Classification of Cyber Attacks

BSCS – 5th FGHI
ICS/IT, The University of Agriculture Peshawar

Lecture 03

Kashif Ali

kashif.nth@aup.edu.pk

Classification of Attacks

According to IATF, security attacks are classified into five categories:

- Passive Attacks
- Active Attacks
- Close-in Attacks
- Inside Attacks
- Distribution Attacks

Passive Attacks

Passive attacks involve intercepting and monitoring network traffic and data flow on the target network and do not tamper with the data.

Attackers perform reconnaissance on network activities using sniffers.

These attacks are very difficult to detect as the attacker has no active interaction with the target system or network.

Passive attacks allow attackers to capture the data or files being transmitted in the network without the consent of the user.

For example, an attacker can obtain information such as unencrypted data in transit, clear-text credentials, or other sensitive information that is useful in performing active attacks.

Examples of Passive Attacks

- Footprinting
- Sniffing and eavesdropping
- Network traffic analysis
- Decryption of weakly encrypted traffic

Active Attacks

Active attacks tamper with the data in transit or disrupt communication or services between the systems to bypass or break into secured systems.

Attackers launch attacks on the target system or network by sending traffic actively that can be detected.

These attacks are performed on the target network to exploit the information in transit.

They penetrate or infect the target’s internal network and gain access to a remote system to compromise the internal network.

kashif.nth@aup.edu.pk

Examples of Active Attacks

- Denial-of-service (DoS) attack
- Bypassing protection mechanisms
- Malware attacks (such as viruses, worms, ransomware)
- Modification of information
- Spoofing attacks
- Replay attacks
- Password-based attacks
- Session hijacking
- Man-in-the-Middle attack
- DNS and ARP poisoning
- Compromised-key attack
- Firewall and IDS attack
- Profiling
- Arbitrary code execution
- Privilege escalation
- Backdoor access
- Cryptography attacks
- SQL injection
- XSS attacks
- Directory traversal attacks
- Exploitation of application and OS software

Close-in Attacks

Close-in attacks are performed when the attacker is in close physical proximity with the target system or network.

The main goal of performing this type of attack is to gather or modify information or disrupt its access.

For example, an attacker might shoulder surf user credentials.

Attackers gain close proximity through surreptitious entry, open access or both.

Examples of Close-in Attacks

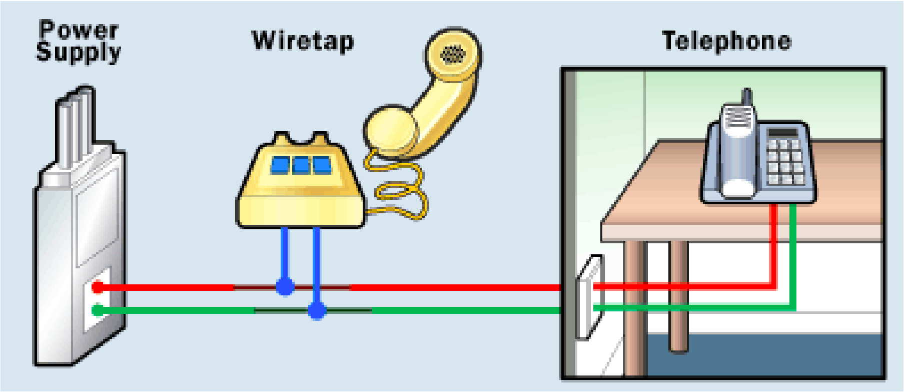
Social Engineering (Eavesdropping, shoulder surfing, dumpster diving, and other methods)

Insider Attacks

- Inside attacks are performed by trusted persons who have physical access to the critical assets of the target.
- An insider attack involves using privileged access to violate rules or intentionally cause a threat to the organization’s information or information systems.
- Insiders can easily bypass security rules, corrupt valuable resources, and access sensitive information.
- They misuse the organization’s assets to directly affect the confidentiality, integrity, and availability of information systems.
- These attacks impact the organization’s business operations, reputation, and profit.
- It is difficult to figure out an insider attack.

Examples of Insider Attacks

- Eavesdropping and wiretapping
- Social engineering
- Data theft and spoliation
- Pod slurping
- Theft of physical devices
- Planting keyloggers, backdoors, or malware



Distribution Attacks

- Distribution attacks occur when attackers tamper with hardware or software prior to installation.
- Attackers tamper the hardware or software at its source or when it is in transit.
- Examples of distribution attacks include backdoors created by software or hardware vendors at the time of manufacture.
- Attackers leverage these backdoors to gain unauthorized access to the target information, systems, or network.
    - Modification of software or hardware during production
    - Modification of software or hardware during distribution

Thank You!

Kashif Ali

kashif.nth@aup.edu.pk