers, routers, smart devices — all connected locally.