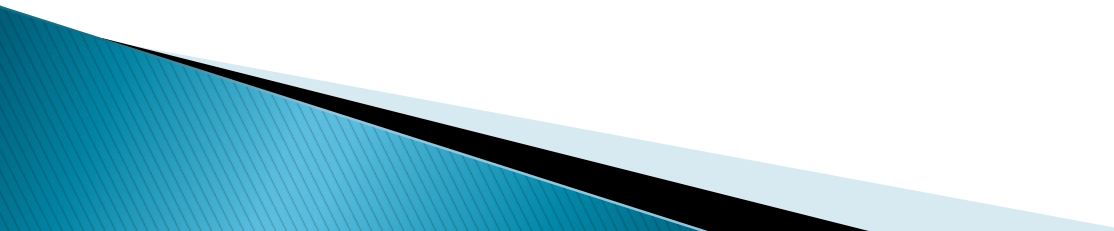


INTRUSION DETECTION SYSTEMS (IDS)

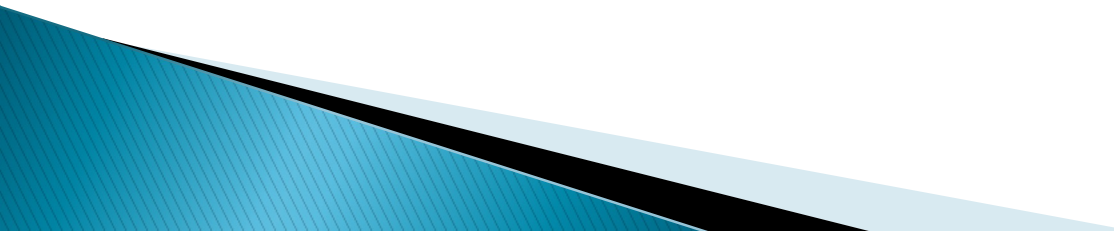
Momodu Bolorunduro James



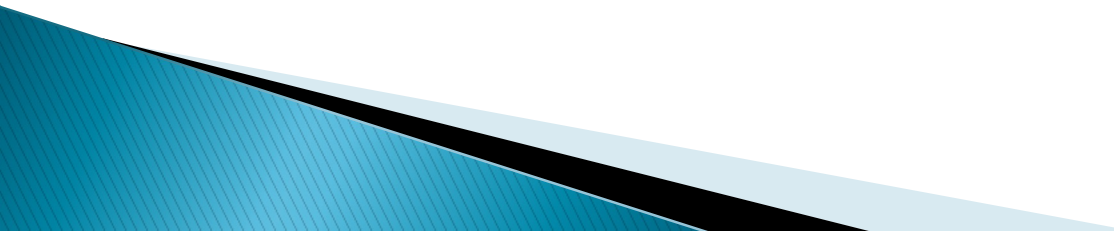
Agenda

- ▶ Sources
 - ▶ What is an Intrusion Detection System
 - ▶ Types of Intrusion Detection Systems
 - ▶ How an IDS Works
 - ▶ Detection Methods
 - ▶ Why are IDS important
 - ▶ How does an IDS fit into your security plan?
 - ▶ Pros and Cons
 - ▶ Questions
- 

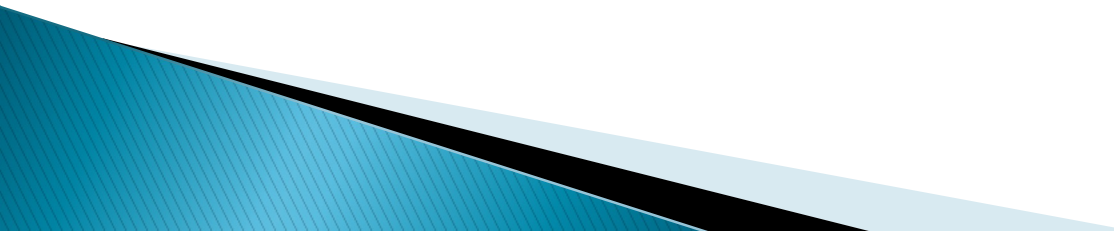
Sources

- ▶ Baker, A. R., & Esler, J. (2007). *Snort IDS and IPS Toolkit*.
 - ▶ Baumrucker, C. T., Burton, J. D., & Dentler, S. (2003). *Cisco Security Professional's Guide to Secure Intrusion Detection Systems*.
 - ▶ Endorf, C., Schultz, E., & Mellander, J. (2004). *Intrusion Detection and Prevention*.
 - ▶ Training, U. A.-I. (n.d.). Intrusion Detection Systems (IDS) and Auditing.
- 

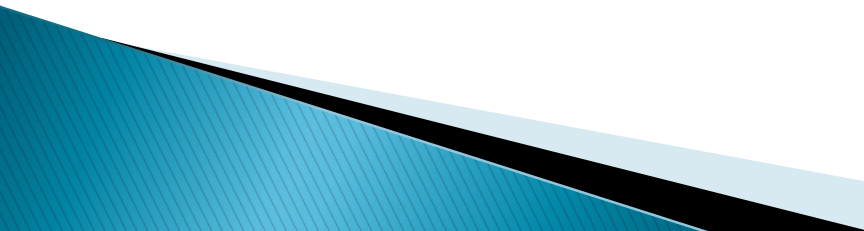
What is an Intrusion Detection System?

- ▶ Defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity.
 - ▶ An IDS detects activity in traffic that may or may not be an intrusion.
 - ▶ IDSes can detect and deal with insider attacks, as well as, external attacks, and are often very useful in detecting violations of corporate security policy and other internal threats.
- 

Host Based Intrusion Detection

- ▶ Are usually installed on servers and are more focused on analyzing the specific operating systems and applications, resource utilization and other system activity residing on the Host-based IDS host.
 - ▶ It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base.
 - ▶ Host-based IDS are often critical in detecting internal attacks directed towards an organization's servers such as DNS, Mail, and Web Servers.
- 

Network Based Intrusion Detection

- ▶ Are dedicated network devices distributed within networks that monitor and inspect network traffic flowing through the device.
 - ▶ Instead of analyzing information that originates and resides on a host, Network-based IDS uses packet sniffing techniques to pull data from TCP/IP packets or other protocols that are traveling along the network.
 - ▶ Most Network-based IDS log their activities and report or alarm on questionable events.
 - ▶ Network-based IDS work best when located on the DMZ, on any subnets containing mission critical servers and just inside the firewall.
- 

Comparison

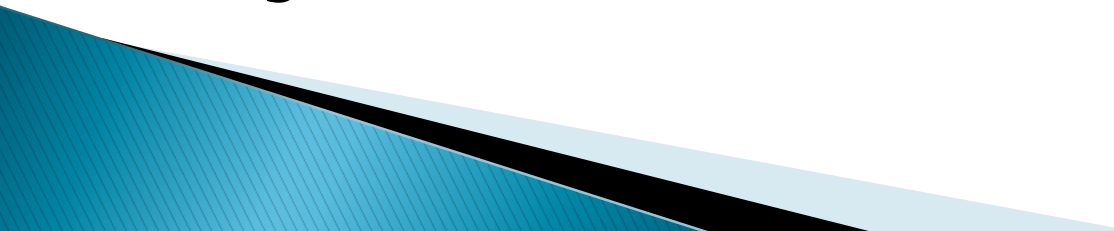
Host Based

- ▶ Narrow in scope (watches only **specific** host activities)
- ▶ More complex setup
- ▶ Better for detecting attacks from the **inside**
- ▶ **More expensive** to implement
- ▶ Detection is based on what any **single host** can record
- ▶ Does not see packet headers
- ▶ Usually only responds **after** a suspicious log entry has been made
- ▶ OS-specific
- ▶ Detects local attacks before they hit the network
- ▶ Verifies success or failure of attacks

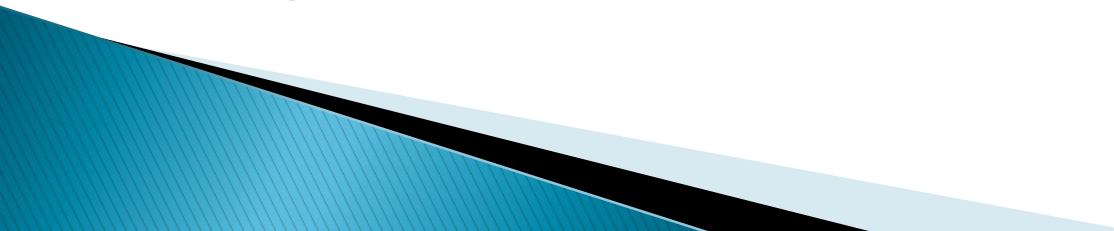
Network Based

- ▶ Broad in scope (watches **all** network activities)
- ▶ Easier setup
- ▶ Better for detecting attacks from the **outside**
- ▶ **Less expensive** to implement
- ▶ Detection is based on what can be recorded on the **entire network**
- ▶ Examines packet headers
- ▶ Near **real-time** response
- ▶ OS-independent
- ▶ Detects network attacks as payload is analyzed
- ▶ Detects unsuccessful attack attempts

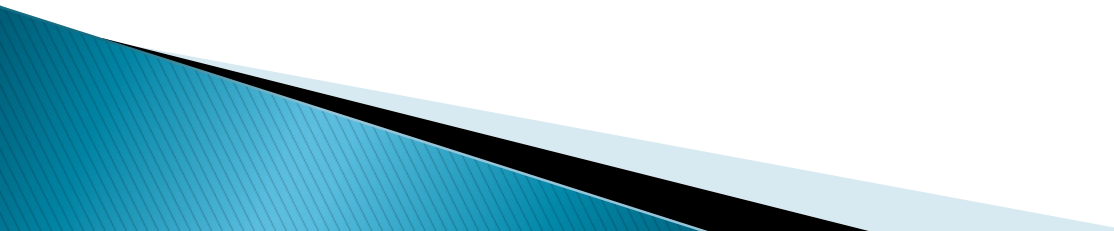
Hybrid Intrusion Detection

- ▶ Are systems that combine both Host-based IDS, which monitors events occurring on the host system and Network-based IDS, which monitors network traffic, functionality on the same security platform.
 - ▶ A Hybrid IDS, can monitor system and application events and verify a file system's integrity like a Host-based IDS, but only serves to analyze network traffic destined for the device itself.
 - ▶ A Hybrid IDS is often deployed on an organization's most critical servers.
- 

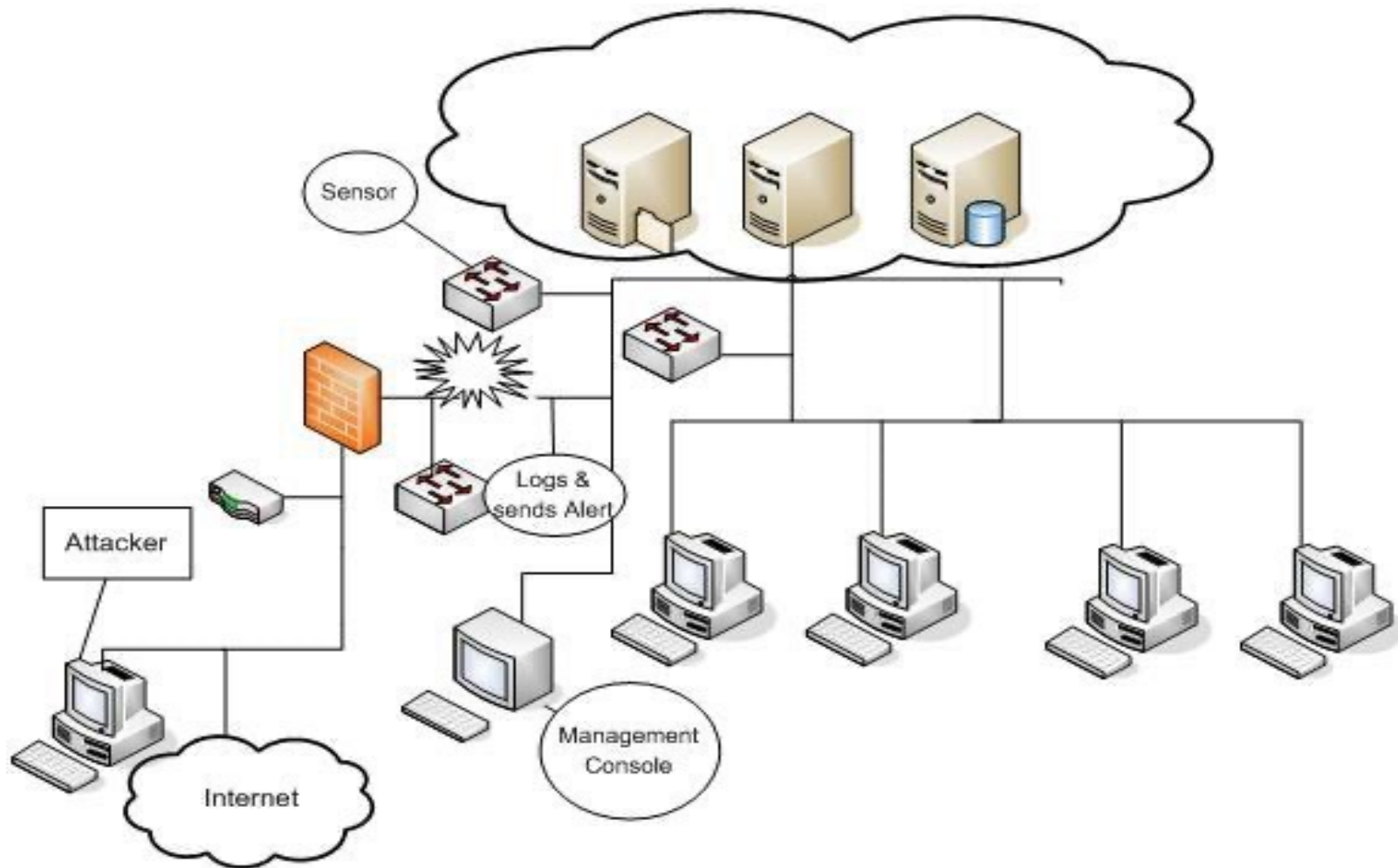
Honeypots

- ▶ Are decoy servers or systems setup to gather information regarding an attacker or intruder into networks or systems.
 - ▶ Appear to run vulnerable services and capture vital information as intruders attempt unauthorized access.
 - ▶ Provide you early warning about new attacks and exploitation trends which allow administrators to successfully configure a behavioral based profile and provide correct tuning of network sensors.
 - ▶ Can capture all keystrokes and any files that might have been used in the intrusion attempt.
- 

Passive Systems

- ▶ Detects a potential security breach
 - ▶ Logs the information
 - ▶ Signals an alert on the console
 - ▶ Does not take any preventive measures to stop the attack
- 

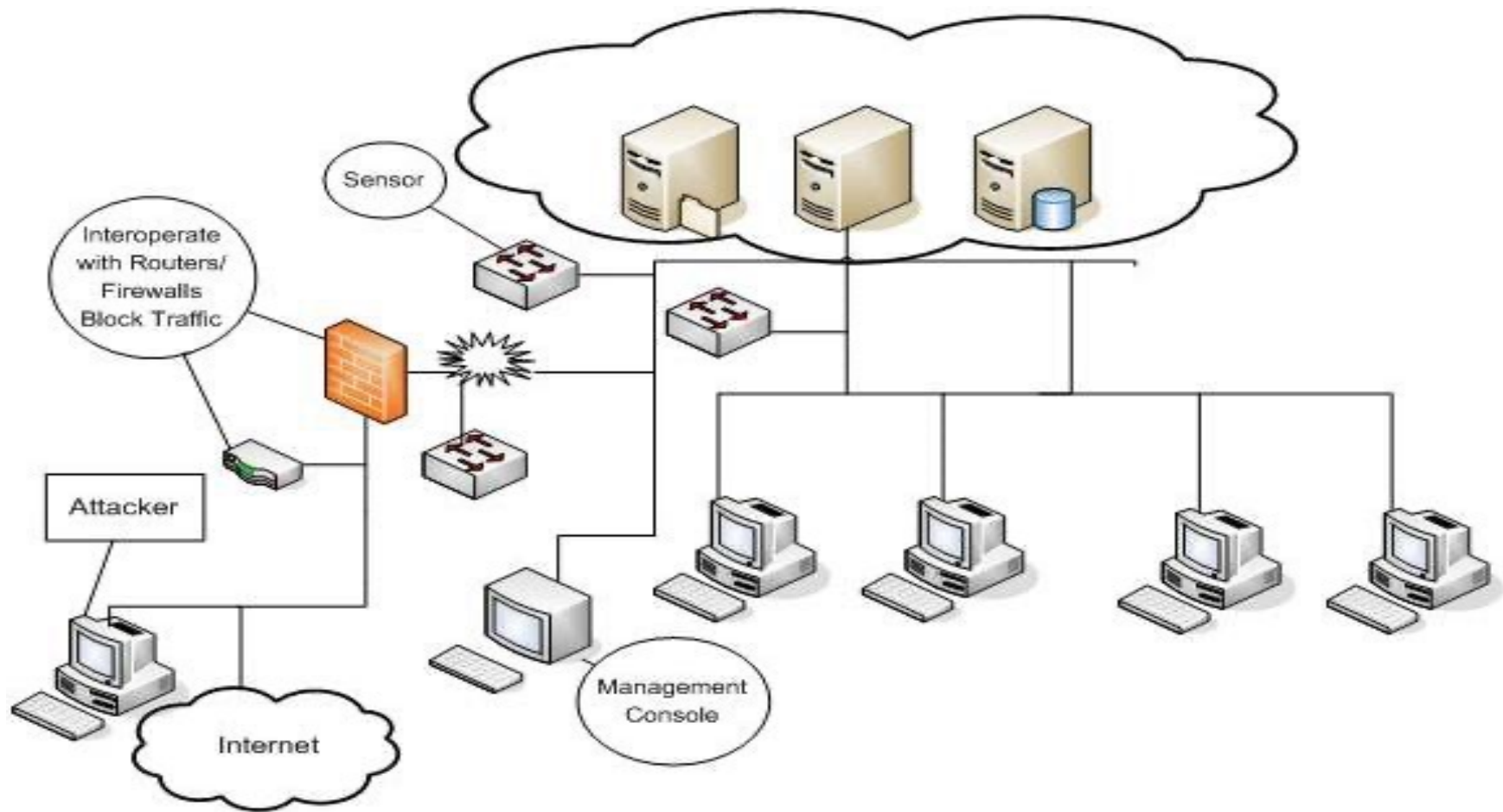
Passive Systems



Reactive/Active Systems

- ▶ Responds to the suspicious activity like a passive IDS by logging, alerting and recording, but offers the additional ability to take action against the offending traffic.

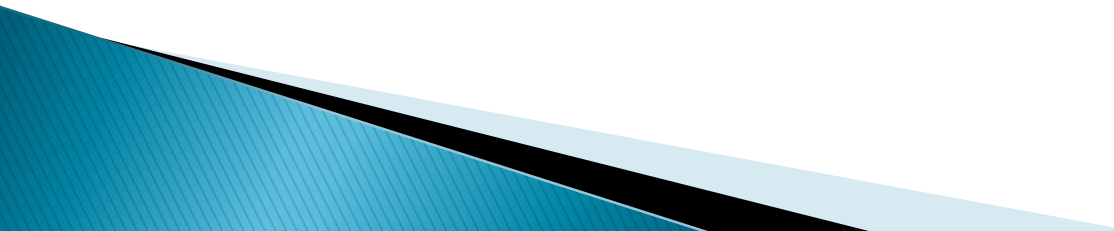
Reactive/Active Systems



Signature Based IDS

- ▶ Monitor network or server traffic and match bytes or packet sequences against a set of predetermined attack lists or signatures.
- ▶ Should a particular intrusion or attack session match a signature configured on the IDS, the system alerts administrators or takes other pre-configured action.
- ▶ Signatures are easy to develop and understand if you know what network behavior you're trying to identify.
- ▶ However, because they only detect known attacks, a signature must be created for every attack.
- ▶ New vulnerabilities and exploits will not be detected until administrators develop new signatures.
- ▶ Another drawback to signature-based IDS is that they are very large and it can be hard to keep up with the pace of fast moving network traffic.

Anomaly Based IDS

- ▶ Use network traffic baselines to determine a “normal” state for the network and compare current traffic to that baseline.
 - ▶ Use a type of statistical calculation to determine whether current traffic deviates from “normal” traffic, which is either learned and/or specified by administrators.
 - ▶ If network anomalies occur, the IDS alerts administrators.
 - ▶ A new attack for which a signature doesn’t exist can be detected if it falls out of the “normal” traffic patterns.
 - ▶ High false alarm rates created by inaccurate profiles of “normal” network operations.
- 

Issues

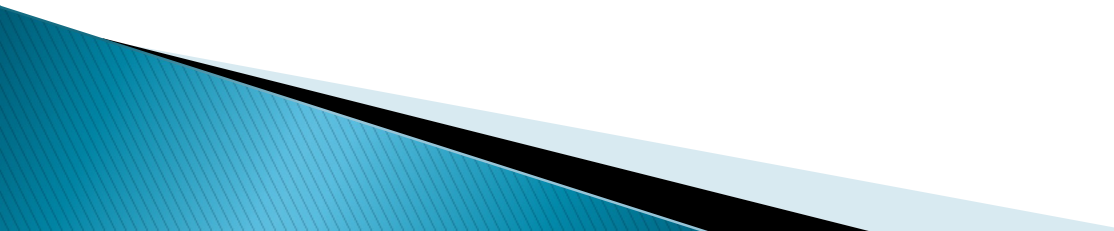
False Negatives

- ▶ When an IDS fails to detect an attack
- ▶ False negatives occur when the pattern of traffic is not identified in the signature database, such as new attack patterns.
- ▶ False negatives are deceptive because you usually have no way of knowing if and when they occurred.
- ▶ You are most likely to identify false negatives when an attack is successful and wasn't detected by the IDS.

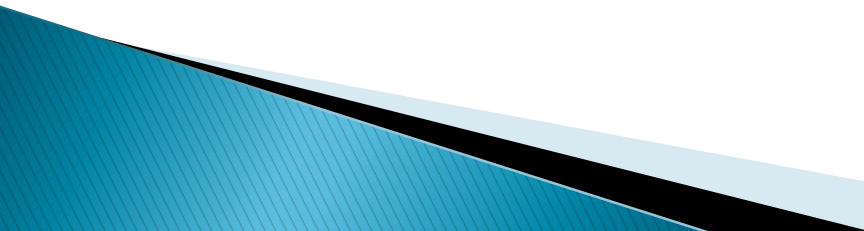
False Positives

- ▶ Described as a false alarm.
- ▶ When an IDS mistakenly reports certain “normal” network activity as malicious.
- ▶ Administrators have to fine tune the signatures or heuristics in order to prevent this type of problem.


Why are IDS important?

- ▶ The ability to know when an intruder or attacker is engaged in reconnaissance or other malicious activity can mean the difference between being compromised and not being compromised.
 - ▶ An IDS can alert the administrator of a successful compromise, allowing them the opportunity to implement mitigating actions before further damage is caused
 - ▶ As Corporations and other Institutions are being legally compelled to disclose data breaches and compromises to their affected customers, this can have profound effects upon a compromised company, in the way of bad press, loss of customer trust, and the effects on their stock.
- 

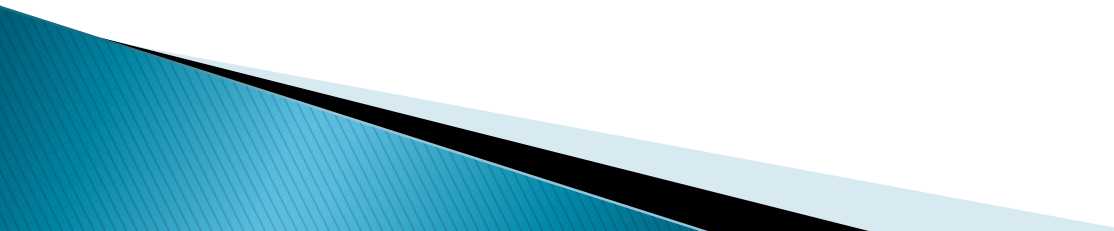
How does it fit into your security plan?

- ▶ As a network security expert you should know you cannot just rely on one or a few tools to secure your network. You need to have a defense in depth mindset and layer your network defenses.
 - ▶ Through the use of inside and outside firewalls, DMZs, Routers and Switches, an IDS is a great addition to your security plan.
 - ▶ You can use them to identify vulnerabilities and weaknesses in your perimeter protection devices, such as: firewalls, switches and routers. The firewall rules and router access control lists can be verified regularly for compliance.
 - ▶ You can use IDSes to enforce security policies, such as: unauthorized Internet access, downloads of executable files, use of file sharing programs like Kazza, or Instant Messenger use.
 - ▶ IDSes are also an invaluable source of evidence. Logs from an IDS can become an important part of computer forensics and incident handling efforts.
- 

Pros

- ▶ Can detect external hackers, as well as, internal network-based attacks
 - ▶ Scales easily to provide protection for the entire network
 - ▶ Offers centralized management for correlation of distributed attacks
 - ▶ Provides defense in depth
 - ▶ Gives administrators the ability to quantify attacks
 - ▶ Provides an additional layer of protection
- 

Cons

- ▶ Generates false positives and negatives
 - ▶ Reacts to attacks rather than preventing them
 - ▶ Requires full-time monitoring and highly skilled staff dedicated to interpreting the data
 - ▶ Requires a complex incident response process
 - ▶ Cannot monitor traffic at higher network traffic rates
 - ▶ Generates an enormous amount of data to be analyzed
 - ▶ Cannot deal with encrypted network traffic
 - ▶ It is expensive
- 

Questions

