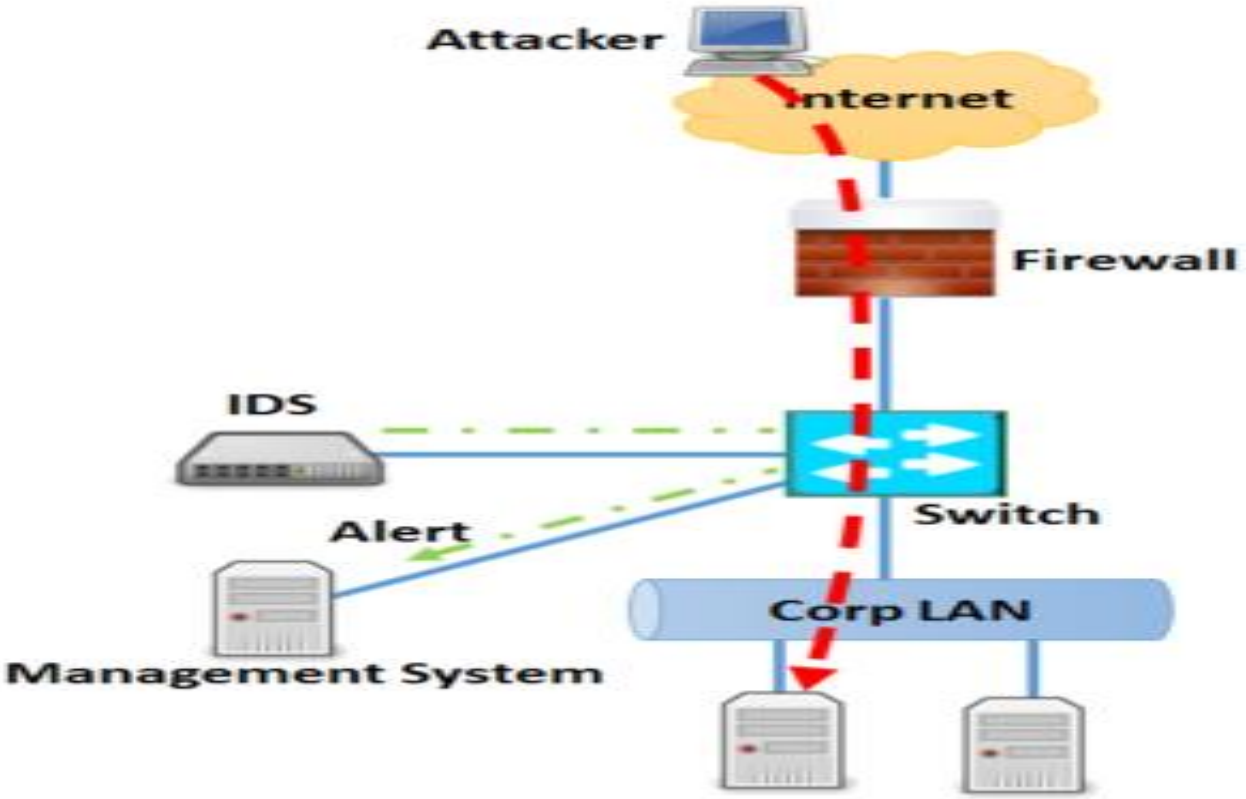
Intrusion Detection Systems (IDS)

What is the Intrusion Detection

- Intrusion detection is the act of detecting unwanted traffic on a network or a device.
- An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable user policies.
- When any malicious activity is detected, an **alert** is generated by the IDS thereby notifying the system administrators of a possible attack to the system.
- Note: -
- Intrusions are the activities that violate the security policy of system.
- Intrusion Detection is the process used to identify intrusions.

Intrusion Detection System

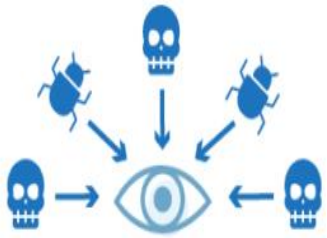


Classification of IDS

- As per the placement of sensors of IDS: -
  - Network based IDS
  - Host based IDS
  - Protocol based IDS
  - Application Based IDS
  - Hybrid IDS

- As per the methodology: -
  - Anomaly Based
  - Signature Based

Anomaly-Based Detection



Signature-based Detection

Anomaly based IDS

- Anomaly-based IDS was introduced to detect the unknown malware attacks as new malware are developed rapidly.
- In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model.
- Machine learning based method has a better generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.
- Anomaly-based IDS typically work by taking a baseline of the normal traffic and activity taking place on the network.
- They can measure the present state of traffic on the network against this baseline in order to detect patterns that are not present in the traffic normally.
- Such methods can work very well when we are looking to detect new attacks or attacks that have been deliberately assembled to avoid IDSes.

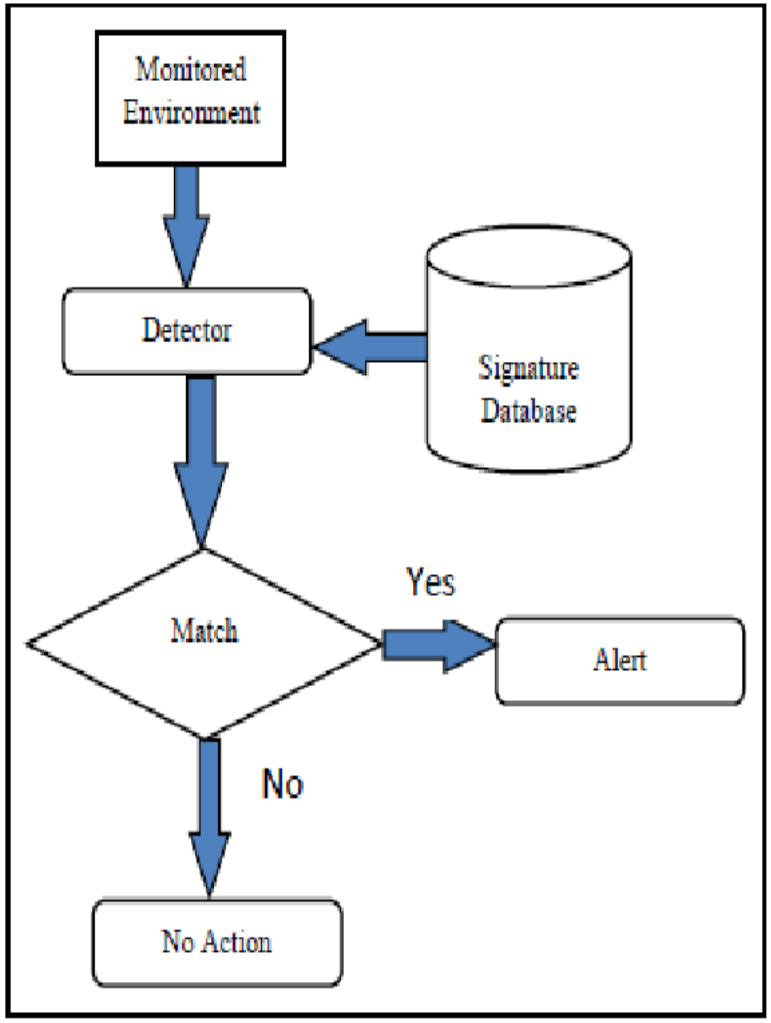
Drawbacks of Anomaly detection IDS

- Assumes that intrusions will be accompanied by manifestations that are sufficiently unusual so as to permit detection.

- It can generate false alarms. As if the traffic on the network changes from what was present when we took our baseline, the IDS may see this as indicative of an attack and likewise for legitimate activity that causes unusual traffic patterns or spikes in traffic.

Signature based IDS

- Signature-based IDSes work in a very similar fashion to most antivirus systems.
- They maintain a database of the signatures that might signal a particular type of attack and compare incoming traffic to those signatures.
- In general, this method works well, except when we encounter an attack that is new, or has been specifically constructed in order to not match existing attack signatures.
- This IDS possess an attacked description that can be matched to sensed attack manifestations.



Signature based IDS (contd.)

- ID system is programmed to interpret a certain series of packets, or a certain piece of data contained in those packets,as an attack. For example, an IDS that watches web servers might be programmed to look for the string “phf” as an indicator of a CGI program attack.
- Most signature analysis systems are based off of simple pattern matching algorithms. In most cases, the IDS simply looks for a sub string within a stream of data carried by network packets. When it finds this sub string (for example, the ``phf'' in ``GET /cgi-bin/phf?''), it identifies those network packets as vehicles of an attack.

Drawbacks of Signature based IDS

- They are unable to detect novel attacks.
- Suffer from false alarms.
- One of the large drawbacks to this method is that many signature-based systems rely solely on their signature database in order to detect attacks. If we do not have a signature for the attack, we may not see it at all. In addition to this, the attacker crafting the traffic may have access to the same IDS tools we are using and may be able to test the attack against them in order to specifically avoid our security measures.

Host/Applications based IDS

Host Intrusion Detection

- Host intrusion detection systems (HIDS) run on independent hosts or devices on the network.
- A HIDS monitors the incoming and outgoing packets from the device only and will alert the administrator if suspicious or malicious activity is detected.
- It takes a snapshot of existing system files and compares it with the previous snapshot.
- If the analytical system files were edited or deleted, an alert is sent to the administrator to investigate.
- An example of HIDS usage can be seen on mission critical machines, which are not expected to change their layout.

Drawbacks of the host based IDS

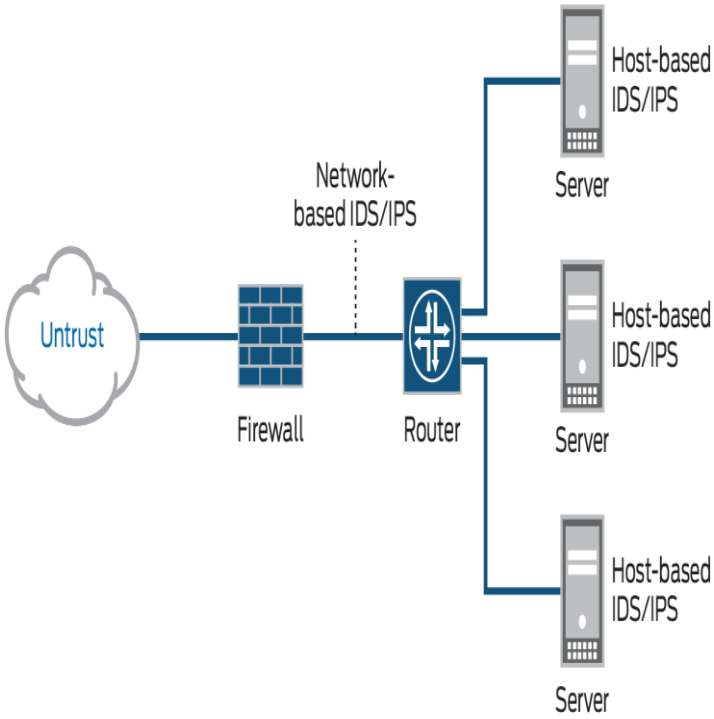
- The kind of information needed to be logged in is a matter of experience.
- Unselective logging of messages may greatly increase the audit and analysis burdens.
- Selective logging runs the risk that attack manifestations could be missed.

Strengths of the host based IDS

- Attack verification
- System specific activity
- Encrypted and switch environments
- Monitoring key components
- Near Real-Time detection and response.
- No additional hardware

Network based IDS

- A Network Intrusion Detection System (NIDS) is one common type of IDS that analyzes network traffic at all layers of the Open Systems Interconnection (OSI) model and makes decisions about the purpose of the traffic, analyzing for suspicious activity.
- Most NIDSs are easy to deploy on a network and can often view traffic from many systems at once.
- Network intrusion detection systems (NIDS) are set up at a planned point within the network to examine traffic from all devices on the network.
- It performs an observation of passing traffic on the entire subnet and matches the traffic that is passed on the subnets to the collection of known attacks.
- Once an attack is identified or abnormal behavior is observed, the alert can be sent to the administrator.
- An example of an NIDS is installing it on the subnet where firewalls are located in order to see if someone is trying crack the firewall.



Strengths of Network based IDS

- Cost of ownership reduced
- Packet analysis
- Evidence removal
- Real time detection and response
- Malicious intent detection
- Complement and verification
- Operating system independence

Benefits of IDS

- Monitors the operation of firewalls, routers, key management servers and files critical to other security mechanisms.
- Allows administrator to tune, organize and comprehend often incomprehensible operating system audit trails and other logs.
- Can make the security management of systems by non-expert staff possible by providing nice user friendly interface.
- Can recognize and report alterations to data files.

Protocol-based Intrusion Detection System (PIDS):

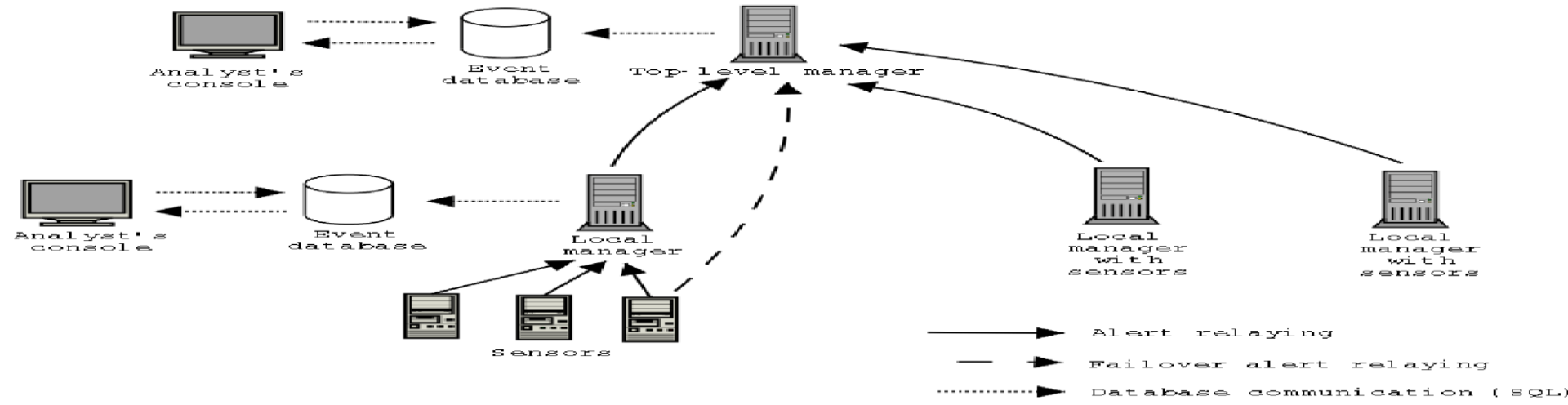
- Protocol-based intrusion detection system (PIDS) comprises of a system or agent that would consistently resides at the front end of a server, controlling and interpreting the protocol between a user/device and the server.
- It is trying to secure the web server by regularly monitoring the HTTPS protocol stream and accept the related HTTP protocol.
- As HTTPS is un-encrypted and before instantly entering its web presentation layer then this system would need to reside in this interface, between to use the HTTPS.

Application Protocol-based Intrusion Detection System (APIDS):

- Application Protocol-based Intrusion Detection System (APIDS) is a system or agent that generally resides within a group of servers.
- It identifies the intrusions by monitoring and interpreting the communication on application specific protocols.
- For example, this would monitor the SQL protocol explicit to the middleware as it transacts with the database in the web server.

Hybrid Intrusion Detection System :

- Hybrid intrusion detection system is made by the combination of two or more approaches of the intrusion detection system.
- In the hybrid intrusion detection system, host agent or system data is combined with network information to develop a complete view of the network system.
- Hybrid intrusion detection system is more effective in comparison to the other intrusion detection system.
- Prelude is an example of Hybrid IDS.



Limitations of IDS

- **False positives** (i.e., generating alerts when there is no real problem). “IDSs are notorious for generating false positives,” Rexroad said, adding that alerts are generally are sent to a secondary analysis platform to help contend with this challenge.
- This challenge also puts pressure on IT teams to continually update their IDSs with the right information to detect legitimate threats and to distinguish those real threats from allowable traffic.
- “IDS systems must be tuned by IT administrators to analyze the proper context and reduce false-positives. For example, there is little benefit to analyzing and providing alerts on internet activity for a server that is protected against known attacks. This would generate thousands of irrelevant alarms at the expense of raising meaningful alarms. Similarly, there are circumstances where perfectly valid activities may generate false alarms simply as a matter of probability,” Rexroad said, noting that organizations often opt for a secondary analysis platform, such as a Security Incident & Event Management (SIEM) platform, to help with investigating alerts.
- **Staffing.** Given the requirement for understanding context, an enterprise has to be ready to make any IDS fit its own unique needs, experts advised.
- “What this means is that an IDS cannot be a one-size-fits all configuration to operate accurately and effectively. And, this requires a savvy IDS analyst to tailor the IDS for the interests and needs of a given site. And, knowledgeable trained system analysts are scarce,” Novak added.
- **Missing a legitimate risk.** “The trick with IDS is that you have to know what the attack is to be able to identify it. The IDS has always had the patient zero problem: You have to have found someone who got sick and died before you can identify it,” Hanselman said.

Future of IDS

- To integrate the network and host based IDS for better detection.

- Developing IDS schemes for detecting novel attacks rather than individual instantiations.