Intrusion Detection and Systems (IDS)

Prepared by:
Isra Brahim
Sarra Barkallah
Rana Elsherif

Supervised by:
Dr. Abdelkarim Erradi

Outline

- Introduction
- Host-based IDS Architecture
- Network-based IDS Architecture
- 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)

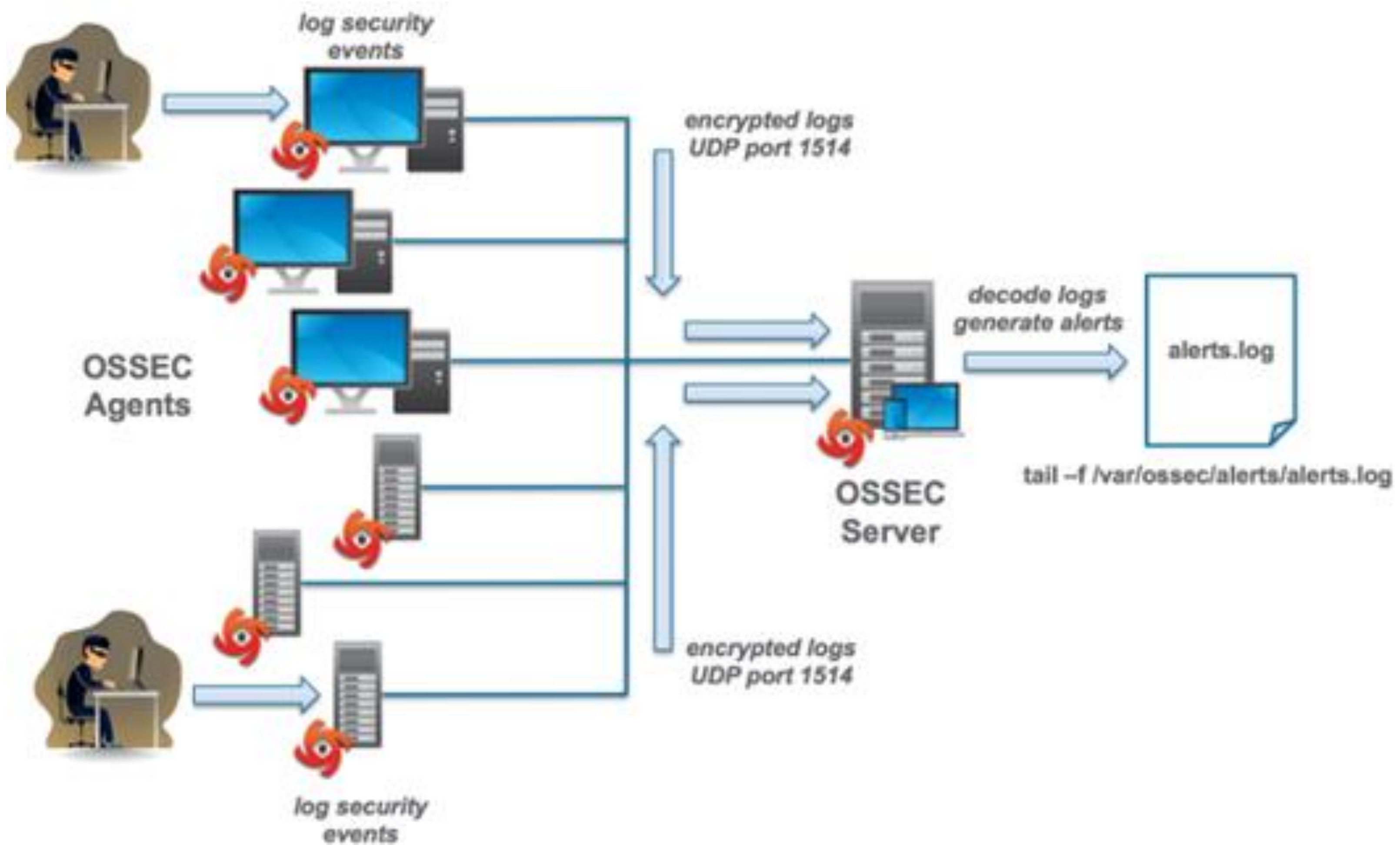
HIDS Architecture

What is HIDS?

- HIDS refers to detection of the malicious intrusions to a system on a single host.
- By deploying a software-based agent on a host device (server or an end device) to monitor the activity of applications.
- HIDS depend on the traces or evidences (e.g., tools used by intruders) that are left after performing a suspicious action in the system.

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

HIDS Architecture (OSSEC)


log security events
encrypted logs UDP port 1514
OSSEC Agents
decode logs generate alerts
alerts.log
tail –f /var/ossec/alerts/alerts.log
OSSEC Server
encrypted logs UDP port 1514
log security events

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

File system and applications monitoring to detect malware

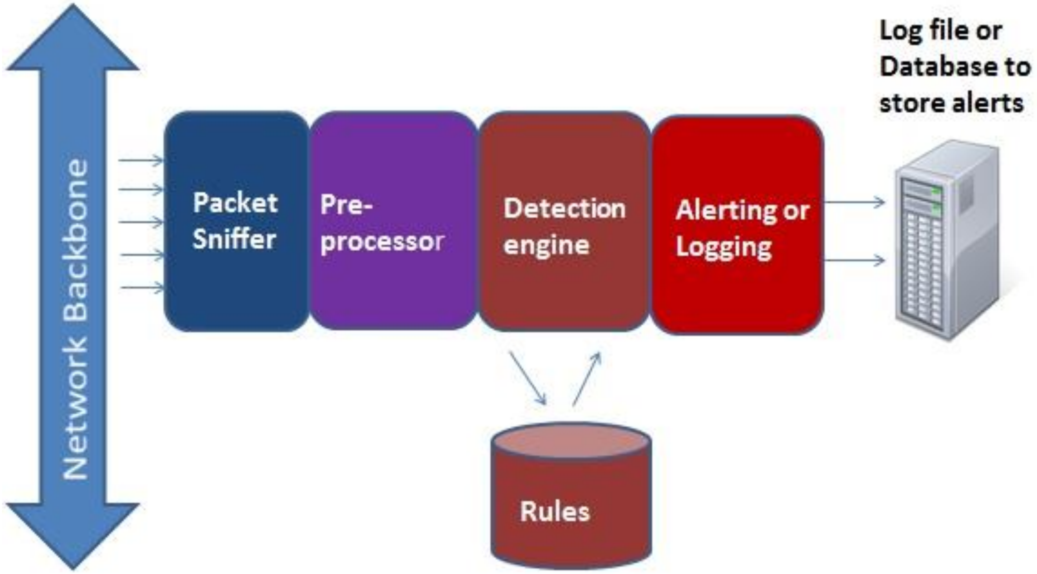
Prevention capability

Stop unauthorized access and file modifications

NIDS Architecture

NIDS Architecture

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



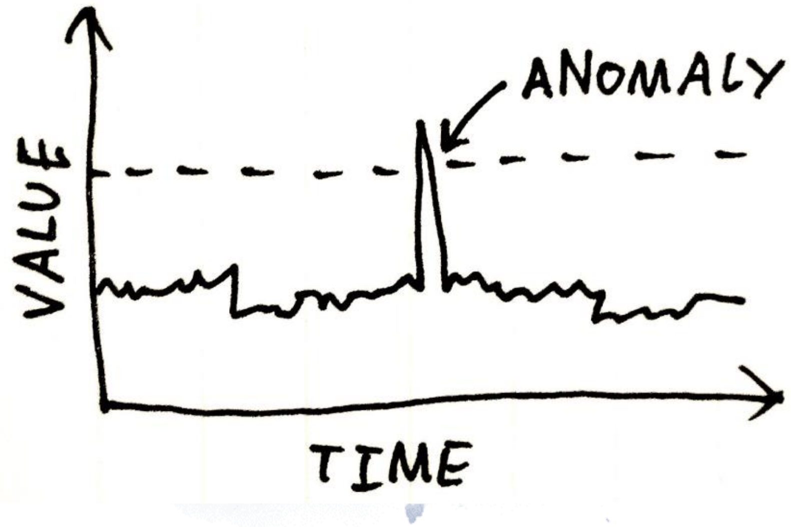
Signature-Based vs. Anomaly-Based Detection

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., byte sequences in network traffic from known malware
- Signature-Based technique initially **stores** some predefined **signature** in a **signature database**
- Analyses network data packets and **compare** them with the set of signature profiles **stored earlier** using a signature engine.
- If there is a match and 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 saves <u>normal behavior</u> of users, hosts , applications and network connections as profiles. These profiles are developed based on some behavioral attributes

  - e.g. number of login attempts that were failed 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 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

- HIDS can detect intrusions using agents deployed in a single host.
- OSSEC is a well-known free open source HIDS used for detecting intrusions.
- NIDS monitors network traffic using sensors (inline, passive) to detect malicious activities
- 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.