CRYPTOGRAPHY AND INFORMATION SECURITY

IT 3203

LECTURE 27

By

Varsha Himthani

Assistant Professor (Selection Grade)

Manipal University Jaipur

Intrusion Detection System (IDS)

Intrusion detection refers to the practice of monitoring a system or network for any unauthorized access or suspicious activity that may indicate an attack or a security breach. Intrusion detection systems (IDS) are designed to identify, alert, and possibly take action against these potential threats.

Types of IDS

1. Host-based Intrusion Detection System (HIDS):

- Installed on individual devices or hosts, such as servers or workstations.
- It monitors and analyzes activity occurring on the device, such as file changes, application logs, or system calls.
- It can detect and alert on signs of unauthorized access or tampering on the host.

2. Network-based Intrusion Detection System (NIDS):

- Monitors network traffic for signs of malicious activity or policy violations.
- It inspects data packets as they traverse the network and looks for known attack patterns or anomalies that could indicate a security threat.

IDS Classification

1. **Statistical Anomaly-based IDS**
2. **Rule-based (Signature-based) IDS**

Statistical Anomaly-based IDS

- It relies on building a model of what constitutes "normal" behavior for a system or network based on historical data.
- The IDS continuously monitors the system or network and compares real-time behavior to the expected patterns.
- If the system detects deviations or anomalies from the established baseline, it raises an alert. These anomalies could include sudden spikes in traffic, unusual access patterns, or other out-of-the-ordinary behaviors.
- The key advantage of anomaly-based detection is its ability to detect previously unknown or novel attacks that may not match known patterns.
- However, anomaly-based IDS can be prone to false positives because normal behavior can sometimes change over time. Care must be taken to ensure that the system adapts to changing patterns while still maintaining a robust baseline.

Rule Based (Signature based) IDS

- Operates by using a database of known attack patterns or signatures. These signatures are based on characteristics of past attacks, such as specific packet sequences, known malicious IP addresses, or unusual combinations of activities.
- The IDS continuously monitors the system or network and compares the observed behavior to the signatures in its database. If it detects a match, it raises an alert indicating a potential attack.
- Rule-based IDS is effective at quickly identifying known attacks and has a low false positive rate for those attacks.
- However, its effectiveness is limited by the quality and comprehensiveness of its signature database. It may not detect novel or previously unseen attacks that do not match any known signatures.

Comparison

Detection Type: Anomaly-based IDS detects deviations from normal behavior, while rule-based IDS detects known attack patterns.

Flexibility: Anomaly-based IDS can potentially detect new or novel attacks, but it may produce false positives. Rule-based IDS is effective at detecting known attacks with lower false positives but may miss new threats.

Maintenance: Anomaly-based IDS requires maintaining an up-to-date model of normal behavior, while rule-based IDS requires updating the signature database with new threats.

Honeypots

- **Honeypot** is a network-attached system used as **a trap for cyber-attackers** to detect and study the tricks and types of attacks used by hackers.

- It acts as a potential target on the internet and informs the defenders about any unauthorized attempt to the information system.

- Honeypots are mostly used by large companies and organizations involved in cybersecurity. It helps cybersecurity researchers to learn about the different type of attacks used by attackers. It is suspected that even the cybercriminals use these honeypots to decoy researchers and spread wrong information

- The **cost of a honeypot** is generally **high** because it requires specialized skills and resources to implement a system such that it appears to provide an organization’s resources still preventing attacks at the backend and access to any production system.

- **Honeynet** is a combination of two or more honeypots on a network.

Types of Honeypots

Research Honeypots: These are set up by security researchers to gather information about attack methods, trends, and behaviors. They help improve threat intelligence and inform defensive strategies.

Production Honeypots: These are placed in real networks to enhance security by diverting attackers away from critical assets. They also help security teams observe the tactics and tools used by attackers in real-world scenarios.

How Honeypots Works

- **Decoy System:** A honeypot is designed to appear as an attractive target to potential attackers. It may resemble a database, web server, or other networked resource, complete with fabricated data and services.

- **Monitoring and Logging:** Once an attacker interacts with the honeypot, the system records and analyzes the attacker's activities, including the attack methods, commands, and tools used.

- **Alerts and Analysis:** When an attack occurs, the honeypot sends alerts to security teams, allowing them to respond quickly and investigate the attack. The data collected can be used for analysis and to improve security measures

Benefits of Honeypots

•**Threat Intelligence:** Honeypots provide valuable insights into attack trends, techniques, and emerging threats.

•**Attack Detection:** They help detect attacks that may go unnoticed by other security measures.

•**Reduced False Positives:** Since honeypots do not serve legitimate users, any interaction with them is likely to be malicious.

•**Diversion of Attacks:** Honeypots can divert attackers away from critical systems, providing additional protection for sensitive data.

Limitations of Honeypots

- **Limited Scope:** Honeypots are limited to monitoring interactions that occur on the decoy system and may not capture all types of attacks.

- **Sophisticated Attackers:** Experienced attackers may recognize honeypots and avoid them or manipulate them to mislead defenders.

- **Maintenance:** Honeypots require ongoing maintenance to ensure they remain believable and up-to-date with current attack methods.

Thank you