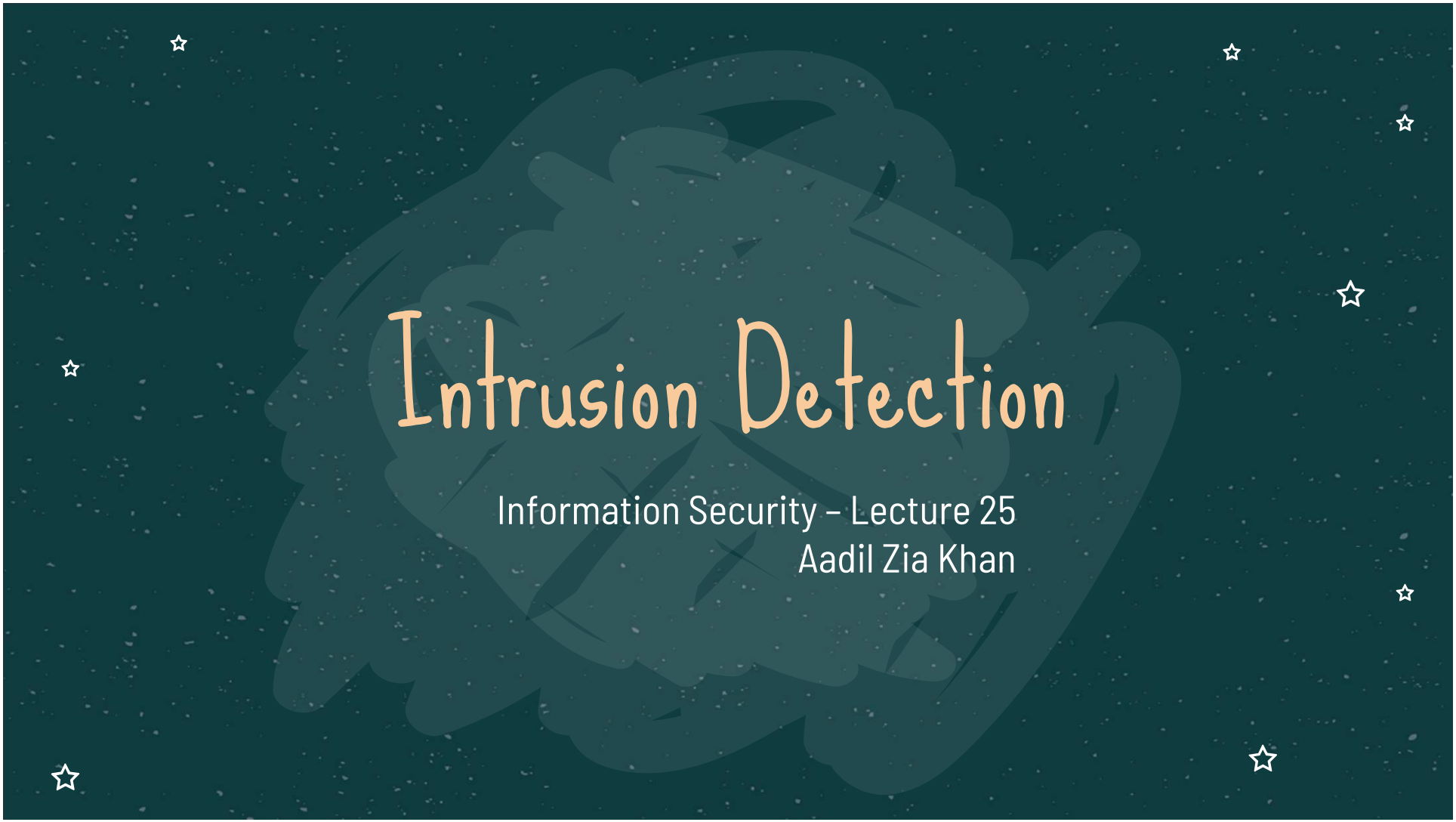
Intrusion Detection
Information Security – Lecture 25
Aadil Zia Khan

Overview

Intrusion: Unauthorized act of bypassing the security mechanisms of a system.

Intrusion detection: A hardware or software function that gathers and analyzes information from various areas within a computer or a network to identify possible security intrusions.

Intrusion Detection System - IDS

Sensors

Types of input to a sensor includes network packets, log files, and system call traces.

Sensors collect and forward this information to the analyzer.

Analyzers

Analyzers receive input from one or more sensors or from other analyzers to determine if an intrusion has occurred.

The analyzer may also provide guidance about what actions to take as a result of the intrusion.

The sensor inputs may also be stored for future analysis and review in a storage or database component.

User Interface

The user interface enables a user to view output from the system or control the behavior of the system.

IDS Monitoring Categories

- Host-based IDS (HIDS): Monitors the characteristics of a single host and the events occurring within that host, such as process identifiers and the system calls they make, for evidence of suspicious activity.
- Network-based IDS (NIDS): Monitors network traffic for particular network segments or devices and analyzes network, transport, and application protocols to identify suspicious activity.

Requirements For An Effective IDS

- Run continually with minimal human supervision.
- Be fault tolerant in the sense that it must be able to recover from system crashes.
- Resist subversion - must be able to monitor itself and detect if it has been modified by an attacker.
- Impose a minimal overhead on the system where it is running.
- Be configurable according to the security policies of the system that is being monitored.
- Be able to adapt to changes in system and user behavior over time.
- Be able to scale to monitor a large number of hosts.
- Graceful degradation of service - if some components of the IDS fail, rest should continue to work.
- Allow dynamic reconfiguration; that is, the ability to reconfigure the IDS without having to restart it.

Analysis Approaches

- Anomaly detection
  - Involves the collection of data relating to the behavior of legitimate users over a period of time.
  - Then, current observed behavior is analyzed to determine whether this behavior is that of a legitimate user or an intruder.

- Signature or Heuristic detection
  - Uses a set of known malicious data patterns (signatures) or attack rules (heuristics) that are compared with current behavior to decide if it is that of an intruder.

Host-Based IDS

Specialized layer of security software added to vulnerable or sensitive systems; such as database servers and administrative systems

- Data Sources and Sensors
  - System call traces: A record of the sequence of systems calls by processes on a system
  - Audit (log file) records: A record of user activity
  - File integrity checksums: A periodic scan of critical files for changes from the desired baseline

Host-Based IDS

Problem???

Cant detect zero-day attacks that do not correspond to the known signatures or heuristic rules

- Signature or Heuristic Detection Techniques
  1. Use either a database of file signatures, which are patterns of data found in known malicious software, or heuristic rules that characterize known malicious behavior to identify intrusion

Host-Based IDS

- Anomaly Detection Techniques
  1. Compare observed sequences of system calls with sequences from the training phase to determines whether the sequence is normal or not
  2. Observe changes in usage pattern from the activity logs
  3. Compare checksums of files with a originals to identify modifications

Network-Based IDS

Special software to monitor traffic at selected points on a network in real time, or close to real time, to attempt to detect intrusion patterns.

- Data Sources and Sensors
  - Inline sensing: Sensor is inserted into a network segment so the packets that are monitored must pass through it – and maybe filtered if needed
  - Passive sensing: Monitors a copy of network traffic; the actual traffic does not pass through the device
    - More efficient than the inline sensor, because it does not add an extra handling step that contributes to packet delay

Network-Based IDS

- Anomaly Detection Techniques
  1. Denial-of-service: Identify either significantly increased packet traffic or connection attempts
  2. Scanning: Identify traffic that corresponds to transport layer (e.g., TCP and UDP port) scanning, and network layer (e.g., ICMP) scanning
  3. Worms: Identify applications using large amounts of bandwidth, or hosts communicating with each other that typically do not, or using ports that they normally do not use

Network-Based IDS

- Signature or Heuristic Detection Techniques
  1. Policy violations: Detect use of forbidden application protocols
  2. Unexpected application services: Determine if the activity on a transport connection is consistent with the expected application protocol and not some backdoor process running an unauthorized service
  3. Network layer reconnaissance: Analyze IPv4, IPv6, ICMP, traffic to observe spoofed IP addresses and illegal IP header values
  4. Transport layer reconnaissance: Analyze TCP and UDP traffic to observe unusual packet fragmentation, vulnerable ports, and TCP-specific attacks like SYN floods
  5. Application layer reconnaissance: Analyze commonly used application protocols' traffic looking for attack patterns that have been identified as targeting these protocols, like buffer overflows, password guessing, and malware transmission

Honeypots

- Honeypots are decoy systems that are designed to lure a potential attacker away from critical systems

- Honeypots are designed to:
  - Divert an attacker from accessing critical systems
  - Collect information about the attacker's activity
  - Encourage the attacker to stay on the system long enough for administrators to respond

slidesgo