Three Ways to Attack - Social, Physical, Network

In cybersecurity, exploits are actions or tools that attackers use to compromise systems. Attacks can generally be grouped into three categories based on the method of exploitation: **social, physical, and network attacks**. Each type uses different tactics to bypass security, obtain access, or gather sensitive information. Here's a breakdown of each attack category and the specific techniques commonly used within them.

1. Social Attacks

> Social attacks **exploit human psychology and trust rather than technical vulnerabilities**. They rely on manipulating individuals to gain access to systems, data, or credentials.

- Ask the Person for Access: Sometimes attackers simply ask for access, relying on the target's trust or lack of suspicion. Posing as legitimate personnel, they may gain entry by asking directly.
- **Phishing**: Attackers send fraudulent messages that appear to come from a trusted source, tricking users into revealing credentials or clicking malicious links.
- **Cognitive Biases**:
    - Attackers exploit cognitive biases such as authority bias (trusting authority figures), reciprocity (feeling obligated to return favors), and urgency (forcing quick decisions).
- **Spear Phishing**: A targeted form of phishing where attackers **tailor their approach to a specific individual or organization**, making it more believable and effective.
- **Water Holing**: Attackers compromise a website frequented by the target group, planting malware that infects visitors who belong to the target organization.
- **Baiting**: Attackers **leave physical media, such as USB drives or CDs**, in locations where employees will find them, hoping curiosity leads them to plug the media into a company computer.
- **Tailgating**: Attackers **follow legitimate employees into secure areas without providing credentials**, often relying on the social courtesy of holding doors open.

2. Physical Attacks

> Physical attacks **require proximity or direct access to devices**. These attacks focus on tampering with hardware or exploiting the lack of physical security measures.

- **Get Hard Drive Access**: Attackers gain direct access to a hard drive, which might lead to unauthorized data retrieval if it's unencrypted.
- **Boot from Linux**: Attackers with physical access can boot a system from an external Linux drive, bypassing the operating system's security to access files directly.
- **Brute Force Password**: Using software or hardware devices, attackers repeatedly guess passwords until they find the correct one.
- **Keyloggers**: Attackers install keyloggers on a computer to capture keystrokes, allowing them to record login credentials, passwords, and other sensitive information. Keyloggers can be hardware or software-based.
- **Frequency Jamming (Bluetooth/WiFi)**: Attackers **disrupt wireless communications by jamming** Bluetooth or Wi-Fi frequencies, potentially interfering with security devices or other network-dependent systems.

- **Covert Listening Devices**: Attackers plant hidden microphones or bugging devices to record conversations and collect intelligence.
- **Hidden Cameras**: Small cameras can be hidden in inconspicuous places, allowing attackers to monitor physical spaces, observe passwords being typed, or track user behavior.
- **Disk Encryption**: Encryption protects data on drives by making it unreadable without the decryption key. Attackers must circumvent encryption to gain access, often requiring sophisticated techniques.
- Trusted Platform Module (TPM): TPMs are hardware-based security modules embedded in devices to secure encryption keys and other sensitive data, providing additional security against physical attacks.
- **TEMPEST (NSA)**: TEMPEST refers to NSA research into spying via unintended signals (electromagnetic, sound, or vibration) emitted by electronic devices. Attackers may use these signals to gather data remotely from devices.

3. Network Attacks

> Network attacks exploit vulnerabilities within the network to intercept data, discover devices, or execute remote attacks.

- **Nmap**: Nmap is **a network scanning tool used to discover live hosts, open ports, and services on a network**. Attackers use Nmap to map network topologies and identify potential targets.
- **Find CVEs for Any Services Running**: Attackers search for known vulnerabilities (CVE IDs) associated with services running on discovered hosts. These vulnerabilities, if unpatched, can provide entry points into the system.
- **Interception Attacks**: Attackers use methods like man-in-the-middle (MitM) to intercept and read data packets sent over the network, often capturing login credentials and other sensitive information.
- Getting Unsecured Info Over the Network: Attackers monitor network traffic for unencrypted data transmissions, including credentials, files, and messages, which can be easily captured and read.

Summary

- **Social Attacks** manipulate people to gain access, leveraging tactics like phishing, cognitive biases, spear phishing, baiting, and tailgating.
- **Physical Attacks** exploit direct access to devices, using techniques such as booting from external drives, keylogging, frequency jamming, hidden cameras, and covert listening.
- **Network Attacks** involve probing the network for vulnerabilities and intercepting data, employing tools like Nmap, exploiting CVEs, interception techniques, and capturing unsecured data.

By understanding these attack vectors, organizations can implement better security practices, such as physical security controls, encryption, user training, and network monitoring, to defend against these varied attack types.