Intrusion Detection Systems (IDS)

Prepared by:
Isra Brahim
Sarra Barkallah
Rana Elsherif

Revised by:
Dr. Abdelkarim Erradi

Outline

- Introduction
- Host-based IDS
- Network-based IDS
- Signature-based vs. Anomaly-based Detection
- Summary

Introduction

What is intrusion?

Intrusion is any unwanted or unauthorized interference into a network of an organization (usually with bad intentions) to collect data from these organizations such as the internal network structure and software systems and applications

What is Intrusion Detection?

Intrusion Detection is the act of detecting unwanted or inappropriate intrusions.

- Intrusion Detection Systems (IDS) is a tool that automate the detections of intrusions.
  2 IDS types:
  - Host-Based IDS (HIDS)
  - Network-Based IDS (NIDS)

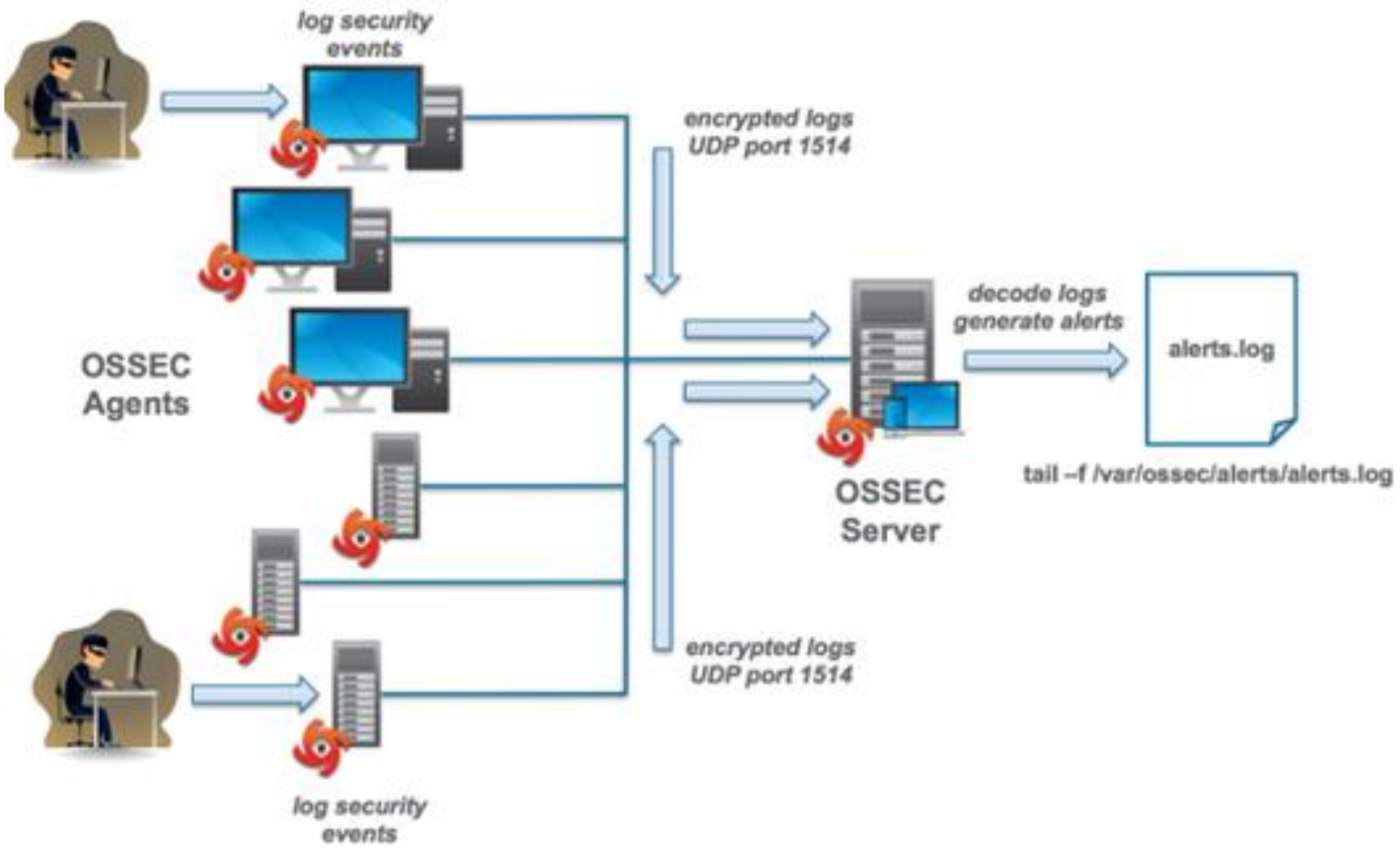
HIDS

What is HIDS?

- HIDS refers to detection of the malicious intrusions to a system on a single host.
- Uses a software-based agent on a host to monitor the activity of applications.
- HIDS detects intrusions using the traces or evidences that are left behind by intruders after performing a suspicious action in the system.

❖ HIDS with prevention techniques is called Host-based Intrusion Detection Prevention System (HIDPS)

HIDS Architecture (OSSEC)



Agents that *monitor* host activities

- Deployed on the most critical servers or all network nodes

Server (**Analyzer**)

- *analyze* and *detect* when something abnormal happens

HIDPS Security Capabilities

Logging capability

(Logs collected Monitoring data)

Detection capability

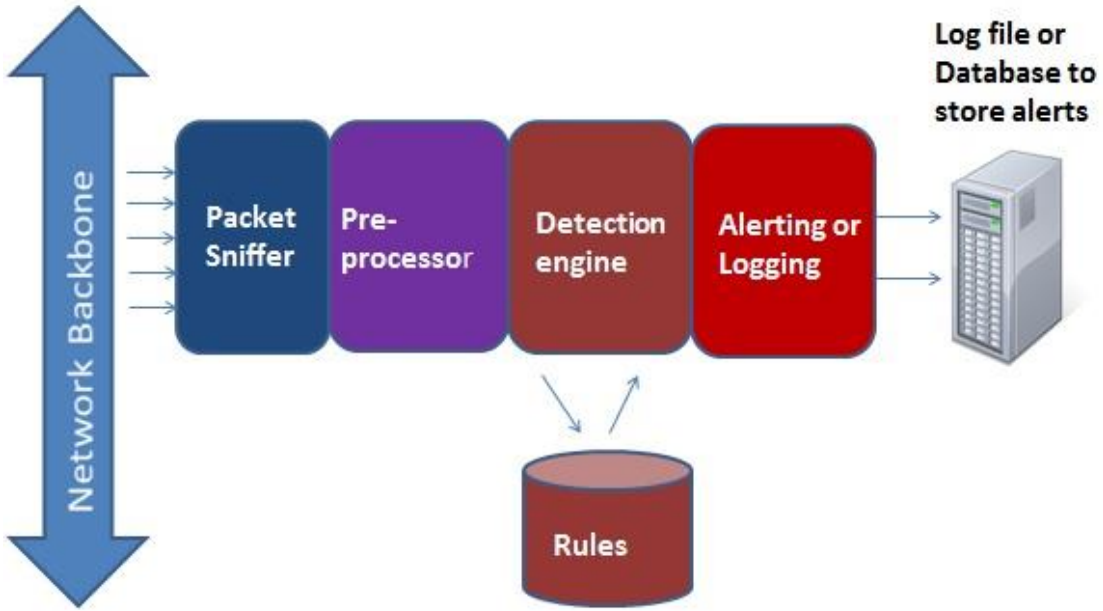
Analyze collected monitoring data to detect intrusions

Prevention capability

Stop unauthorized access and file modifications

NIDS

NIDS Architecture



- Monitors network traffic using sensors
  - **Inline Sensor**: Network traffic passes through it
  - **Passive Sensor**: Monitors copies of traffic
- Detects malicious activities and raises alerts
  - E.g., incoming traffic higher than normal

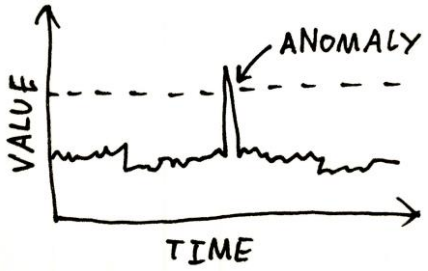
Signature-Based vs. Anomaly-Based Detection

There are mainly two approaches for detecting intrusions:

- **Signature** based detection techniques
- **Anomaly** based detection techniques

Signature Based detection

- A signature represents a **pattern** of a recognized **threat**
  - A **set of rules** that an IDS can use to detect an intrusive activity, such as a DoS attack
  - e.g., check character strings in a packet against database of known virus, attack strings
- IDS has a predefined **signatures** in a **signature database**
- IDS analyzes collected monitoring data and **compares** them with the set of known signatures. If there is a match an alert is raised.
- Highly **effective** for **known threats** but failed for unknown ones



Anomaly-Based detection

- Operates by comparing whether an activity is considered normal (usual) or anomalous based on some observed events.
- Anomaly-based technique learns and saves normal behavior of users, hosts , applications and network connections as profiles. These profiles are developed based on some behavioral attributes:
  - e.g. number failed login attempts for a host, number of e-mails sent by a user, the level of processor usage for a host.
  - These profiles are developed over a period of time by monitoring the characteristics of typical (usual) activity.
- A user/app/network behavior is compared with the predefined behavior, if it is in accordance then it is accepted, otherwise an alert is raised
  - e.g., a network profile shows that during typical workday hours, web activity involves 13% as an average of network bandwidth at the internet border. Then suddenly, a significantly more bandwidth than expected by this web activity was detected. This is considered as an anomaly.

Summary

- Host-based Intrusion Detection System (HIDS)
  - Uses agents to monitor the activities of a single host for suspicious activity
- Network-based Intrusion Detection System (NIDS)
  - Monitors network traffic (using inline or passive sensors) and analyzes network, transport, and application protocols to identify suspicious activity
- Three logic components in IDS
  - Sensors: collect data
  - Analyzers: determine if intrusion has occurred
  - User interface: view output or control system behavior
- HIDS and NIDS can use Signature-based and/or Anomaly-based techniques to detect intrusions
- Anomaly-based detection techniques are **more effective** than Signature-based in detecting unknow attacks