Chapter2

Access Control

Access control refers to any administrative policy, organizational procedure, software, or physical mechanism used to regulate who is permitted to access system resources. Its primary roles include:

- **Granting or Restricting Access**: Allowing authorized individuals to access resources while denying access to unauthorized users.
- **Monitoring Attempts**: Logging successful and unsuccessful access attempts.
- **User Identification**: Identifying who is attempting to access resources.
- **Authorization**: Verifying whether a user has the appropriate permissions to access resources.

Monitoring

Monitoring involves using software to hold users accountable for their actions within a system and to detect unauthorized or abnormal activities. Its key aspects are:

Importance of Monitoring:

- **Detecting Malicious Activities**: Identifying unauthorized access or intrusion attempts.
- **Event Analysis**: Reconstructing the timeline of events.
- **Providing Evidence**: Collecting data for legal or forensic investigations.
- **Problem Reporting**: Analyzing and understanding system failures.

Handling Log Files:

- **Data Volume Challenge**: Managing large volumes of collected data.
- **Data Reduction**: Using data mining tools to extract relevant information from massive datasets.
- **Real-Time Detection**: Employing Intrusion Detection Systems (IDS) for instant analysis and alerting.

Accountability

Accountability ensures that user and system activities are logged and traceable.

Key Measures:

1. **Audit Trails**:
    - Recording significant events in logs, such as user activities, system failures, and potential attacks.
2. **System Health Analysis**:
    - Logs help identify system failures caused by:

        - Faulty programs.
        - Corrupted drivers.
        - Intrusion attempts.
    - Logs also aid in event reconstruction to understand root causes of failures.

Monitoring Functions:

- **Attack Pattern Detection**: Identifying real-time attacks from internal or external sources.
- **Auditing**: Documenting all interactions between users and resources.
- **Strengthening Defenses**: Adding additional security layers based on monitoring data.

Importance of Monitoring in System Security

1. **Event Reconstruction**: Retracing the history of a breach or failure.
2. **Early Detection**: Quickly identifying unusual activities to prevent damage.
3. **Enhancing Security Policies**: Identifying and mitigating vulnerabilities.

Intrusion Detection (ID) and Intrusion Detection Systems (IDS)

Role of IDS:

IDS analyzes monitored data to detect potential attacks. It complements monitoring by offering:

- Real-time detection of threats.
- Insights into system failures and overall performance.

Sources of Attacks Detected by IDS:

- **External Communications**: Internet or partner networks.
- **Viruses and Malware**: Malicious codes targeting systems.
- **Internal User Activities**: Actions by trusted insiders attempting unauthorized tasks.
- **Unauthorized Access Attempts**: Including those from trusted sources.

IDS Response Types:

1. **Active Response**: Directly countering malicious activities, such as blocking suspicious traffic.
2. **Passive Response**: Logging attack details and alerting administrators.
3. **Hybrid Response**: Combining active and passive measures.

Capabilities of IDS:

- **Monitor Suspicious Activities**: Detecting spoofed traffic and policy violations.
- **Send Alerts**: Through notifications, emails, or logs.

- **Stop Attacks**: Actions include blocking ports, disabling segments, or removing suspicious packets.

IDS vs. Firewall:

- **IDS**: Focuses on detection.
- **Firewall**: Focuses on prevention.
- Both require support from physical restrictions and logical access controls.

Actions After Detecting Intrusion

- **Containment**: Preventing the threat from spreading.
- **Rebuilding Systems**: Restoring compromised systems.
- **Updating Policies**: Revising access control lists, service settings, and user accounts.

IDS Categories

1. **Host-Based IDS (HIDS)**:
    - Monitors activities on individual devices, focusing on system files and processes.
    - **Advantages**: High accuracy and detailed insights.
    - **Disadvantages**:
        - Cannot detect network-based attacks.
        - Consumes host resources.
        - Requires complex management on each device.
2. **Network-Based IDS (NIDS)**:
    - Monitors an entire network by analyzing packets.
    - **Advantages**:
        - Wide coverage.
        - Operates in stealth mode, undetected by attackers.
        - Minimal impact on device performance.
    - **Disadvantages**:
        - Cannot analyze encrypted data.
        - Struggles with high network loads.
        - Provides limited information about affected systems or files.

Intrusion Detection Techniques

1. **Knowledge-Based Detection** (Signature-Based):
    - Uses a database of known attack signatures.
    - **Advantages**: Effective against known threats.
    - **Disadvantages**: Cannot detect new or modified attacks; requires frequent updates.
2. **Behavior-Based Detection** (Statistical or Heuristic):
    - Learns normal system behavior and detects deviations.
    - **Advantages**: Detects new and unknown threats.
    - **Disadvantages**: Generates false positives and requires time to learn normal behaviors.

Types of Detected Attacks:

1. **Network Attacks**:
    - Examples: Denial of Service (DoS) attacks or exploitation of vulnerabilities.
2. **Host Attacks**:
    - Examples: Unauthorized access to files or processes.
3. **Protocol-Based Attacks**:
    - Examples: Identifying the use of protocols beyond allowed boundaries.

Advantages and Recommendations for IDS

- Both HIDS (Host-based Intrusion Detection System) and NIDS (Network-based Intrusion Detection System) have unique advantages and drawbacks, making each more effective depending on the scenario.
- Combining both systems provides a comprehensive protection framework.
- For optimal performance, signatures should be regularly updated, and behavior-based systems should be implemented to address emerging threats.

IDS-Related Tools:

These tools enhance the effectiveness of IDS by improving performance and reducing false alarms.

1. Honey Pots

- **Definition**: Decoy systems or networks designed to appear real but are entirely fake.
- **Purpose**: To attract attackers and retain them for information gathering.
- **Usage**:

    - Records malicious activities.
    - Helps security teams understand the nature of attacks and identify attackers.
- **Features**:
    - Effective in data collection as attackers stay engaged longer, enabling detailed analysis.

---

2. Padded Cells

- **Definition**: Similar to Honey Pots but isolate attackers once detected by the IDS.
- **Mechanism**:
    - The attacker is automatically redirected to a fake environment mimicking the real network.
    - **Environment Characteristics**:
        - Attackers cannot perform malicious activities.
        - Sensitive data remains inaccessible.
- **Features**:
    - **Attack Isolation**: Tracks attackers without alerting them.
    - **Fake Data Presentation**: Keeps attackers engaged for further analysis.

---

3. Vulnerability Scanners

- **Definition**: Tools for scanning systems to identify known vulnerabilities.
- **Mechanism**:
    - Analyzes the system and provides detailed reports on areas needing security improvements.
    - Reports include recommendations for patches and security settings adjustments.
- **Features**:
    - **Reduces False Alarms**: Helps IDS differentiate normal activities from real threats.
    - **Enhances Security**: Fixes vulnerabilities promptly.
- **Challenges**: Requires regular updates to vulnerability databases.

---

4. Intrusion Prevention Systems (IPS)

- **Definition**: Extends IDS functionality by actively preventing attacks.
- **Examples**: Blocking unauthorized connection attempts or illegal traffic patterns.

- **Types**: Similar to IDS classifications: Host-Based IPS, Network-Based IPS, Behavior-Based IPS, and Signature-Based IPS.
- **Features**:
    - Can analyze high-level application protocols to detect and stop attacks.

---

5. Penetration Testing

- **Definition**: Simulating real attacks to test the security environment.
- **Mechanism**:
    - Attempts to exploit systems using all available means.
    - Often conducted by external consultants to ensure unbiased results.
- **Purpose**:
    - Identifies all exploitable vulnerabilities in the system.
    - Implements corrective measures before exploitation.
- **Tools**:
    - Open-source: Metasploit.
    - Commercial: Core IMPACT.
- **Best Practices**:
    - Obtain prior management approval.
    - Ensure no harm is caused during the tests.

Summary Table of IDS Tools:

Feature	Honey Pots	Padded Cells	Vulnerability Scanners	IPS	Penetration Testing
Purpose	Attract attackers	Isolate attackers	Detect vulnerabilities	Actively prevent attacks	Test system defenses
Access	Allows malicious activity	Prevents malicious actions	Identifies vulnerabilities without allowing harm	Prevents and mitigates attacks	Executes attacks to analyze systems
Detection	Logs and analyzes attacks	Isolates ongoing attacks	Identifies vulnerabilities	Detects and stops real-time attacks	Identifies flaws through simulation
Features	Captures attacker interest	Provides isolated environments	Generates detailed security reports	Analyzes traffic to detect threats	Simulates real-world attacks
Challenges	Difficulty in identifying attackers	May be disconnected from real networks	Requires regular database updates	May generate false alarms if outdated	Potential harm if poorly managed

---

Attack Methods

Common attack methods include:

1. **Brute-Force and Dictionary Attacks**
    - **Brute-Force**: Systematically guesses all possible combinations of passwords.
        - **Prevention**: Use complex passwords, strong encryption, and multi-factor authentication.
    - **Dictionary**: Utilizes precompiled lists of common passwords.
        - **Prevention**: Restrict access to password files and monitor suspicious activities.
2. **Denial-of-Service (DoS) Attacks**
    - Overwhelms systems with massive requests to prevent legitimate access.
    - Includes Distributed (DDoS) and Reflection (DRDoS) variants.
    - **Prevention**: Firewalls, advanced threat detection systems, and resource optimization.
3. **Man-in-the-Middle Attacks**
    - Intercepts communications to read or alter transmitted data.
    - **Prevention**: Use encrypted protocols (e.g., TLS) and mutual authentication.
4. **Flooding Attacks**
    - Includes SYN Flood, Smurf, and Ping of Death.
    - **Prevention**: Disable broadcast traffic, limit ICMP packet size, and restrict external traffic.
5. **Botnets**
    - Networks of compromised devices used for large-scale attacks.
    - **Prevention**: Regular updates, monitoring abnormal patterns, and deploying security measures.

Access Control Compensations

Compensations mitigate or recover from access control violations:

- **Backups**: Quickly restore lost or corrupted data.
- **RAID Systems**: Enhance fault tolerance by distributing data across multiple disks.
- **Fault Tolerance**: Ensures system resilience with failover mechanisms.
- **Business Continuity Planning**: Includes protocols to recover from disruptions.
- **Insurance**: Protects critical assets financially in case of major breaches.

Comparison of Attack Types

Attribute	Brute-Force and Dictionary Attacks	Denial-of-Service (DoS) Attacks	Man-in-the-Middle (MITM) Attacks	Flooding Attacks	Botnets	Spoofing Attacks
Purpose	Cracking passwords using all possibilities or a pre-set list	Denial of legitimate access by flooding requests	Intercepting and modifying data between endpoints	Flooding the system with massive data packets	Using compromised devices to launch large-scale attacks	Impersonating another identity for infiltration
Objective	Crack passwords and gain unauthorized access	Prevent system response or cause downtime	Intercept or modify exchanged data	Overload servers or networks with traffic	Disrupt systems or exploit compromised devices	Spoof source address or sender identity
Preventive Measures	Strong passwords, encryption, two-factor authentication	Firewalls, IDS/IPS, performance optimization	Encryption (e.g., TLS), identity verification	Disable broadcasting, restrict ICMP, detection systems	Regular updates, network monitoring	Encryption and mutual identity verification
Tools Used	Brute force tools (e.g., Hydra), dictionary tools (e.g., John the Ripper)	DDoS tools (e.g., LOIC), botnet software	Data capturing tools (e.g., Wireshark), proxies	Flooding tools (e.g., LOIC) or botnets	Botnet control software (e.g., Zeus)	Spoofing tools (e.g., Hping, Scapy)
Impact	Password theft or unauthorized access	System downtime or degraded service access	Data interception or modification	Service disruption or system downtime	System disruption or exploitation of devices	Conceal attacker's identity and infiltrate
Affected Systems	Databases, login systems	Servers, networks	Networks, connected systems	Servers, networks, personal devices	Compromised networks and servers	Systems failing to verify sender identity