SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107

An Autonomous Institution

Accredited by NBA – AICTE and Accredited by NAAC – UGC with 'A' Grade
Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING-IoT Including CS & BCT

COURSE NAME :19SB701 PATTERN RECOGNITION TECHNIQUES IN CYBER CRIME

IV YEAR / VII SEMESTER

Unit V- **CYBER CRIME**

Topic :Understanding Network Intrusions and Attacks.

Network Intrusion

A **network intrusion** is any unauthorized access or breach of a network by malicious actors. These intrusions can compromise the confidentiality, integrity, and availability of data, leading to data theft, service disruptions, or even full system compromise.

Types of Network Intrusions:

- **External Intrusions**: Attacks initiated from outside the network, typically by hackers who breach firewalls and other security barriers.
- **Internal Intrusions**: Attacks originating from within the network by employees, contractors, or other insiders with some level of access.
- **Active Intrusions**: Where attackers alter or damage data within the network after gaining access.
- **Passive Intrusions**: The attacker monitors network traffic and collects information without altering any data.

Common Indicators of Intrusion:

- Unexpected system behaviors (e.g., unexplained slowdowns).
- Unusual login times or locations.
- Abnormal traffic patterns.
- Unaccounted changes in file configurations.
- Unexplained installation of new programs or software.

Network Attack

A **network attack** is an attempt to gain unauthorized access to a network with the intention of stealing data, disrupting services, or causing damage. Unlike an intrusion, which is about unauthorized access, an attack may involve multiple methods to damage, disrupt, or control the network.

Key Types of Network Attacks:

1.Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks:

1. **DoS Attack**: The attacker floods a network resource (like a website or server) with excessive traffic, rendering it unavailable to legitimate users.
2. **DDoS Attack**: A more sophisticated form of DoS, where multiple compromised systems (often called a botnet) attack the target simultaneously, overwhelming it with traffic.

2.Impact: Service downtime, reputational damage, and financial losses.

Man-in-the-Middle (MitM) Attacks:

•In a MitM attack, the attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other.

•This allows the attacker to steal sensitive information (like login credentials or financial information) or inject malicious content into the conversation.

Phishing and Spear Phishing:

- **Phishing**: The attacker sends fraudulent communications (usually emails) that appear to come from a trusted source. The goal is to steal sensitive information like usernames, passwords, or credit card details.

- **Spear Phishing**: A targeted form of phishing where specific individuals or organizations are attacked, often using personal information to appear more convincing.

SQL Injection:

An attacker exploits vulnerabilities in a web application by injecting malicious SQL statements into input fields. This can lead to unauthorized access to the database, allowing the attacker to read, modify, or delete data.

Brute Force Attacks:

The attacker attempts to gain access to accounts or systems by systematically trying every possible combination of passwords or encryption keys until the correct one is found.

Ransomware: A type of malware where the attacker encrypts a victim's files and demands a ransom (often in cryptocurrency) to restore access.

Zero-Day Exploits: Attacks that exploit vulnerabilities in software or hardware that are unknown to the vendor and, thus, have no patches or fixes available. These are highly dangerous because they target weaknesses that defenders cannot anticipate.

Spoofing:

•**IP Spoofing**: The attacker falsifies the source IP address to impersonate another system.

•**DNS Spoofing**: Manipulating DNS records to redirect traffic from legitimate sites to malicious ones.

•**Email Spoofing**: Faking the sender's email address to trick recipients into believing they are receiving messages from trusted sources.

How Network Intrusions and Attacks are Carried Out:

Attackers use various techniques and tools to intrude upon and attack networks. Here are some common methods:

- **Social Engineering**: Manipulating individuals into divulging confidential information (like phishing, baiting, or pretexting).
- **Exploiting Vulnerabilities**: Attackers often scan for known vulnerabilities in systems or software to gain access (e.g., outdated software with known bugs).
- **Malware**: Malicious software like viruses, worms, trojans, and spyware that are designed to damage or gain unauthorized access to systems.
- **Network Sniffing**: Attackers can use tools like Wireshark or tcpdump to capture unencrypted network traffic, potentially exposing sensitive information like passwords.
- **Password Cracking**: Tools like John the Ripper or Hashcat are used to crack weak or poorly secured passwords.
- **Backdoors**: Attackers often install backdoor programs, allowing them persistent access to the compromised system in the future.

Defending Against Network Intrusions and Attacks

Protecting against network intrusions and attacks requires a multi-layered approach:

1. Firewalls and IDS/IPS:

- **Firewalls**: Act as barriers between trusted internal networks and untrusted external ones. They filter traffic based on predefined security rules.
- **Intrusion Detection Systems (IDS)**: Monitor network traffic for suspicious activity and generate alerts.
- **Intrusion Prevention Systems (IPS)**: Take IDS a step further by actively blocking detected threats.

2. Encryption:

•Encrypting data (both in transit and at rest) ensures that even if it is intercepted, it cannot be read without the proper decryption key. VPNs (Virtual Private Networks) are commonly used to encrypt network traffic.

3. Strong Authentication:

•Enforce strong password policies, multi-factor authentication (MFA), and use security tokens to prevent unauthorized access.

4. Regular Patching:

•Ensure that all systems and software are updated regularly to patch known vulnerabilities. This limits the exposure to zero-day exploits and other vulnerabilities.

5. Network Segmentation:

•Dividing a network into segments limits the damage an attacker can do if they infiltrate one part of the network. Sensitive data and critical services should be isolated from less secure areas of the network.

6. Security Awareness Training:

•Educating employees on recognizing phishing attempts, social engineering attacks, and suspicious activities is essential for preventing human error-based intrusions.

7. Incident Response Plan:

•Organizations should have a defined plan for responding to network intrusions, including how to identify, contain, and remediate attacks.

Tools for Monitoring and Preventing Intrusions

- **Wireshark**: A powerful network protocol analyzer that helps in monitoring and troubleshooting networks.
- **Snort**: An open-source intrusion detection and prevention system (IDPS).
- **Nmap**: A network scanning tool that can identify open ports and potential vulnerabilities on systems.
- **OSSEC**: A free, open-source host-based intrusion detection system that monitors system files for unauthorized changes.

Any Query????

Thank you……