INTRUSION DETECTION SYSTEMS

SASHANK NARAIN

INTRUSION DETECTION SYSTEMS (IDS)

- **Detect intrusions** on systems and network activity
  - **Monitor user and system activity**
  - **Recognize known attack patterns** in network activity

- Two types
  - **Host-based Intrusion Detection Systems (HIDS)**
  - **Network-based Intrusion Detection Systems (NIDS)**

HOST-BASED IDS

- **Host-based Intrusion Detection Systems (HIDS)**
  - **Assess integrity** of critical system and data files
  - Check for **file system changes** compared to a database of known good state
  - E.g., **AIDE**, Tripwire, Fail2Ban

SETUP FOR HOST-BASED IDS

- Step 1 – **create a database of system / sensitive files** in a known good state
  - **Include hashes, permissions and timestamps** of the files
  - Store the database in a known **secure location**
  - **MUST ensure that this database is not tampered**
- Step 2 – **create an automated task to check filesystem** regularly against database
  - Load database from the known secure location
  - **System alerts of changes** to file contents, permissions or timestamps
- Step 3 – **perform analysis to determine cause** of the changes and repeat step 1, if necessary

HOST-BASED IDS DEMO

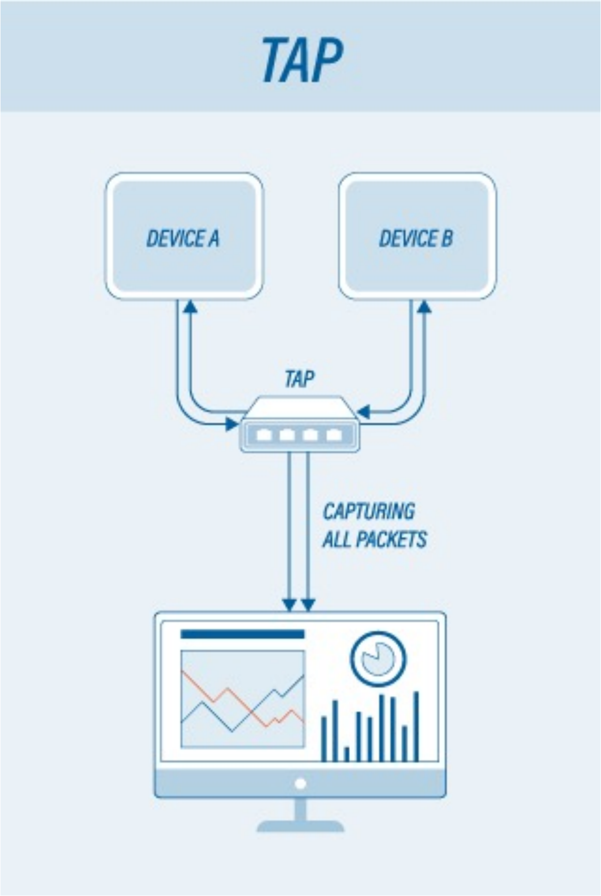
- **Popular** Host-based Intrusion Detection Systems -
  - Tripwire (commercial)
  - AIDE (open-source)

AIDE Demo

NETWORK-BASED IDS

- **Network Intrusion Detection Systems (NIDS)**
  - **Recognize known attack patterns** in network activity
  - **Identify abnormal activity** through statistical analysis
  - **Manage audit trails** and **highlight policy violations**
  - E.g., **Snort**, Suricata, OSSEC, SecurityOnion

SIMPLE SETUP FOR NETWORK-BASED IDS



Source: https://insights.profitab.com/

TYPES OF NETWORK-BASED IDS

- Detection methods
  - Signature-based
  - Heuristic
- Capabilities
  - Passive
  - Active (known as Intrusion Prevention Systems (IPS))

NETWORK-BASED IDS DEMO

Snort Demo