BITS Pilani
Pilani Campus

BITS Pilani Presentation

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Ethical Hacking
Session No: 14 (Defense Processes and Tools)

Agenda

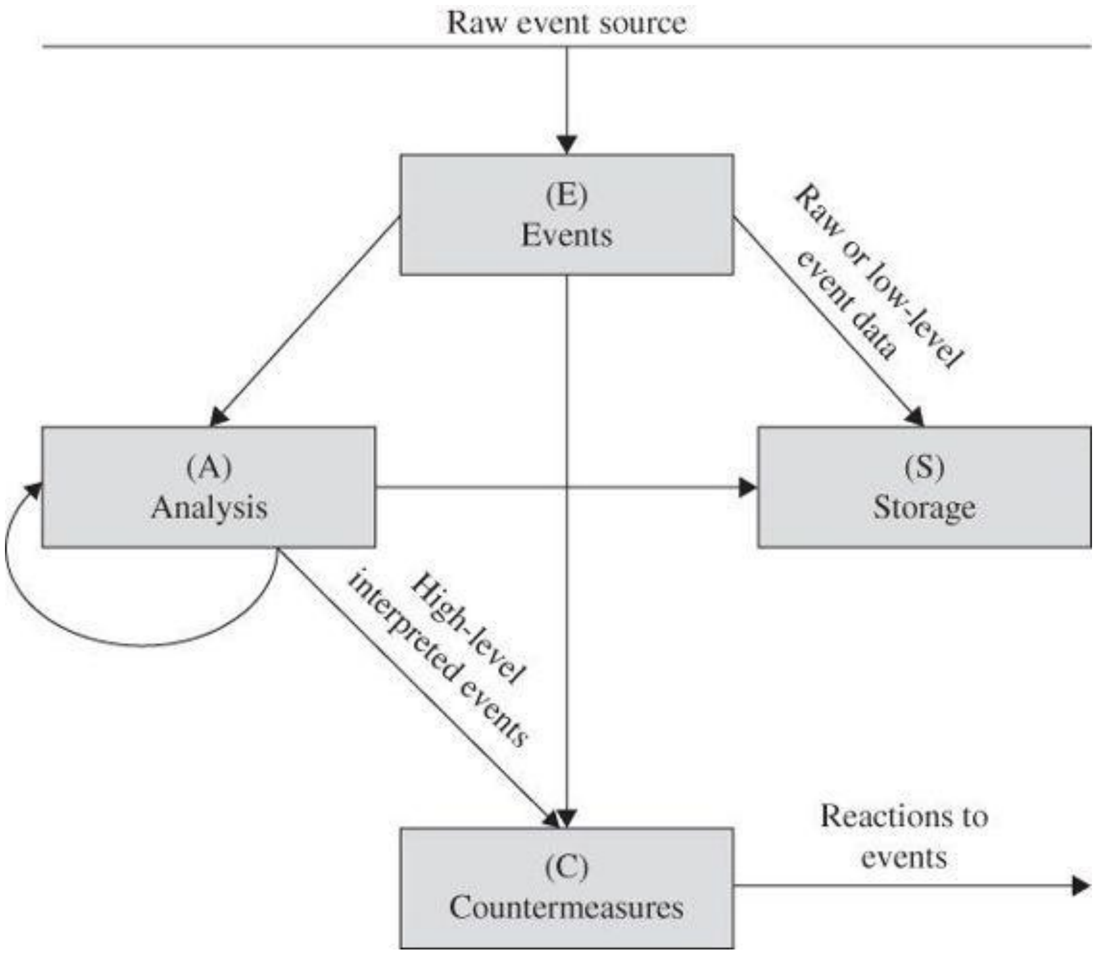
- IDS/IPS
  - Overview
  - Components
  - Architecture
  - Implementation

Intrusion Detection & Prevention System (IDPS)

What is an IDS?

- Intrusion Detection System (IDS) is a system that monitors network traffic for suspicious activity and issues alerts when such activity is discovered
- IDS is like a smoke detector that raises alarm if specific events occur
- IDS response may be:
  - **Manual:** raise alarm for someone to take action
  - **Automate:** get into protection mode to isolate the intruder (IPS)

How does IDS Work?



- Raw inputs from sensors
- Data storage of raw inputs
- Analysis of events
- Intrusion identification
- Countermeasure plan
- Response to events

Functions of IDS

- Monitor the operation of routers, firewalls, key management servers and files
- Help administrators to tune, organize and understand operating system audit trails and other logs to highlight policy violation
- Assess integrity of critical system files for vulnerabilities and misconfiguration
- Provide a user-friendly interface so non-expert staff members can assist with managing system security
- Build and maintain an extensive attack signature database
- Recognize and report when data files have been altered
- Correct system configuration errors
- Install and operate traps to record information about intruders
- Generate an alarm and notify when security has been breached
- React to intruders by blocking them or blocking the server

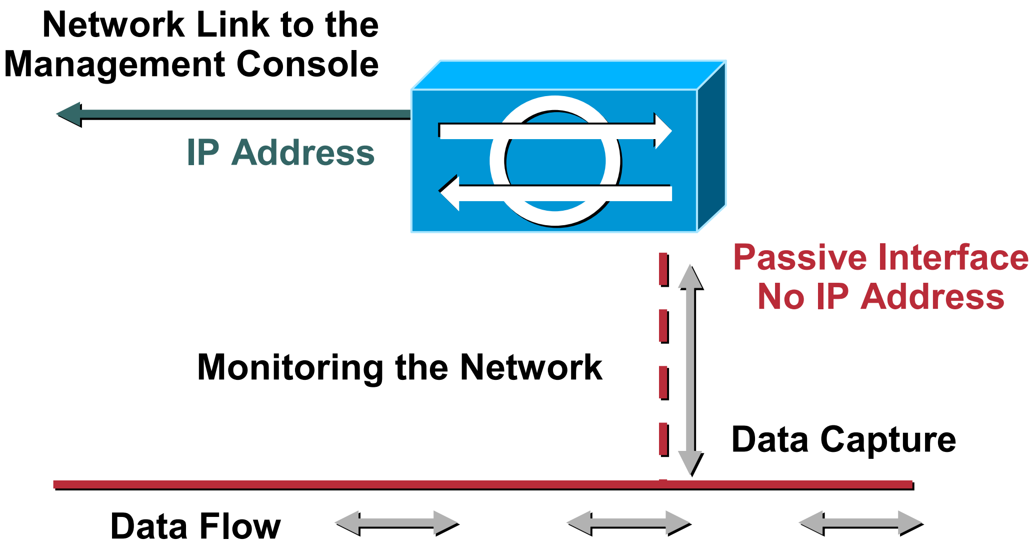
Components of IDS

- Network sensors
- Alert systems
- Command console
- Response systems
- Database of attack signatures or behaviours

Network Sensors

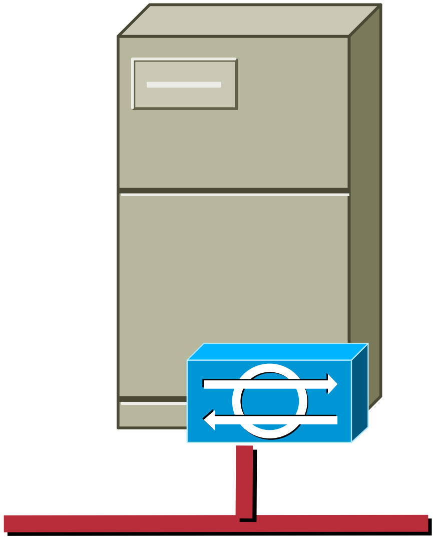
- Sensors:
  - Electronic ‘Eye’ oof the IDS
  - Hardware or software that monitors traffic in network and triggers alerts
  - Attacks detected by an IDS sensors
    - Single session attacks
    - Multiple session attacks
- Sensor Types
  - Host based
    - Server specific agents
    - Provide both packet and system level monitoring
  - Network based
    - Specialized software and/or hardware used to collect and analyse network traffic
    - Applications, modules embedded in network infrastructure

Network Sensors



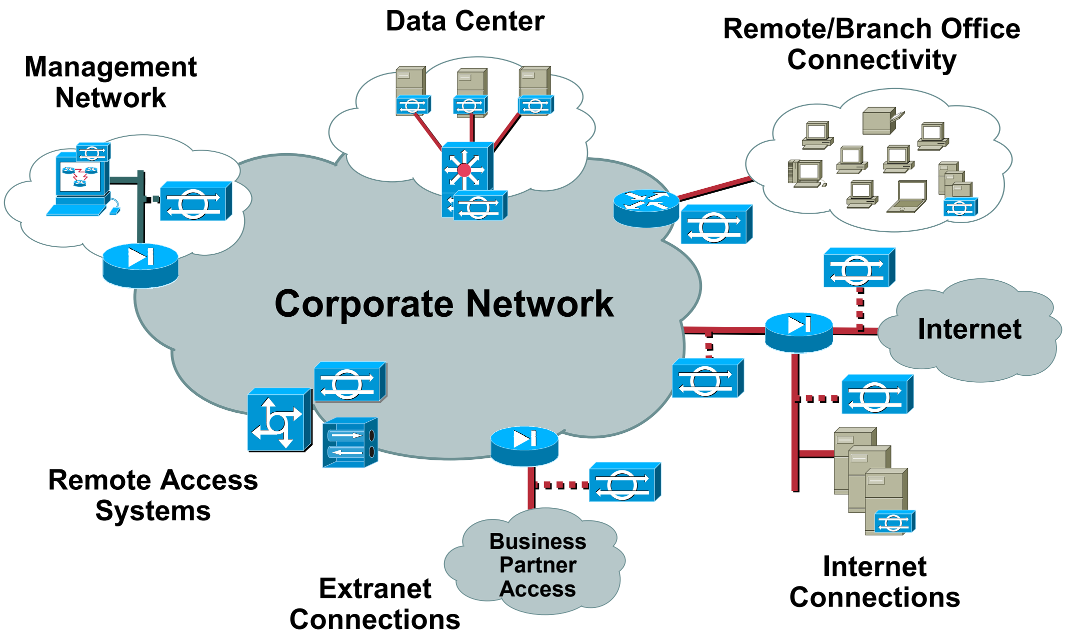
- Monitors all traffic on a given segment
- Compare traffic against well known attack patterns (signatures); also look for heuristic attack patterns (DoS, multi-host scans)
- Includes fragmentation and stream reassembly logic for de-obfuscation of attacks
- Primarily an alarming and visibility tool, but also allows active response: IP session logging, TCP reset, shunning (blocking)

Host Sensors/Agents



- Distributed Agent residing on each server to be protected
- Intimately tied to underlying operating system
  - Can allow very detailed analysis
  - Can allow some degree of Intrusion Protection
- Allows analysis of data encrypted for transport
- • Monitors kernel-level application behaviour, to mitigate attacks such as buffer-overflow and privilege escalation

Placement Strategies



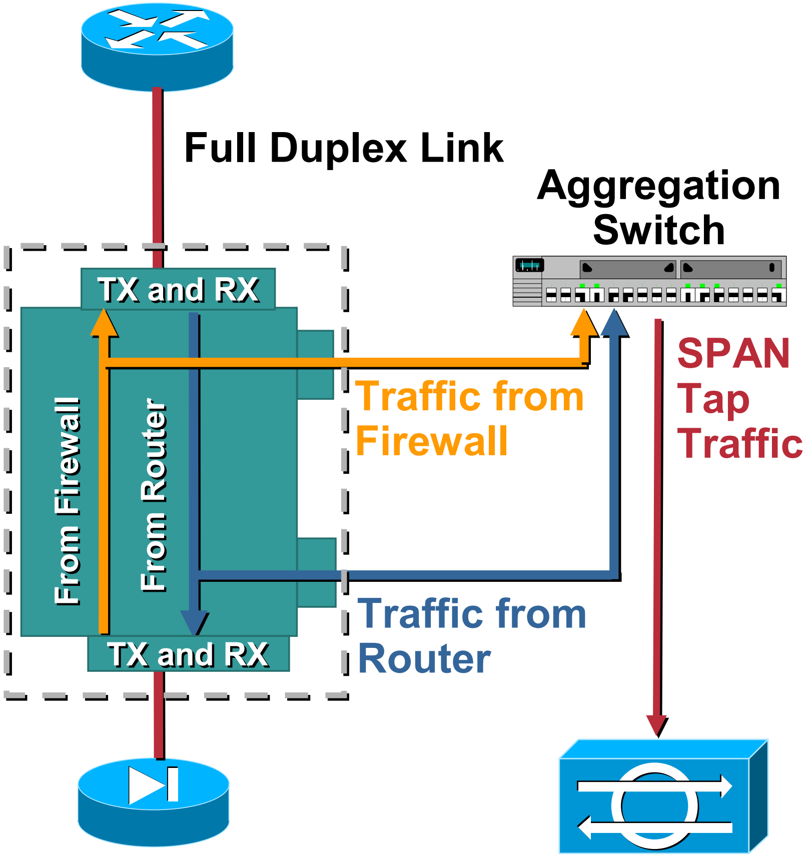
- Monitor your critical traffic
- Deploy network sensors at security policy enforcement points throughout the network
- Deploy host sensors on business critical servers
- Beware of sensor overload—sensors must be able to handle peak traffic loads

Getting Traffic to Network Sensors

- Traffic must be mirrored to network sensors (replicated)
- Options:
  - Shared media (hubs)
  - Network taps
  - Switch-based traffic mirroring (SPAN)
  - Selective mirroring (traffic capture—VACLs)

Using a Network Tap

- Tap splits full duplex link into two streams
- For sensors with only one sniffing interface, need to aggregate traffic to one interface
- Be careful of aggregate bandwidth of two tapped streams
  - Don't exceed SPAN port or sensor capacity



Network Sensors

- Sensors should be placed at common entry points
  - Internet gateways
  - Connection between one LAN and another
  - Remote access server that receives connections from remote users
  - VPN devices
- Management program console sensors
- Sensors could be positioned at either side of firewall
  - Behind the firewall is more secure position

Alert Systems

- Triggers
  - Circumstances that cause an alert to be sent

- Types of triggers
  - Detection of an anomaly
  - Detection of misuse
  - Matching of a signature

Alert Systems

- Anomaly detection
  - Requires use of profiles
    - For each authorized user of group of users
    - Describe services and resources normally used by users
  - Some IDS can create user profiles
    - During training period
  - Accuracy issues
    - False negative
    - False positive

Alert Systems

- Signature based
  - Triggers alarm based on characteristics signature of known attacks
  - IDS comes equipped with a databse of signatures
    - can start protecting the network immediately
  - Needs to maintain state information
- Other detection mechanisms
  - Traffic rate monitoring
  - Protocol state tracking
  - IP packet re-assembly

Command Console

- Provides a graphical user interface to an IDS
  - Enables administrators to receive and analyze alert messages and message log files
- IDS can collect information from security devices throughout network
- Command console should run on a computer dedicated solely to an IDS
  - Maximize the speed of response
  - Isolate the IDS from attacks

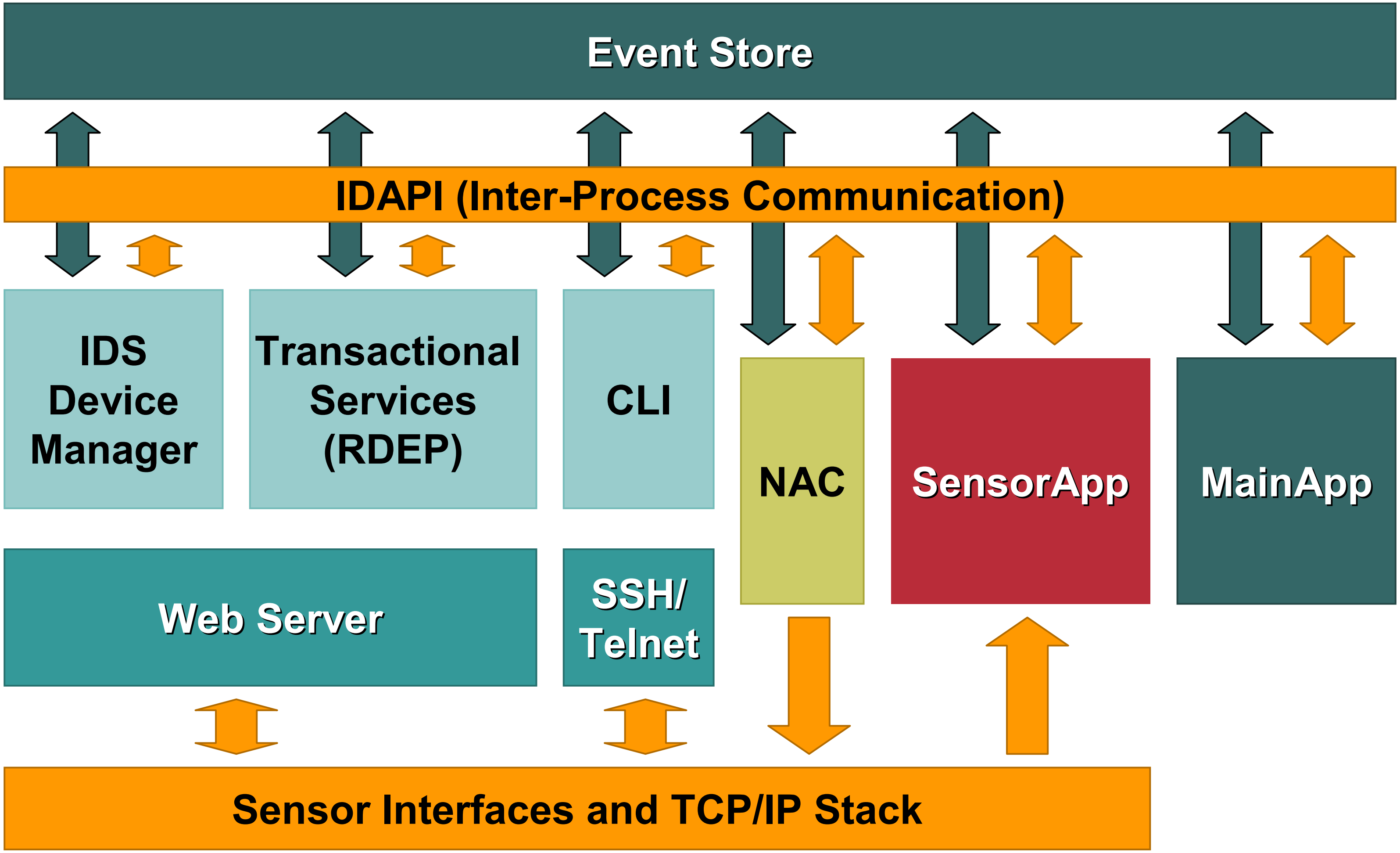
Response System

- IDS can be setup to take some countermeasures
- Response systems do not substitute administrators
  - Administrators can use their judgement to detect a false positive or false negative
  - Administrators can determine whether an alert needs to be escalated

Database of Attacks Signatures or Behaviours

- IDS don’t have the capability to use judgement
  - can make use of a source of information for comparing the traffic they monitor
- Signature or rule based
  - Reference a database of known attack signatures
  - If traffic matches a signature, it sends an alert
  - Keep database updated
  - Passive detection mode
- Anomaly based IDS
  - Store information about users in database

IDS Architecture


Event Store
IDAPI (Inter-Process Communication)
IDS Device Manager
Transactional Services (RDEP)
CLI
NAC
SensorApp
MainApp
Web Server
SSH/ Telnet
Sensor Interfaces and TCP/IP Stack

IDS Architecture

- Sensor Interfaces: Traffic inspection points
- Sensor App: “Sniffing” application
- Main App: Core IDS application
- Event Store: Storage for all events (system & alarm)
- IDAPI: Communication channel between applications
- Web Server: Services all web and SSL requirements, including the IDS Device Manager (the integrated GUI), and transactional services such as remote management and monitoring through RDEP
- SSH/Telnet: Services SSH and telnet requirements, for the CLI application
- NAC: Application for active response (shunning)

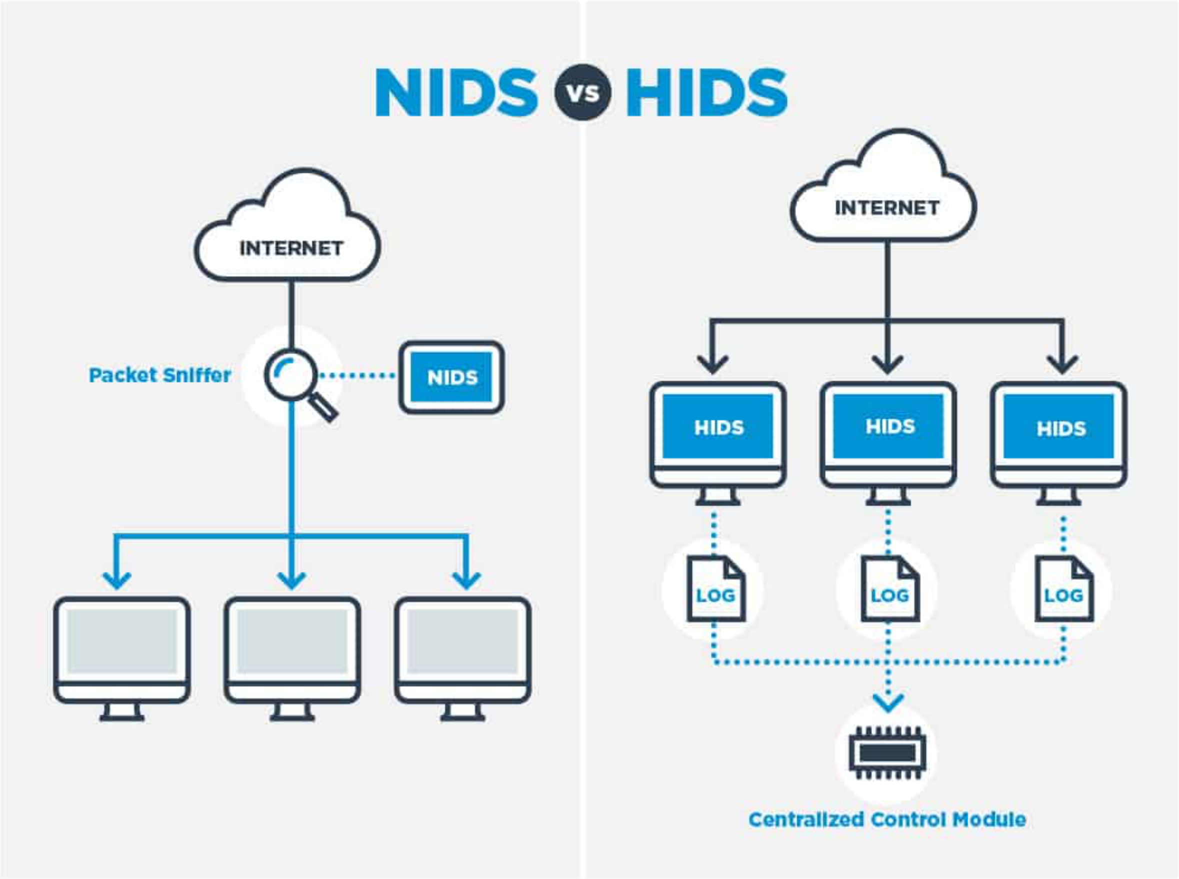
Host Based IDS (HIDS)

- Examines events on a computer in a network rather than the traffic that passes around the system.
- Mainly operates by looking at data in admin files including log and config files on the computer that it protects.
- HIDS will back up the config files so system can restore settings, should a malevolent virus loosen the security of the system by changing the setup of the computer.
- Guards root access on Unix-like platforms or registry alterations on Windows systems. **A HIDS won't be able to block these changes, but it would be able to raise alert if any such access occurs**.
- HIDS must be installed on each host it is expected to monitor for effective monitoring of overall network.
- This ensures that config changes on any of the host are not overlooked.
- A **distributed HIDS system needs to include a centralized control module**.

Network Based IDS (NIDS)

- NIDS examines the traffic on the network. A typical **NIDS** includes a packet sniffer in order to gather network traffic for analysis.
- The analysis engine of a NIDS is rule-based which supports addition, deletion and modification of rules.
- With many NIDS, the provider of the system, or the user community make rules available which can be imported into system for implementation.
- **There is no need to dump all of the traffic into files or run the whole lot through a dashboard** because it wouldn't be able to analyze all of that data.
- Rules that drive analysis in a NIDS also create selective data capture. For example, if there is a rule for a type of worrisome HTTP traffic, NIDS should only pick up and store HTTP packets that display those characteristics.
- Typically, a NIDS is installed on a dedicated piece of hardware. A NIDS requires a sensor module to pick up traffic, so it should be possible to load it onto a LAN analyzer, or may choose to allocate a computer to run the task.

NIDS v/s HIDS



- A NIDS gives a lot more monitoring power than a HIDS as it can intercept attacks as they happen, whereas a HIDS only notices anything wrong once a file or a setting on a device has already changed
- NIDS is usually installed on a stand-alone piece of equipment and doesn’t drag down the server processors
- The activity of HIDS is not as aggressive as that of NIDS and can be fulfilled by a lightweight daemon on the computer with very small load on host CPU
- Neither NIDS nor HIDS generate extra network traffic

Front-End IDS

- Placed at entry point of a network
- Monitors traffic coming to network
- Can analyze the traffic and initiate action against suspicious traffic
- Visible to outside world and is exposed to attack
- Can not monitor internal traffic

Internal IDS

- Monitors activity within network
- Can spot suspicious activities from within network
- If an attacker sends a normal packet to a compromised machine and asks it to launch DOS attack, this implementation will be able to spot it
- Well protected from outside attack
- Can learn the typical behavior of internal users and spot any sudden change in their behavior

IDS Implementation

- 7 Step process:
  - Install the IDS database
  - Gather data
  - Send alert messages
  - IDS responds
  - Administrator assesses the damage / risk
  - Follow escalation procedures
  - Log and review the event

Install the IDS Database

- IDS uses the database to compare traffic detected by sensors
- Anomaly based systems
  - Requires a training period (normally one week)
  - IDS observes traffic and compiles a network baseline
- Signature based systems
  - Can use database immediately
  - Database can be sourced from third party suppliers

Tuning the Sensors

- Understand the environment and traffic patterns
- List out potential false positives i.e. analyze each alert and classify stimulus and response
- Define policy, and policy exceptions i.e. ping sweeps generate alarms, except when coming from the management network
- Turn down severity of signatures not applicable to that environment
- Iterative process: as traffic patterns change, sensors can require re-tuning

Gather Data

- Network sensors gather data by reading packets
- Sensors need to be positioned where they can capture all packets
  - Sensors on individual hosts capture information that enters and leaves a host
  - Sensors on network segments read packets as they pass through the segment
- Sensors on network segments can not capture all packets
  - If traffic levels become too heavy

Send Alert Message

- Sensor captures a packets
- IDS software compares captured packet with information in its database
- IDS sends alert message
  - If captured packet matches an attack signature
  - Deviates from normal network behaviour

IDS Responds

- Command console receives alert messages
  - Notifies the administrator
- IDS can be configured to take action when a suspicious packet is received
  - Send an alarm message
  - Drop a packet
  - Stop and restart the network

Administrator Assesses Damage

- Administrator monitors alerts
  - Determines if countermeasures are required
- Administrator needs to fine tune the database
  - Goal is to avoid false negative by training the IDS
- Line between acceptable and unacceptable network use may not be clear always

Administrator Assesses Damage

- Administrator monitors alerts
  - Determines if countermeasures are required
- Administrator needs to fine tune the database
  - Goal is to avoid false negative by training the IDS
- Line between acceptable and unacceptable network use may not be clear always

Follow Escalation Procedures

- Escalation procedures
  - Set of actions to be followed is IDS detects a true positive
- Should be spelled out in organization's security policy
- Incident levels
  - Level 1: can be managed quickly
  - Level 2: represents a more serious threat
  - Level 3: represents the highest degree of threat

Log and Review Events

- IDS events are stored in log files or database
- Administrator should review logs
  - to determine pattern of misuse
  - administrator can spot a gradual attack
- IDS should also provide accountability
  - capability to track an attempted attack or intrusion back to the responsible party
  - some systems have built-in tracking/tracing features

Other IDS Technologies…

- Protocol-based Intrusion Detection System (PIDS)
- Application Protocol-based Intrusion Detection System (APIDS
- Hybrid Intrusion Detection System
- Code modification checkers: (Tripwire)
- Vulnerability scanners: (ISS Scanner, Nessus)

IDS Strengths and Limitations

- Strengths:
  - Can detect ever growing number of attacks
  - New signatures can be configured
  - Have become cheaper and easy to operate
  - Can operate in stealth mode to avoid attackers
- Limitations:
  - Requires strong defense else attacker can render an IDS ineffective
  - Attackers tend to gain insight into IDS working over a period of time
  - Poor sensitivity could limit accuracy
  - Someone needs to monitor IDS reports for actions

Popular IDS Products

- McAfee NSP
- Trend Micro TippingPoint
- HillStone NIPS
- Darktrace Enterprise Immune System
- NSFocus NGIPS
- H3C SecBlade IPS
- Huawei NIP
- Entrust IoTrust Identity and Data Security
- Cisco FirePower NGIPS

Firewalls v/s IDS v/s IPS

- Firewall is first line of perimeter defense. Best practices recommend that firewall be explicitly configured to DENY all incoming traffic and then you open up holes where necessary. You may need to open up port 80 to host websites or port 21 to host an FTP file server.
- Each of these holes may be necessary from one standpoint, but they also represent possible vectors for malicious traffic to enter network rather than being blocked by the firewall.
- That is where IDS would come in, the IDS will monitor the inbound and outbound traffic and identify suspicious or malicious traffic which may have somehow bypassed the firewall or it could possibly be originating from inside network as well.
- An IPS is essentially a firewall which combines network-level and application-level filtering with a reactive IDS to proactively protect the network.

Demo

- Intrusion Detection Systems

  https://www.youtube.com/watch?v=VPLSIsRegFI

- Network Intrusion Detection using Snort

  https://www.youtube.com/watch?v=iBsGSsbDMyw

- Network Intrusion Detection & Prevention Systems

  https://www.youtube.com/watch?v=hEgWPWIuq_s

Thank You

IDS Methods

- **Signature based:**
  - Monitor all the packets traversing the network
  - Compares traffic against a database of signatures or attributes of known malicious threats,
  - Works similar to antivirus software
- **Anomaly based:**
  - Monitor network traffic and compare it against an established baseline,
  - Determines what is considered normal for the network with respect to bandwidth, protocols, ports and other devices.
  - Also known as Heuristic based IDS

Signature Based IDS

- Monitors for known patterns of malicious behavior
  - Port scan i.e. same sender trying to communicate with multiple ports at same time
  - Abnormal packet sizes i.e. ICMP packet size of 65535 will crash the protocol stack
- Simple pattern matching i.e. Look for “root”
- Stateful pattern matching i.e. Decode a telnet session to look for “root”
- Protocol Decode and Anomaly detection i.e. RPC session decoding and analysis
- Heuristics i.e. Rate of inbound SYNs—SYN flood?

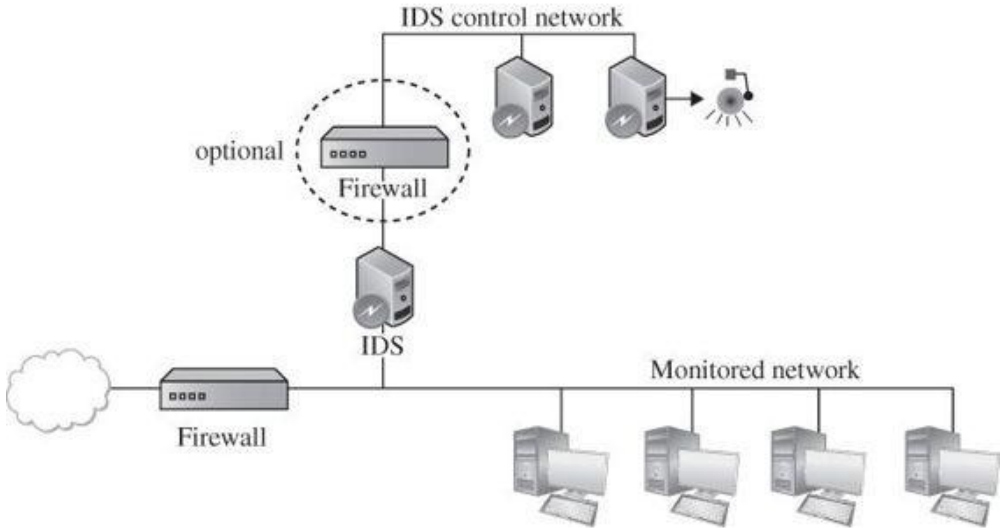
Anomaly Based IDS

- Monitors abnormal behavior:
  - One user normally performs email reading, word processing and file backup activities
  - If suddenly he starts executing administrator functions then it's suspicious – someone else might be using his account
- Monitors the system 'dirtiness' factor and raises alarm when it crosses a threshold.
- Activities classified as good/benign, suspicious, unknown
- Evaluates combined impact of asset of events
  - Ana tries to connect to Amit's machine, Amit's machine denies access (unusual)
  - Ana tries to connect to Abhay's machine, gets an open port and connects (more unusual)
  - Ana obtains listing of folder from Abhay's machine (suspicious)
  - Ana copies files from Abhay's machine (attack – raise alarm)
- Inference engine makes the decision to categorize actions and raise alarm

Inference Engine Types

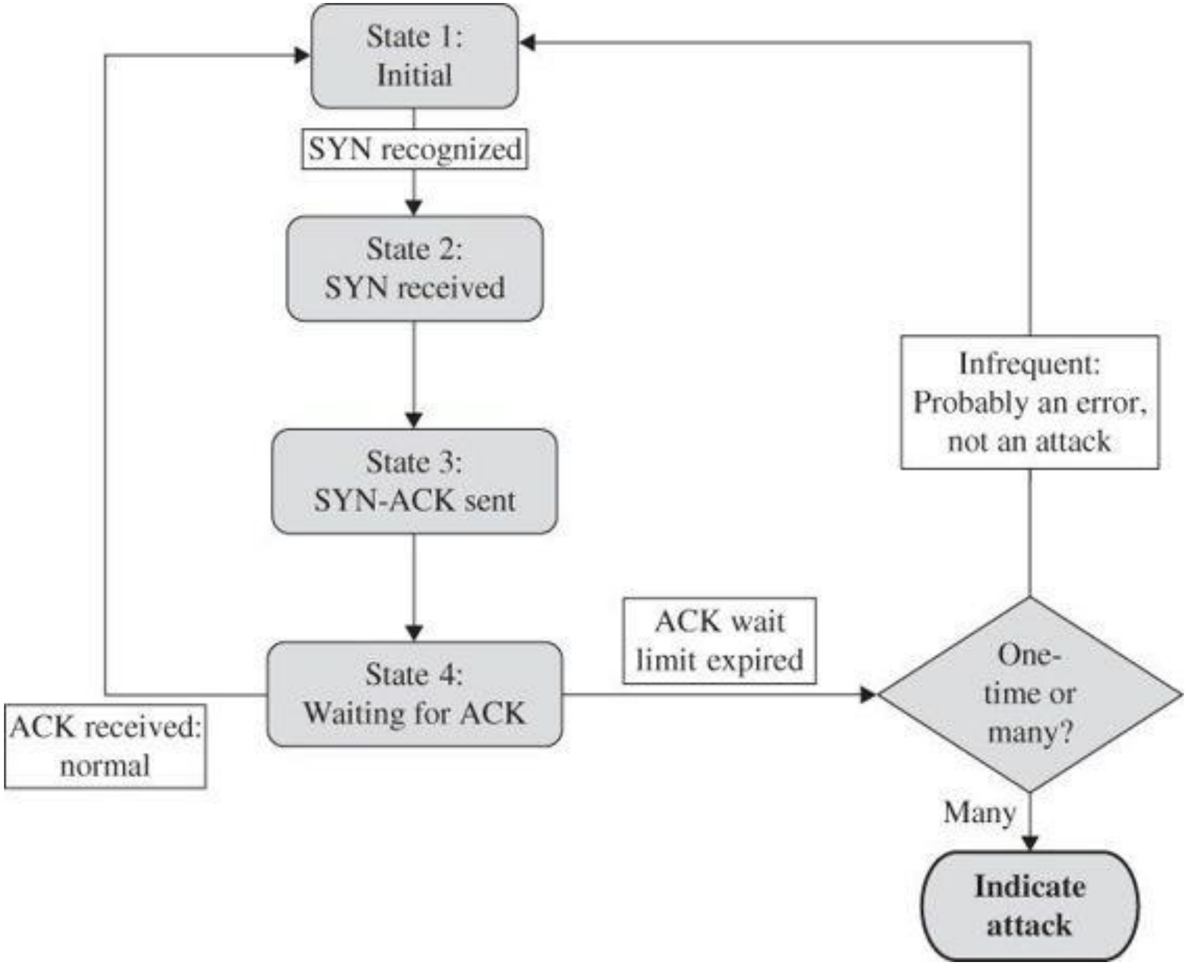
- State based
  - Monitors system going thru overall state change
  - Identify when a system has veered into unsafe state
- Model based
  - List of known bad activities
  - Each activity has a degree of bad
  - Action when an activity of certain bad degree occurs
  - Overall cumulative activities cross a certain degree of bad
- Misuse intrusion detection
  - Compare real activity with a known representation of normality
  - Ex: password file being access by utilities other than login, change password, create user etc

IDS Deployment



- IDS runs in stealth mode to avoid attack (DDOS etc)
- IDS has two network interfaces:
- A. For the network being monitored – used only for inputs – this interface is not published – it's a wiretap
- B. for alerts a separate control network interface is configured

Stateful Protocol Analysis: SYN Flood Attack


State 1:
Initial
SYN recognized
State 2:
SYN received
State 3:
SYN-ACK sent
State 4:
Waiting for ACK
ACK received:
normal
ACK wait
limit expired
One-
time or
many?
Many
Indicate
attack
Infrequent:
Probably an error,
not an attack