Module Flow

*So important chapter

- IDS vs IPS
- Signature vs anomaly detection
- HIDS vs NIDS
- Active vs Pasive IDS
- False +ve / False -ve
- IDS Placement
- Snort

1. Understand Different Types of Network Segmentation
2. Understand Different Types of Firewalls and their Role
3. **Understand Different Types of IDS/IPS and their Role**
4. Understand Different Types of Honeypots
5. Understand Different Types of Proxy Servers and their Benefits
6. Discuss Fundamentals of VPN and its importance in Network Security
7. Discuss Security Incident and Event Management (SIEM)
8. Discuss User Behavior Analytics (UBA)
9. Understand Various Antivirus/Anti-malware Software

Intrusion Detection and Prevention System (IDS/IPS)

Stands for

01

An intrusion detection and prevention system (IDS/IPS) is a network security appliance that inspects all inbound and outbound network traffic for suspicious patterns that might indicate a network or system security breach

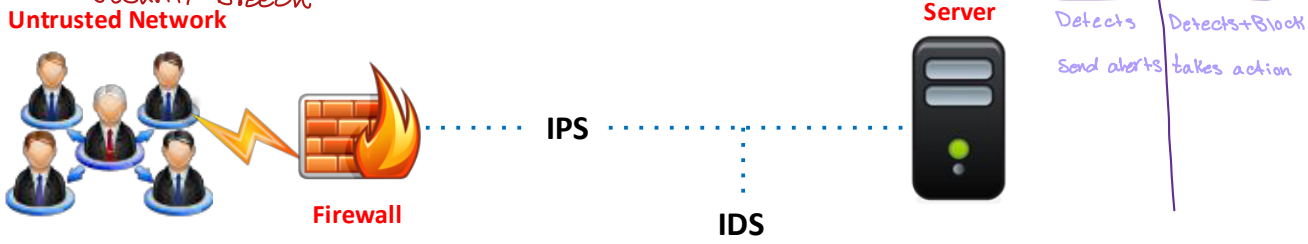
- intrusion
- Attack
- Security breech

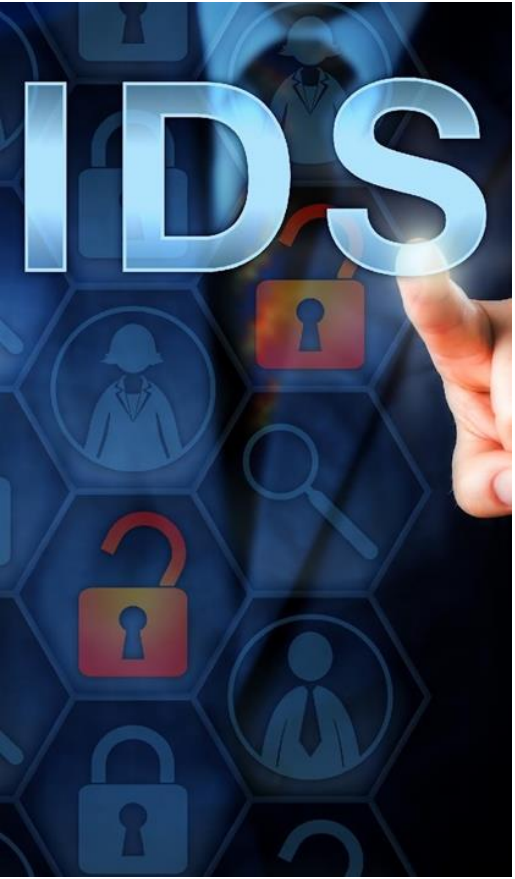
02

If found, the IDS will alert the administrator about the suspicious activities

03

IDS checks the network traffic for signatures that match known intrusion patterns and triggers an alarm when a match is found





How does an IDS Work?

traffic enters

Internet

Router

Firewall

IDS

Enterprise Network

Switch

IDS Preprocessor

Signature File Comparison

Signature File Database

Cisco log sever

Matched?

Anomaly Detection

Alarm notifies admin and packet can be dropped

Matched?

Action Rule

Alarm

Connections are cut down from that IP source

Stateful Protocol Analysis

Matched?

Packet is dropped

Role of an IDS in Network Defense

*Firewall filters traffic
IDS analyze traffic deeply

—IDS helps detect attacks that bypass firewalls

- An IDS works from inside the network, unlike a firewall which only looks **outside** the network for intrusions
- An IDS is placed behind the firewall, inspecting all the traffic, looking for **heuristics** and a **pattern** match for intrusions

How an IDS Detects an Intrusion?

3 methods

Signature Recognition

Signature recognition, also known as misuse detection, tries to **identify events** that indicate an abuse of a system or network resource

look for: Known attack patterns

ex: if Packet matches SQL injection signature, IDS alerts admin

Anomaly Detection

It detects the **intrusion based** on the fixed behavioral characteristics of the users and components in a computer system

IDS learns: Normal network behavior, then detects deviations

ex: Sudden huge bandwidth usage

Protocol Anomaly Detection

In this type of detection, models are built to explore **anomalies** in the way in which vendors deploy the **TCP/IP specification**

IDS Capabilities

- IDS provides an additional layer of security to the network under the **defense-in-depth** principle
- IDS does several things that basic **firewalls** cannot do
- IDS helps minimize the chance of **missing security threats** that could come from firewall evasions

IDS/IPS Functions

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Recognizing typical attack patterns
- Analyzing abnormal activity patterns
- Tracking user policy violations

IDS/IPS Limitations: What an IDS/IPS is NOT?

IDS/IPS cannot act as or replacement of

- Network Logging Systems
- Vulnerability Assessment Tools
- Antivirus Products
- Cryptographic Systems

IDS/IPS Security Concerns

- Improper IDS/IPS configuration and management will make an IDS/IPS **ineffective**
- IDS/IPS deployment should be done with careful planning, preparation, prototyping, testing, and specialized training

Common Mistakes in IDS/IPS Configuration

- ✓ Deploying an IDS in a location where it **does not see** all the network traffic
- ✓ Frequently **ignoring** the **alerts** generated by the IDS
- ✓ Not having the proper **response policy** and the best possible solutions to deal with an event
- ✓ Not fine-tuning the IDS for **false negatives** and **false positives**
- ✓ Not updating the IDS with the **latest new signatures** from the vendor
- ✓ Only monitoring **inbound connections**

General Indications of Intrusions

File System Intrusions

- The presence of new or unfamiliar files, or programs
- Changes in file permissions
- Unexplained changes in a file's size
- Rogue files on the system that do not correspond to the master list of signed files
- Missing files

Network Intrusions

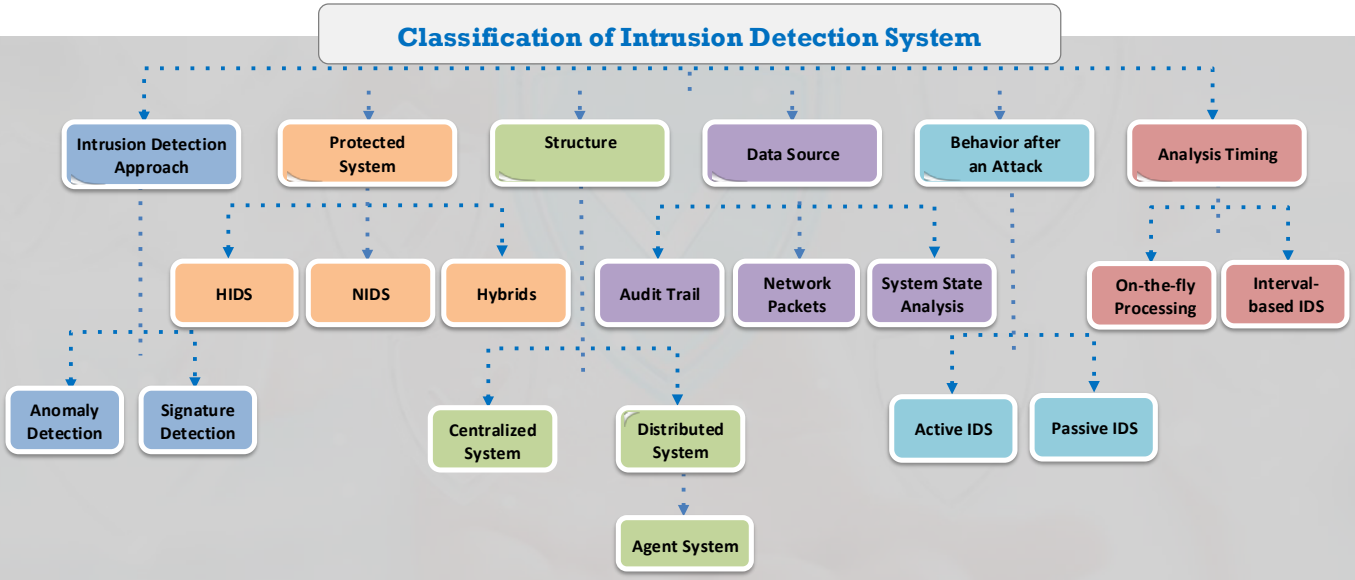
- Repeated probes of the available services on your machines
- Connections from unusual locations
- Repeated login attempts from remote hosts
- A sudden influx of log data

System Intrusions

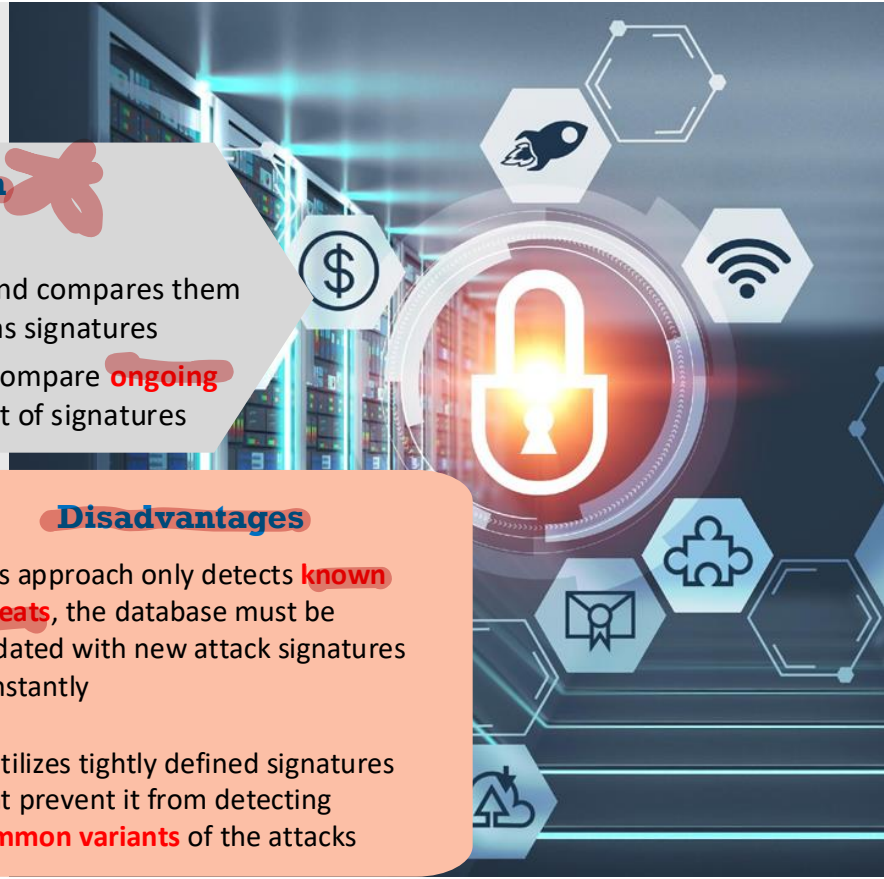
- Short or incomplete logs
- Unusually slow system performance
- Missing logs or logs with incorrect permissions or ownership
- Modifications to system software and configuration files
- Unusual graphic displays or text messages
- Gaps in system accounting
- System crashes or reboots
- Unfamiliar processes

IDS Classification

An IDS is **classified** based on an approach, protected system, structure, data source, behavior, and time analysis



Approach-based IDS



Signature-Based Detection

- Known as misuse detection
- Monitors patterns of data packets in the network and compares them to pre-configured network attack patterns, known as signatures
- This method uses string comparison operations to compare ongoing activity, such as a packet or a log entry, against a list of signatures

Advantages

- It detects attacks with minimal false alarms
- It can quickly identify the use of a specific tool or technique
- It assists administrators to quickly track any potential security issues and initiate incident handling procedures

Disadvantages

- This approach only detects known threats, the database must be updated with new attack signatures constantly
- It utilizes tightly defined signatures that prevent it from detecting common variants of the attacks

Approach-based IDS (Cont'd)

Anomaly-based Detection

- In this approach, alarms for **anomalous** activities are generated by evaluating network patterns such as what sort of bandwidth is used, what protocols are used, and what ports and which devices are connected to each other
- An IDS monitors the typical activity for a particular time interval and then builds the **statistics** for the network traffic
- For example: anomaly-based IDS monitors activities for normal Internet bandwidth usage, failed logon attempts, processor utilization levels, etc.

Advantages

- ✓ An anomaly-based IDS identifies **abnormal** behavior in the network and detects the symptoms for attacks without any clear details
- ✓ Information acquired by anomaly detectors is further used to define the signatures for **misuse detectors**

Disadvantages

- ✓ The rate of generating **false alarms** is high due to unpredictable behavior of users and networks
- ✓ The need to create an **extensive set of system events** in order to characterize normal behavior patterns

Approach-based IDS (Cont'd)

This method **compares** observed events with predetermined profiles based on accepted definitions of benign activity for each protocol to identify any deviations of the protocol state

It also detects variations in command length, minimum/maximum values for **attributes** and other **potential anomalies**

Stateful Protocol Analysis

It can identify unpredictable sequences of commands. For example, it can identify activities such as issuing the same commands repeatedly or arbitrary commands being used

For any protocol performing **authentication**, the IDS/IPS will keep track of the authenticator being used for each session and will record the authenticator involved in the suspicious activity

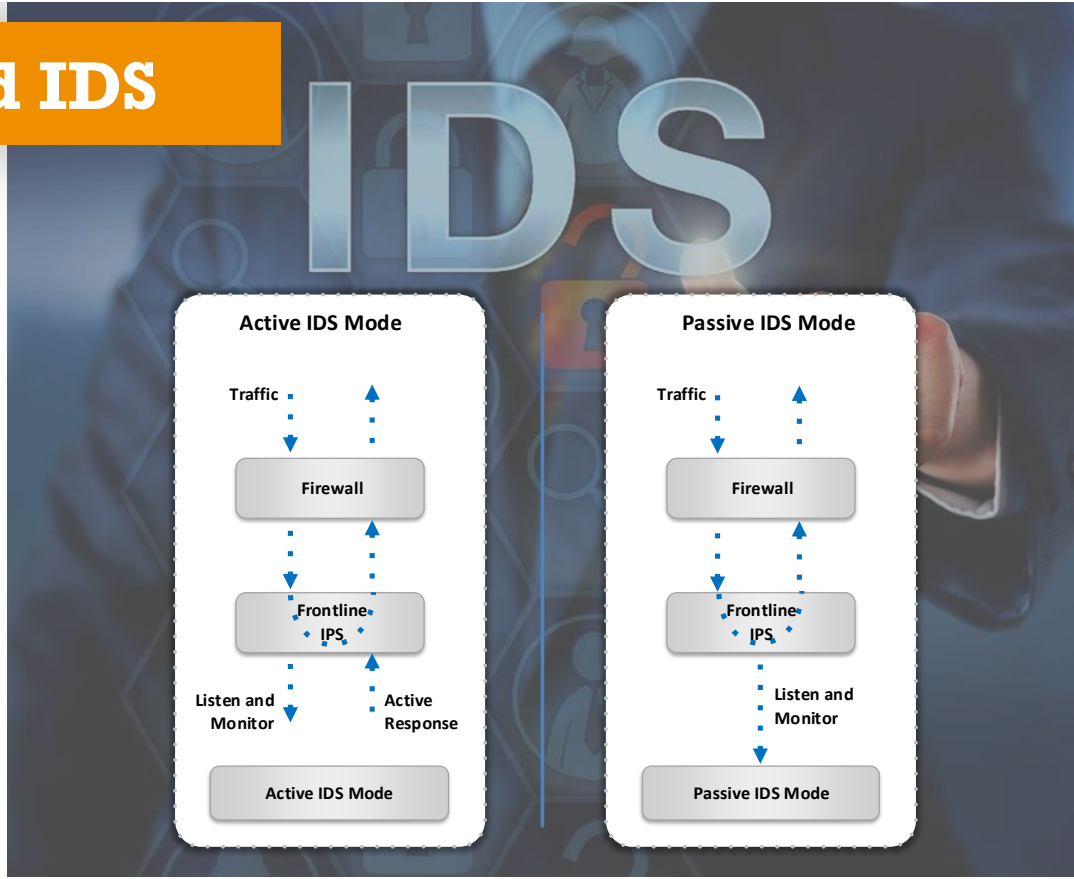
Anomaly and Misuse Detection Systems

Misuse Detection System

Anomaly Detection System

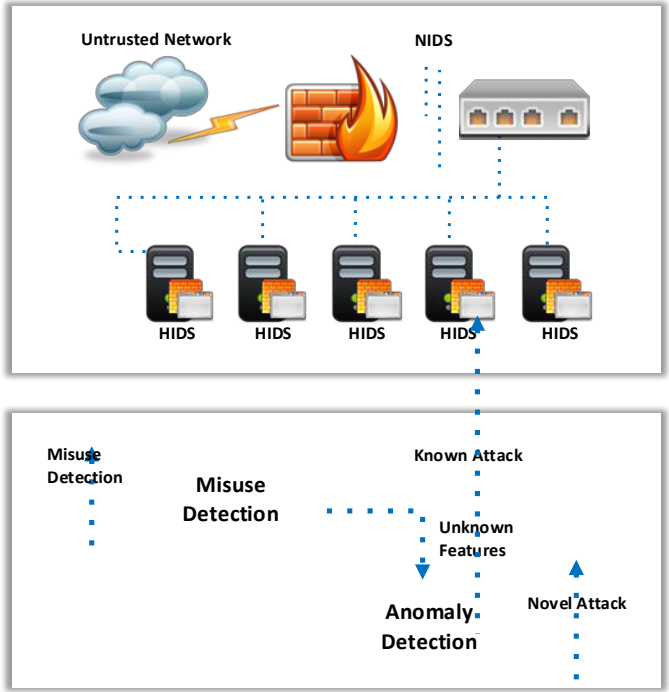
Behavior-based IDS

- An IDS is categorized based on how it reacts to a **potential intrusion**
- It functions in one of two modes, active or passive, based on the behavior after an attack
  - ✓ **Active IDS: Detects** and **responds** to detected intrusions
  - ✓ **Passive IDS: Only detects** intrusions

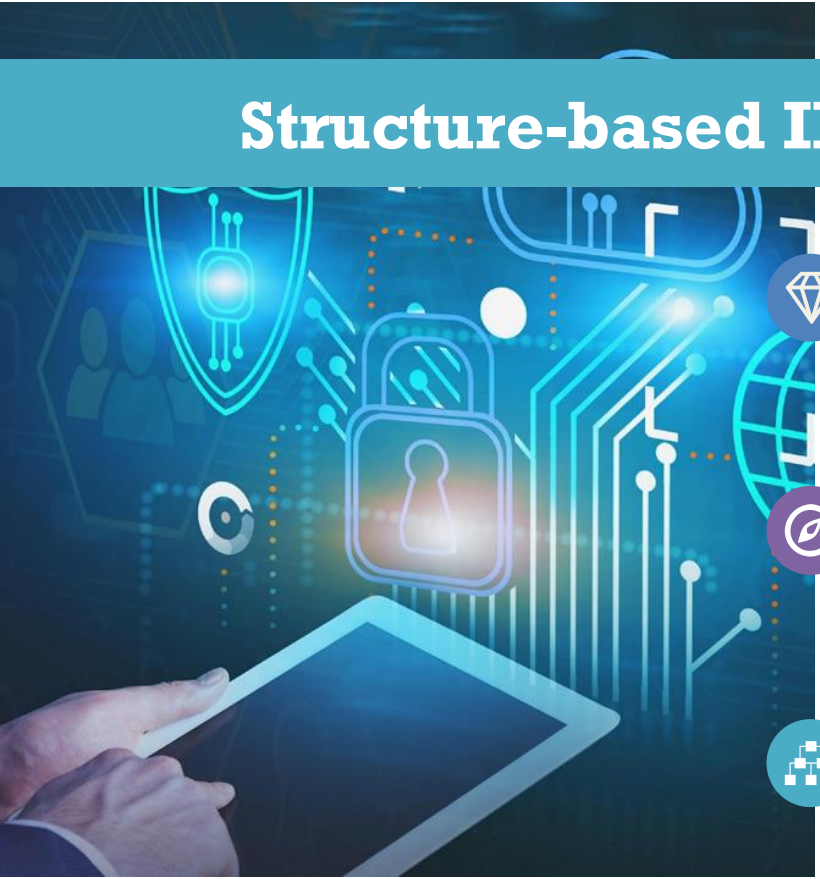


Protection-based IDS

- An IDS is classified based on the system/network if offers **protection** to
  - If it protects the network, it is called a network intrusion detection system (**NIDS**)
  - If it protects a host, it is called a host intrusion detection system (**HIDS**)
  - If it protects the network and a host, it is called a hybrid intrusion detection system (**Hybrid IDS**)
- A hybrid IDS combines the advantages of both the **low false-positive rate** of a NIDS and the anomaly-based detection of a HIDS to detect unknown attacks



Structure-based IDS



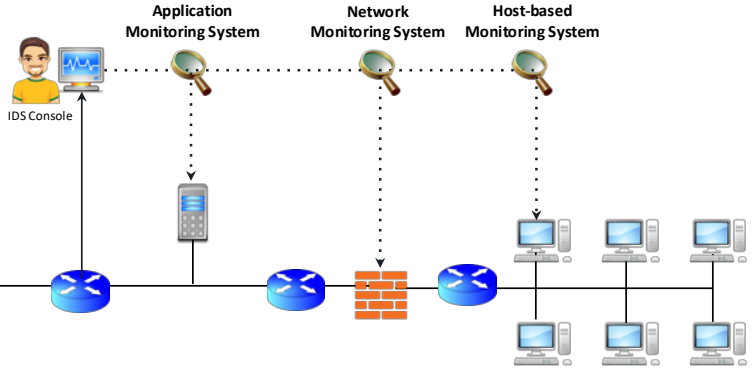
An IDS is also classified as a **centralized IDS** or a **distributed IDS**, this classification is based on the structure of the IDS

In a centralized IDS, all data is shipped to a **central location** for analysis, independent of the number of hosts that are monitored

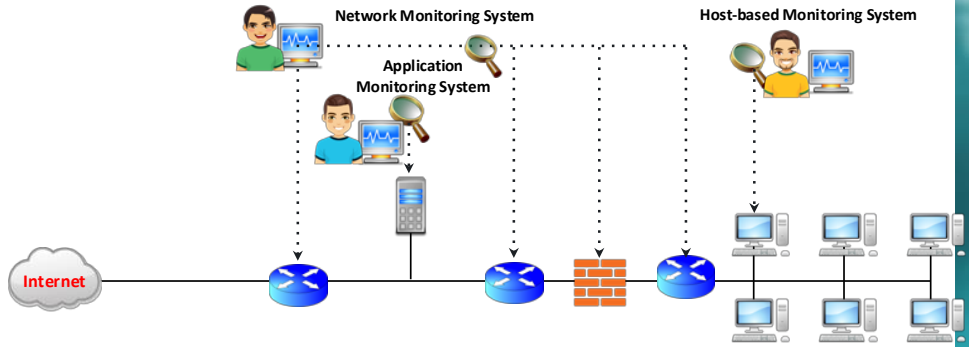
In a distributed IDS, **several IDS** are deployed over a large network and each IDS communicates with each other for traffic analysis

Structure-based IDS (Cont'd)

Centralized Control



Fully Distributed (Agent-based) Control



Analysis Timing–based IDS

Analysis time is a **span of time elapsed** between the events occurring and the analysis of those events

An IDS is Categorized based on Analysis Time as:

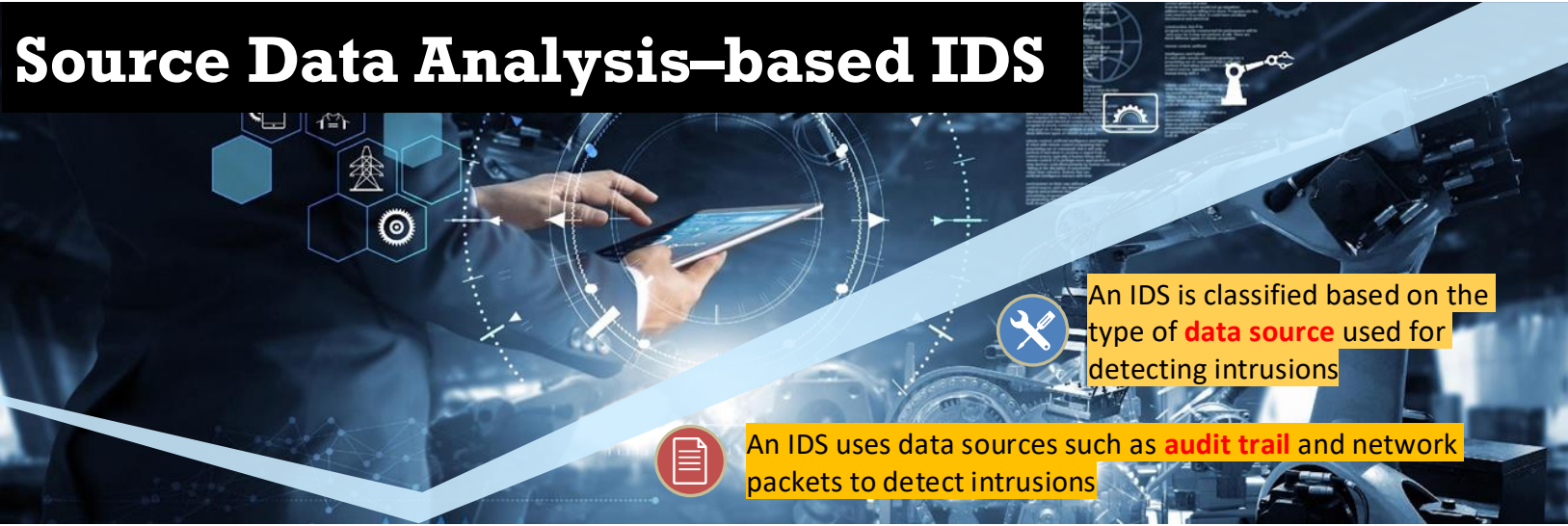
Interval-based IDS

- The information about an intrusion detection does not flow continuously from monitoring points to analysis engines, it is simply **stored and forwarded**
- It performs analysis of the detected intrusion **offline**

Real-Time–based IDS

- The information about an intrusion detection **flows continuously** from monitoring points to analysis engines
- It performs analysis of the detected intrusion **on the fly**

Source Data Analysis–based IDS



An IDS is classified based on the type of **data source** used for detecting intrusions

An IDS uses data sources such as **audit trail** and network packets to detect intrusions

Intrusion Detection Using Audit Trails

- **Audit trails** help the IDS detect performance problems, security violations, and flaws in applications

Intrusion Detection Using Network Packets

- Capturing and analyzing **network packets** help an IDS detect well-known attacks

IDS Components

An IDS system is built on various components. Knowledge of their **functions** and **placement** is required for effective IDS implementation

IDS Components

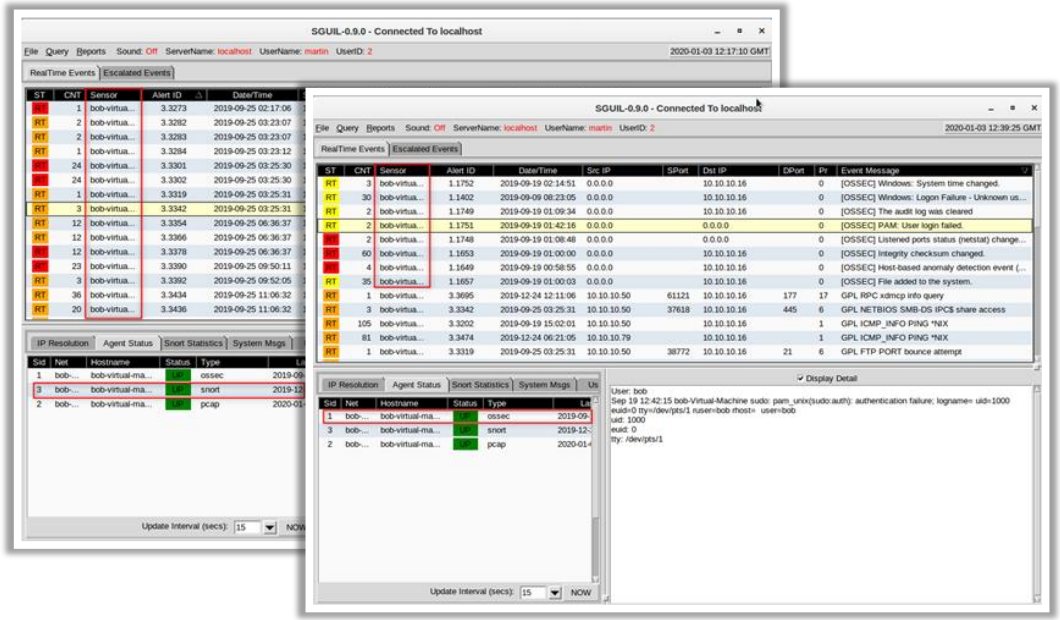
- Network Sensors
- Alert Systems
- Command Console
- Response System
- Attack Signature Database

Network Sensors

Network sensors are hardware and software components that **monitor** network traffic and trigger **alarms** if any abnormal activity is detected

Network sensors should be placed and located at common entry points in a network such as:

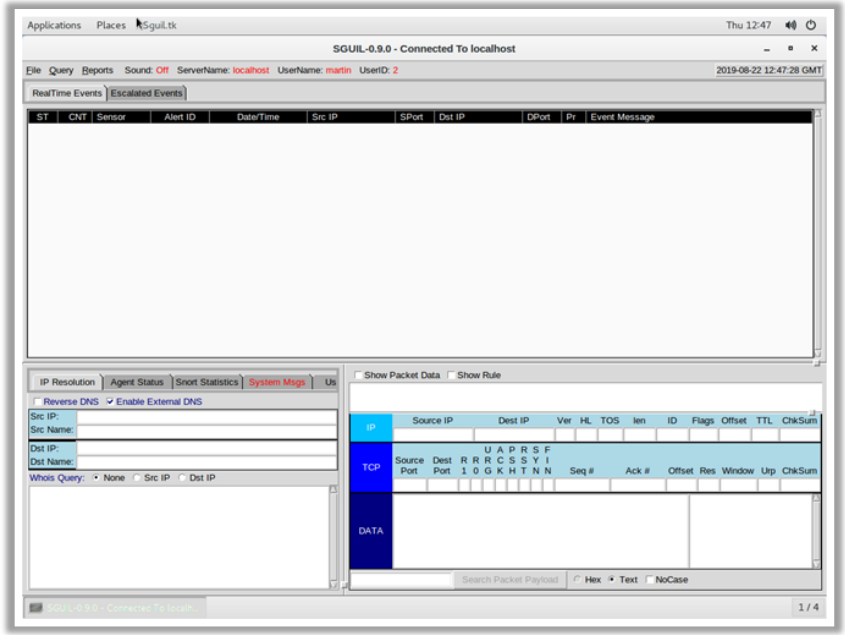
- Internet gateways
- In between LAN connections
- Remote access servers used to receive dial-up connections
- VPN devices
- Either side of firewall



Command Console

- Command console software is installed and runs on a **separate system** that is dedicated to the IDS
- It provides a **user interface** to an administrator for the purpose of receiving and analyzing security events, alert message, and log files
- It evaluates **security event** information from different security devices
- **Caution**: If the command console is installed on a non-dedicated computer system (e.g., firewall, backup server), it will drastically slow down the response to security events as those systems may be busy handling other tasks

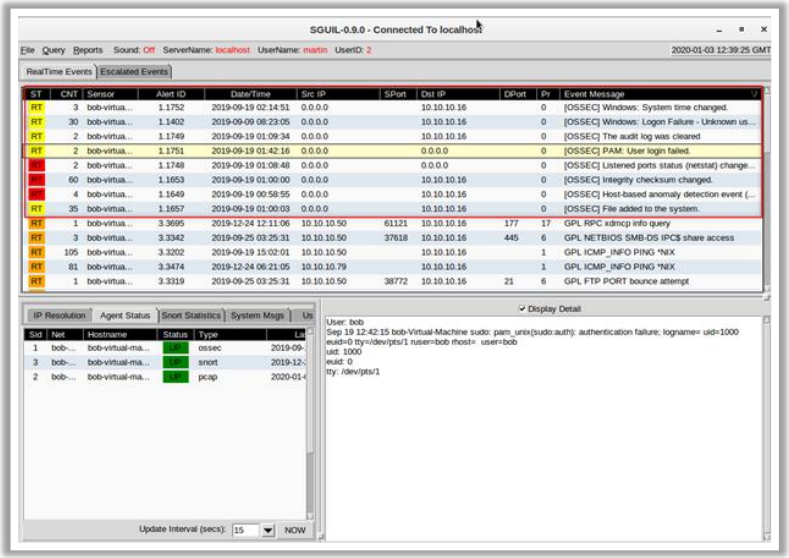
Sguil Command Console



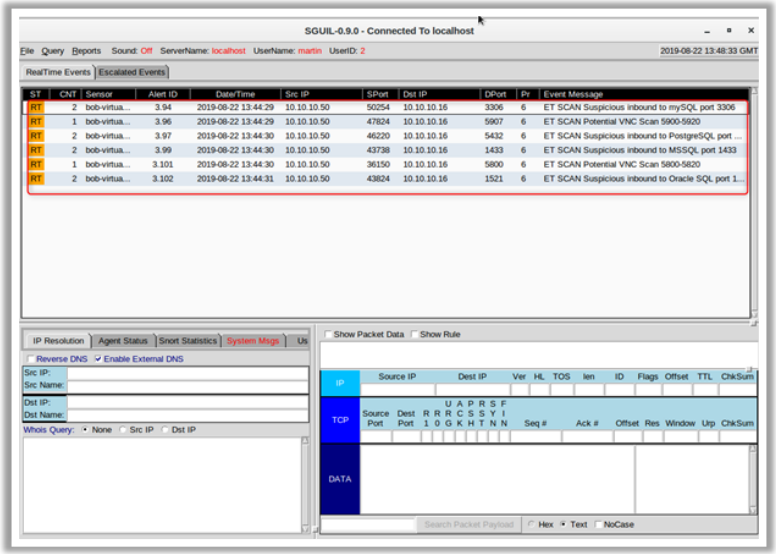
Alert Systems

An alert system sends an **alert message** when any anomaly or misuse is detected

OSSEC HIDS Alerts in Sguil



Snort NIDS Alerts in Sguil



Response System

The response system issues **countermeasures** against any intrusion that is detected

You also need to involved in the decision during incident response and should have the ability to respond on your own. You need to make **decisions** on how to deal with false positives and when a response needs escalation

Recommendation: You should not solely rely on an IDS response system for an intrusion response

Attack Signature Database

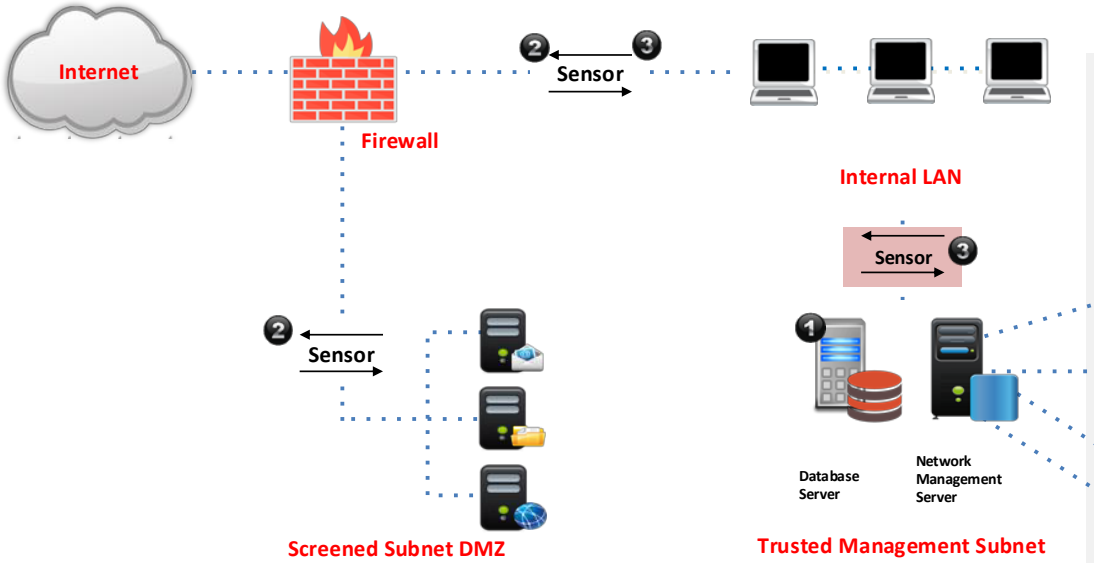
An IDS does not have the capability to make a decision, instead it maintains a **database** of attack signatures and patterns

Network traffic is compared against these known **attack signatures** and then a decision can be made

If any matches are found, the IDS will raise an alert and **block** the suspicious traffic

Recommendation: You need to periodically update the IDS attack signature database

Collaboration of IDS Components in Intrusion Detection

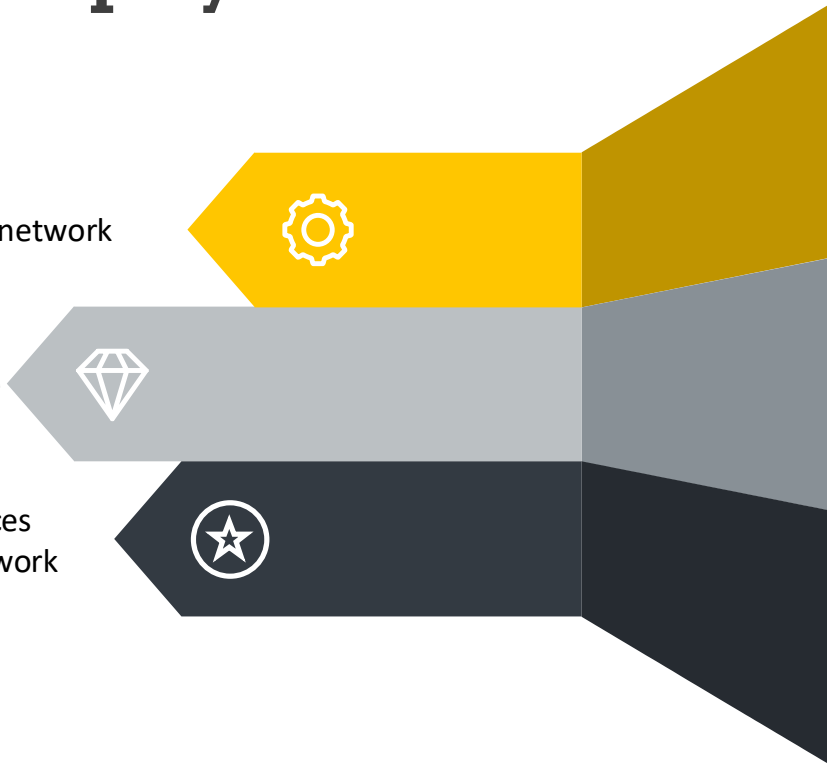


1. Install Database Signatures
2. Gather Data
3. Alert Message Sent
4. IDS Responds
5. Administrator Assesses Damage
6. Escalation Procedures Followed if Necessary
7. Events are Logged and Reviewed

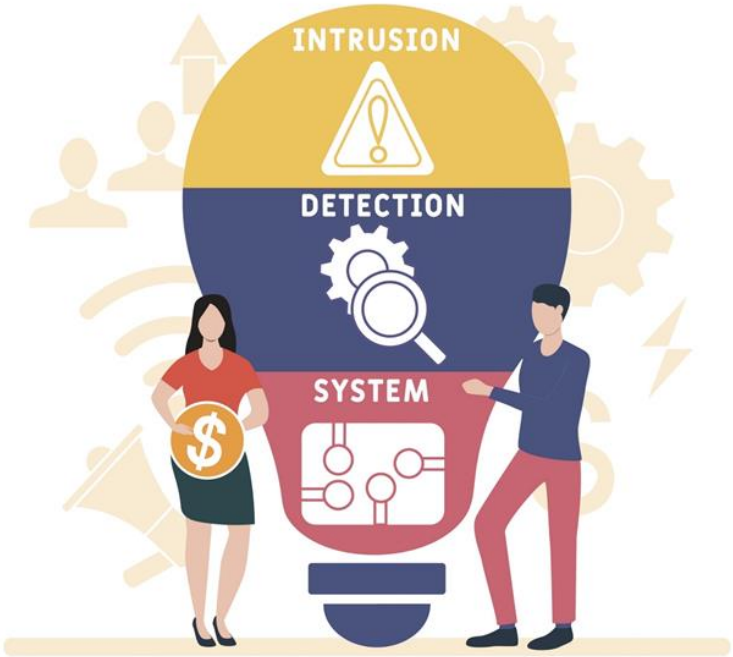
Deployment of Network and Host-based IDS

Staged IDS Deployment

- You should **plan** for a staged IDS deployment in their network
- A staged deployment will help you gain **experience** and **discover** how much monitoring and maintenance of network resources is actually required
- The **monitoring** and **maintenance** of network resources varies depending on the size of an organization's network



Deploying Network-based IDS

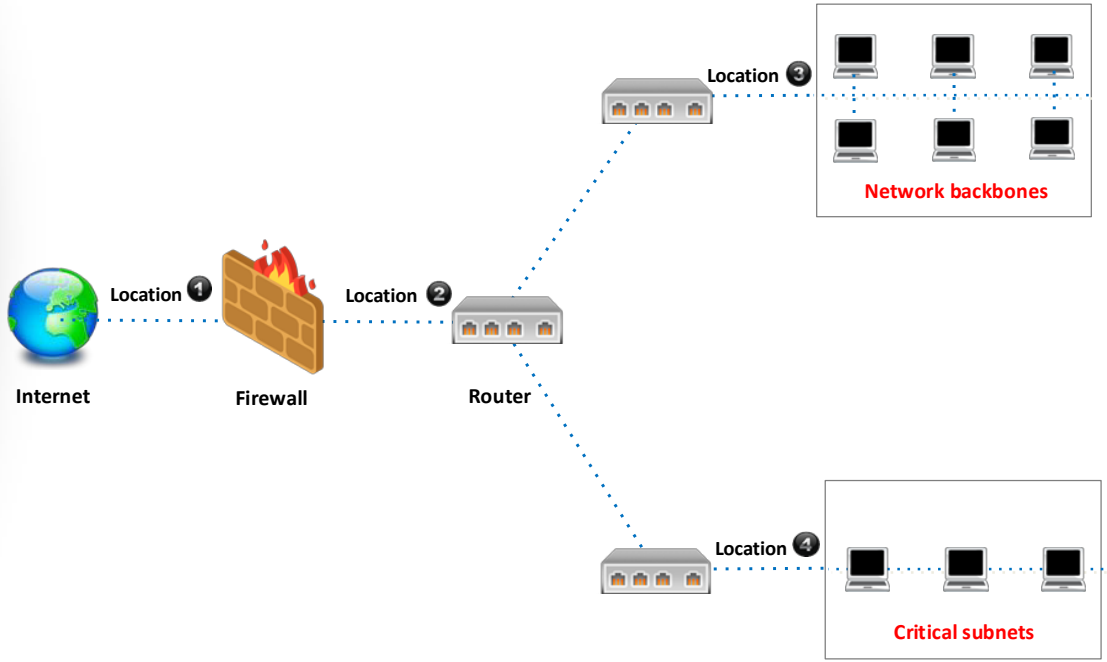


An effective deployment of NIDS requires a lot of attention concerning the **network topology** of the organization

The possible IDS deployment options are categorized based on the location of IDS sensors

Consider all possible **options** and its associated **advantages/disadvantages** when placing a network-based IDS

Deploying Network-based IDS (Cont'd)



Deploying Network-based IDS (Cont'd)

Location 1

- Place an IDS sensor behind each **external firewall** and in the **network DMZ**

Advantages

- ✓ Monitors attacks originating from the outside world
- ✓ Highlights the inability of the firewall and its policies to defend against attacks
- ✓ It can see attacks which target the web or FTP servers located in the DMZ
- ✓ Monitors outgoing traffic results from a compromised server

Location 2

- Place an IDS sensor outside an **external firewall**

Advantages

- ✓ Ability to identify the number and types of attack originating from the Internet to the network

Deploying Network-based IDS (Cont'd)

Location 3

- ❑ Place an IDS sensor on major **network backbones**

Advantages

- ✓ Monitors and inspects large amounts of traffic, increasing the chance for attack detection
- ✓ Detects unauthorized attempts from outside the organization

Location 4

- ❑ Place an IDS sensor on **critical subnets**

Advantages

- ✓ Detects attacks on critical systems and resources
- ✓ Focuses on specific critical systems and resources

Deploying a Host-based IDS

Deploying a host-based IDS provides an **additional layer of security**

This type of IDS must be installed and configured on **each critical system** in the network

You should consider installing a host-based IDS on **every host** in the organization

When deploying a host-based IDS, it is recommended that it has **centralized management** and **reporting** functions, which reduces the complexity for managing alerts from a large number of hosts

What is an IDS Alert?

- Alert is a **graduated event**, which notifies that a particular event (or series of events) has reached a specified threshold and needs proper action by a responsible party

- It sends the notification, indicating that something is wrong and **requires immediate attention** and monitoring

Types of IDS Alerts

True Positive (Attack - Alert)	❑ An IDS raises an alarm when a **legitimate attack** occurs
False Positive (No Attack - Alert)	❑ An IDS raises an alarm when **no attack** has taken place
False Negative (Attack - No Alert)	❑ An IDS does not raise an alarm when a **legitimate attack** has taken place
True Negative (No Attack - No Alert)	❑ An IDS does not raise an alarm when an **attack** has not taken place

Characteristics of Good IDS Solutions

01 Run continuously with **less human intervention**

02 Must be **fault tolerant**

03 Resistant to **subversion**

04 **Minimal overhead** on the system

05 Observe **deviations** from normal behavior

06 Not easily **deceived**

07 Tailored to specific **system needs**

08 Copes with **dynamic system behavior**

Selection of an Appropriate IDS/IPS Solutions

- IDS products must meet certain **criteria** to be deployed in an organization
- Compare the different technology types, then select the most appropriate **technology** to meet the requirements

The products should be evaluated based on organizational requirements such as:

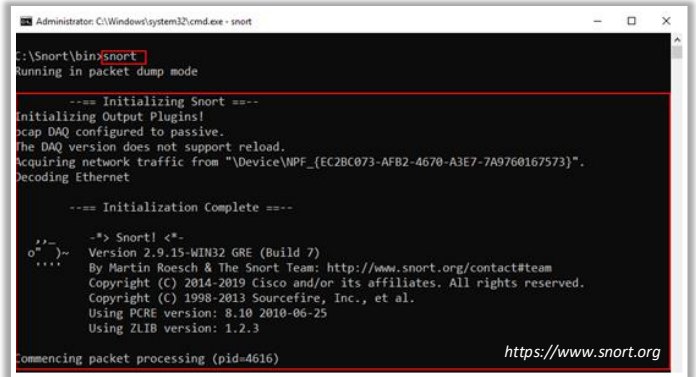
General requirements	❑ Evaluate the general requirements the IDS products will have to meet post deployment ❑ Size of an organization also modifies the number of IDS products needed
Security Capability Requirements	❑ The selection of an IDS depends on an organization's environment and policies as well as the current security and network infrastructure
Performance requirements	❑ Evaluate an IDS product's general performance characteristics by assessing its capacity to handle the network traffic or packet monitoring capabilities for NIDS and event monitoring capabilities for HIDS
Management requirements	❑ The products need to comply with the organization's management policy in order to be used effectively
Life Cycle Costs	❑ Estimated lifecycle costs of the products should be within the available budget

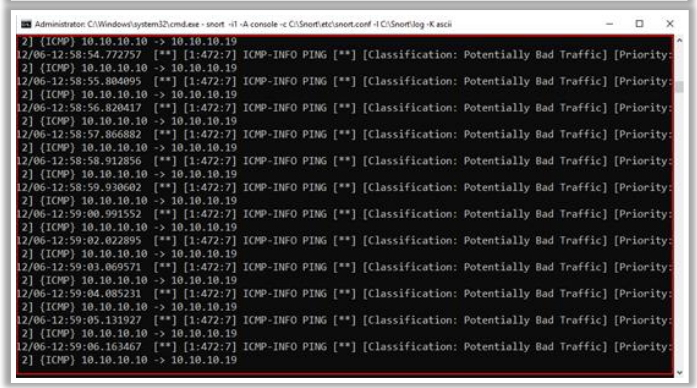
Intrusion Detection with Snort

01 Snort is an open-source network intrusion detection system, capable of performing real-time **traffic analysis and packet logging on IP networks**

02 It can perform **protocol analysis** and **content searching/matching**, and is used to detect a variety of **attacks and probes**, such as buffer overflows, stealth port scans, and OS fingerprinting attempts

03 It uses a flexible **rules language** to describe traffic that it should collect or pass, as well as a **detection engine** that utilizes a modular plug-in architecture

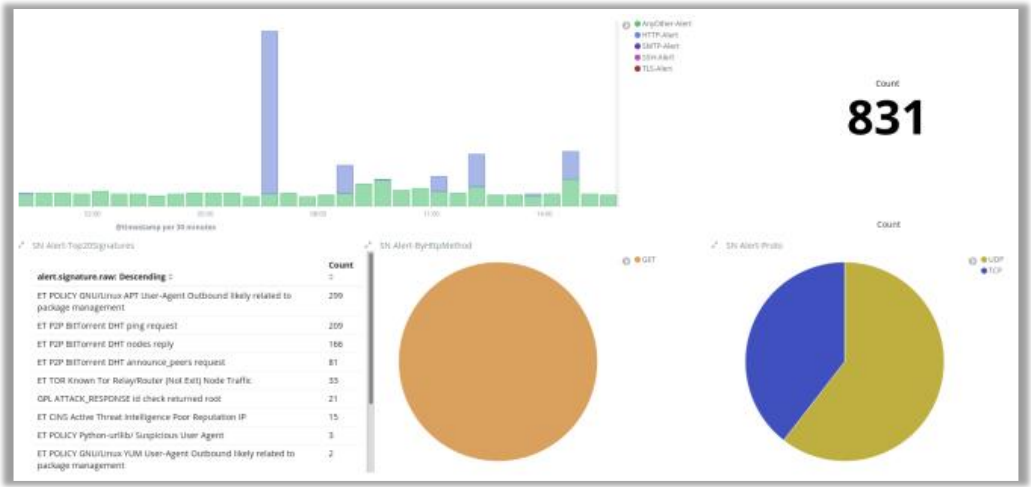




Intrusion Detection Tools

Suricata

Suricata is a robust network threat detection engine capable of **real-time intrusion detection (IDS)**, **inline intrusion prevention (IPS)**, **network security monitoring (NSM)**, and **offline pcap processing**



https://suricata-ids.org

AlienVault® OSSIM™
https://cybersecurity.att.com

SolarWinds Security Event Manager
https://www.solarwinds.com

OSSEC
https://www.ossec.net

Zeek
https://zeek.org

Sagan Log Analysis Engine
https://quadrantsec.com