BITS Pilani Presentation

BITS Pilani
Pilani Campus

Jagdish Prasad
WILP

innovate achieve lead

BITS Pilani
Pilani Campus

SSZG575: Ethical Hacking
Session: 14 (Defense Processes and Tools)

Agenda

innovate achieve lead

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

Intrusion Detection System (IDS)

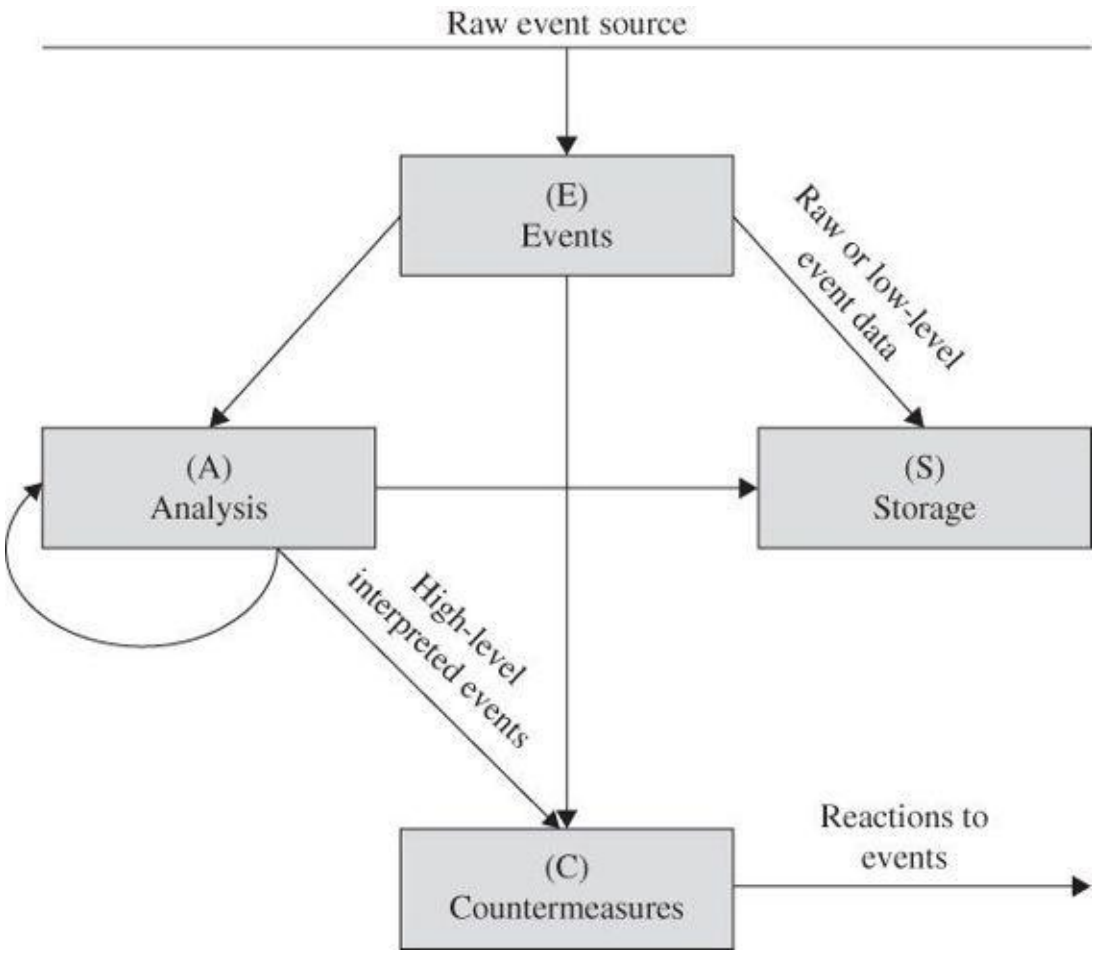
What is an IDS?

- 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)

What is the function 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

How does IDS Work?



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

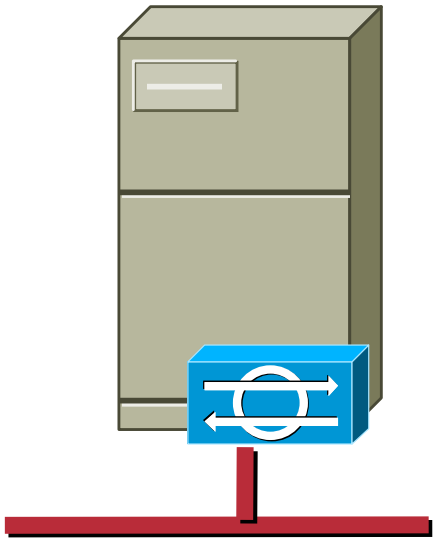
Components of IDS

- Network sensors
- Alert systems
- Command console
- Response systems
- Attack signature and behavior database

Network Sensors

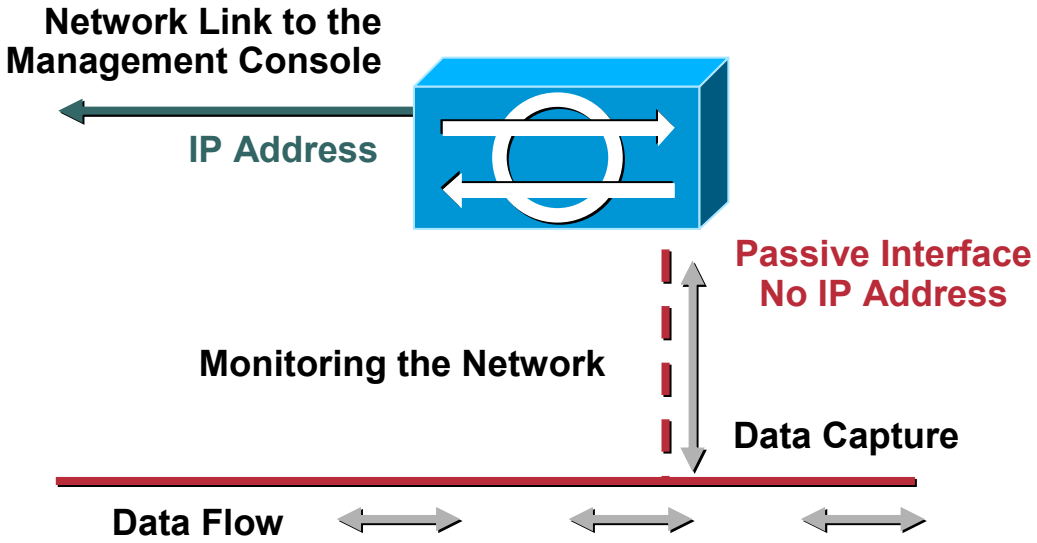
- Sensors:
  - Electronic ‘Eye’ of an IDS
  - Hardware and/or software that monitors the traffic in network and triggers alerts
  - Type of attacks detected by IDS sensors
    - Single session attacks
    - Multiple session attacks
- Sensor Types
  - Host based
    - Server specific agents
    - Provide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

Host Sensors/Agents



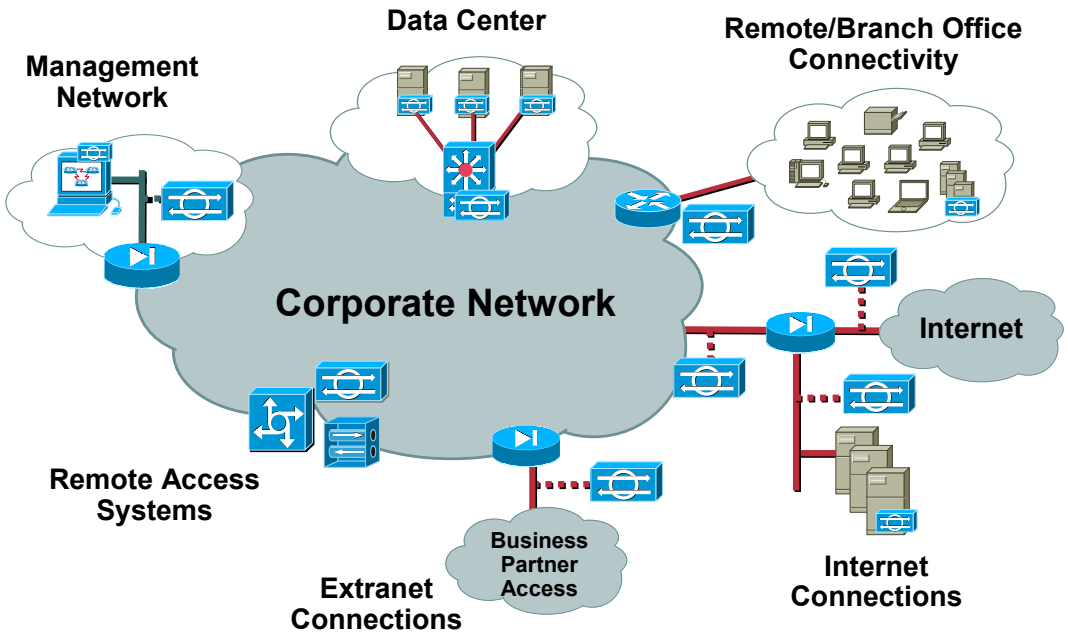
- Distributed Agent residing on each server that needs to be protected
- Closely tied to underlying operating system
  - Can allow very detailed analysis
  - Can allow some degree of Intrusion Protection
- Allows analysis of data encrypted for transport
- Monitors kernel-level application behaviour
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

Network Sensors



- Monitors all traffic on a given segment
- Compare traffic against well known attack patterns (signatures)
- 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
- Allows active response:
  - IP session logging,
  - TCP reset,
  - Shunning (blocking)

Sensor Placement Strategies



- Must monitor critical traffic
- Deploy network sensors at security policy enforcement points throughout the network
- Deploy host sensors on business critical servers
- Ensure sensor are not overloaded
  - Sensors must be able to handle peak traffic loads

Sensor Placement Strategies

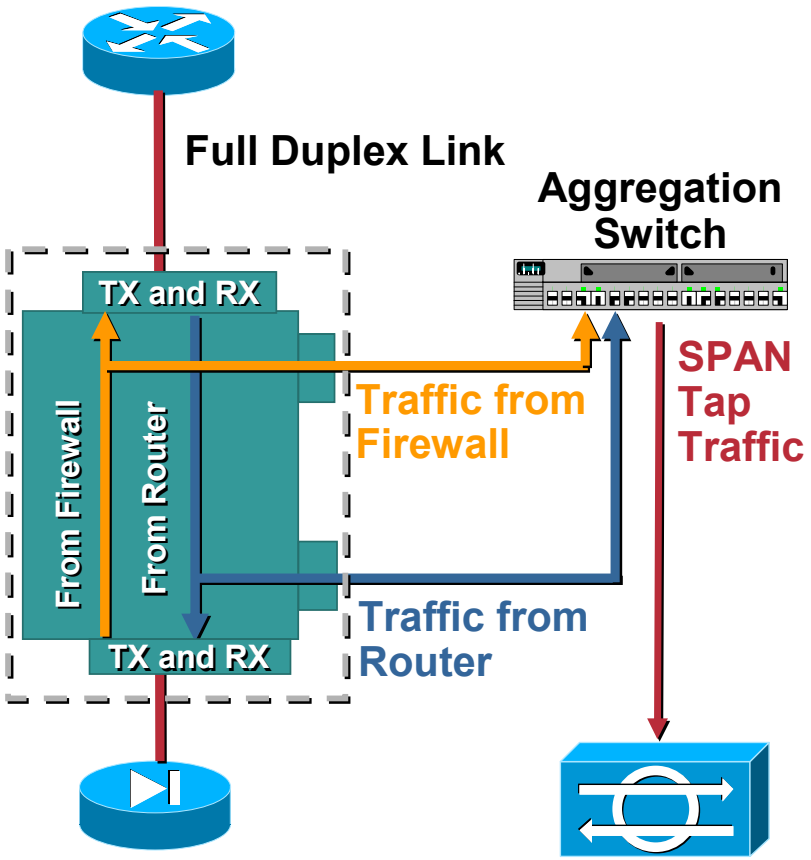
- Sensors should be placed at common entry points
  - Internet gateways
  - Connection between one LAN and another
  - Remote access server that receives connections from remote users
  - VPN devices
- Sensors could be positioned at either side of firewall
  - Behind the firewall is more secure position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

Getting Traffic to Network Sensors

- Traffic must be mirrored to network sensors (replicated)
- Options:
  - Shared media (hubs)
  - Network taps
  - Switch-based traffic mirroring (SPAN – Switch Port Analyser)
  - Selective mirroring (traffic capture – VACLs – VLAN Access List)

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



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 based detection
  - Requires use of profiles
    - For each authorized user of group of users
    - Describe services and resources normally used by users
    - Can create user profiles during pilot/training period
  - Accuracy issues
    - False negative
    - False positive

Alert Systems

- Signature based detection
  - Triggers alarm based on characteristics signature of known attacks
  - IDS comes equipped with a database of signatures
    - can start protecting the network immediately after installation
  - Maintains state information
- Other detection methods
  - 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

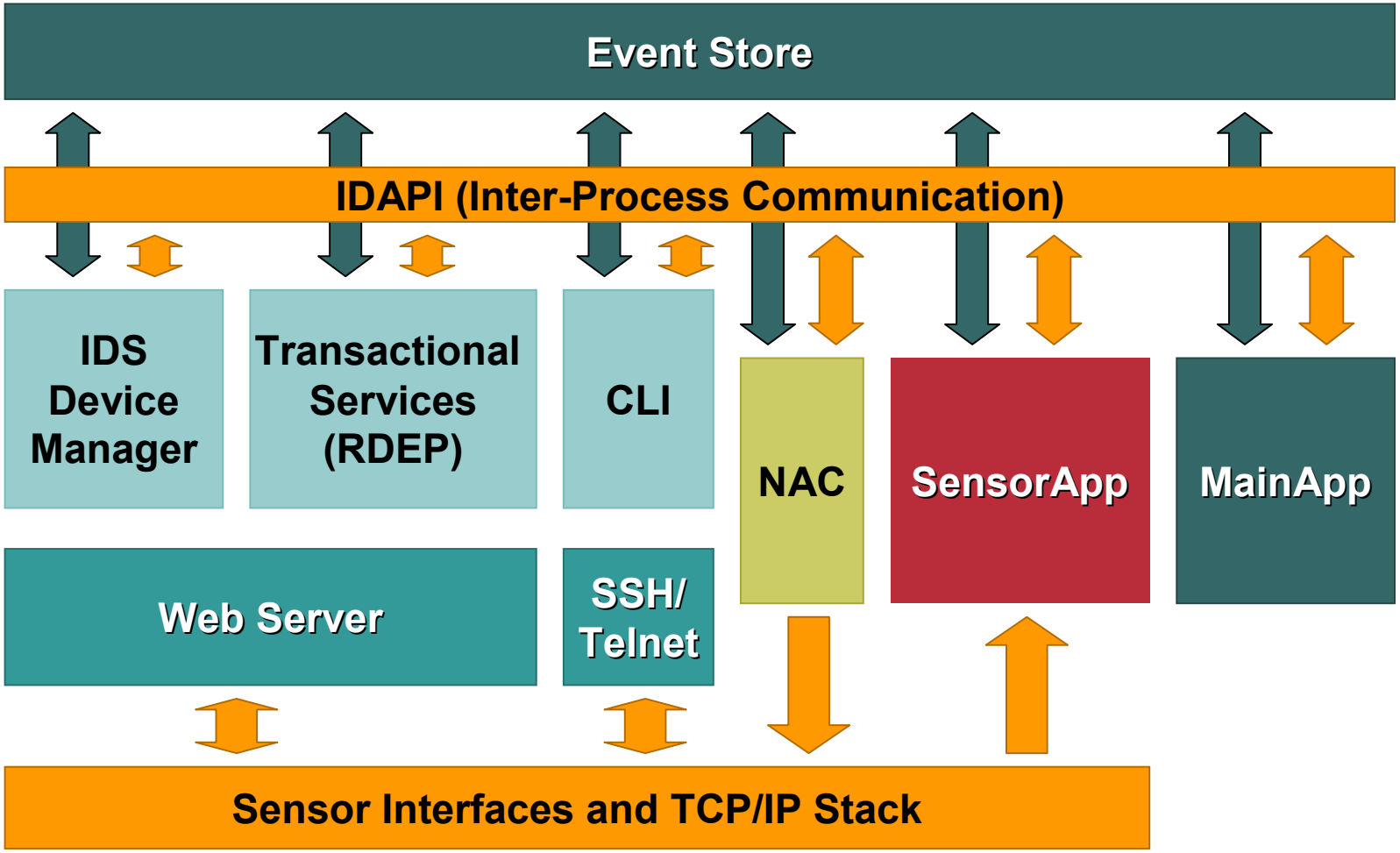
Response System

- IDS can be setup to take limited countermeasures
- Response system does 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

Attack Signature & Behaviors Database

- IDS doesn'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 then generate an alert
  - Keep database updated
  - Passive detection mode
- Anomaly based IDS
  - Store information about users and their behaviors in database

Typical IDS Architecture



IDS Architecture

innovate achieve lead

Component	Description
Sensor Interface	Traffic inspection point
Sensor App	“Sniffing” application
Main App	Core IDS application
Event Store	Storage for all events (system and alerts)
IDAPI	Communication channel between applications
Web Server	Services all web and SSL requirements, including: • IDS Device Manager (the integrated GUI) • Transactional services (Remote management and monitoring through RDEP)
SSH/Telnet	Services SSH and telnet requirements (for the CLI application)
NAC	Application for active response (shunning)

Types of IDS

- Host based
- Network based

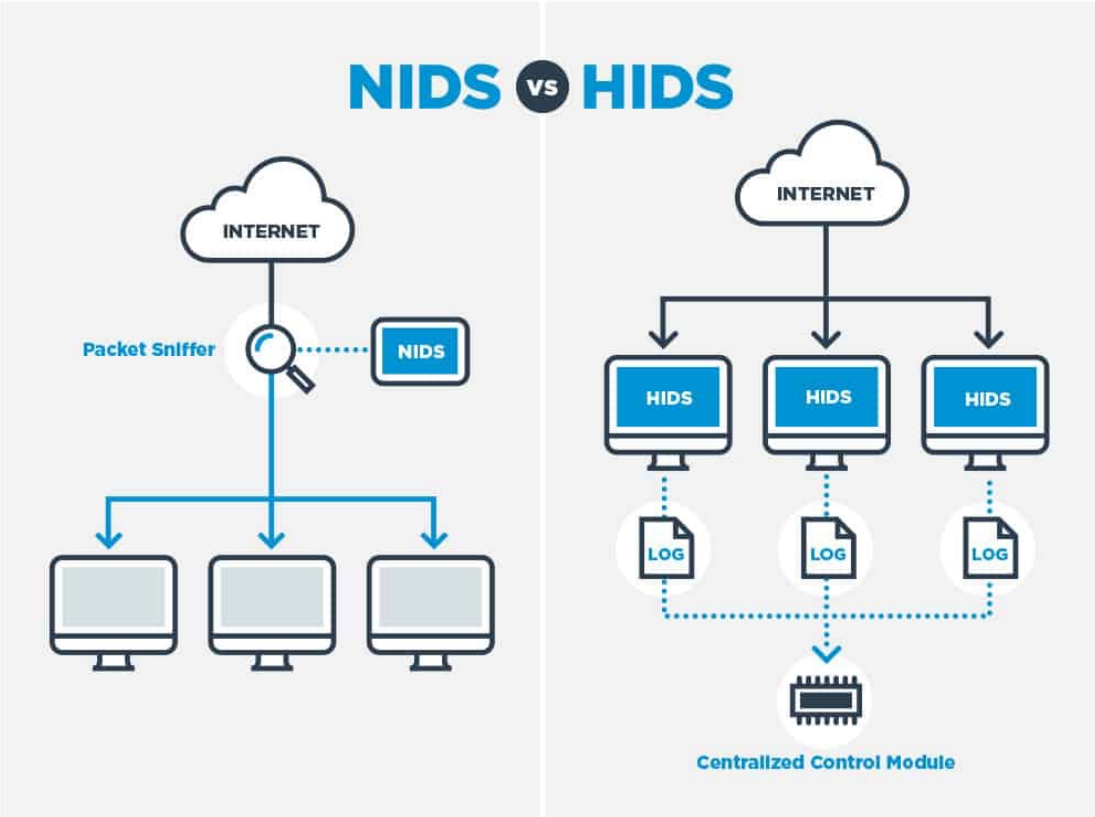
Host Based IDS (HIDS)

- Installed on the host (computer) that needs to be protected.
- Examines events on a computer in a network rather than the traffic that passes around the system.
- Looks at data in admin files including log and config files on the computer that it protects.
- Backs up the config files so system can restore settings, in case a virus attack weakens the security of the system by changing the config files.
- Guards root access on Unix-like platforms or registry alterations on Windows systems.
  - A HIDS won't be able to block the changes, but it would be able to raise alert if any such access occurs.
  - 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)

- Examines traffic on the network.
- A typical **NIDS** has a packet sniffer to collect network traffic for analysis.
- NIDS has a rule-based analysis engine with facilities to add, delete and modify rules.
  - Many NIDS supplier or user community make rules available which can be imported into system for implementation.
- Do not dump all of the traffic into files or run the whole lot through a dashboard as it wouldn't be able to analyze all of that data.
  - Rule Engine can facilitate selective data capture.
  - Example: A rule for a type of worrisome HTTP traffic, can pick up and store HTTP packets that display those characteristics.
- Typically, a NIDS is installed on a dedicated computer.
  - A NIDS requires a sensor module to pick up traffic
  - Traffic should be loaded onto a LAN analyser and allocate a computer to run the task.

NIDS v/s HIDS



- A NIDS gives a lot more monitoring power than a HIDS
  - NIDS can intercept attacks as they happen
  - HIDS notices anything wrong once a file or a setting on a device has already changed
- NIDS is installed on a stand-alone piece of equipment and doesn't drag down other computers
- HIDS actions are not resource heavy
  - Can be fulfilled by a lightweight daemon on the computer with very small load on host CPU
- NIDS or HIDS do not generate extra network traffic

NIDS Placement

FRONT END

- 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

- 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

innovate achieve lead

- 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

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
- Snort

Firewalls v/s IDS v/s IPS

- Firewall is first line of perimeter defense.
  - Firewall must be explicitly configured to DENY all incoming traffic
  - Open up holes (rules) where necessary
  - Ex: Open port 80 to host websites or port 21 to host an FTP file server
- Each of the holes may be necessary from requirement point
  - Malicious traffic conforming to firewall rules can enter network
- IDS will monitor the inbound and outbound traffic passed by firewall
  - Identify suspicious or malicious traffic that bypassed the firewall
  - Malicious traffic originating from inside network
- An IPS is a firewall + IDS which
  - Combines network-level and application-level traffic filtering
  - A reactive IDS to proactively initiate action to protect the network

SNORT: Overview

innovate achieve lead

- **SNORT** is a network based intrusion detection system which is written in C programming language.
- Developed in 1998 by Martin Roesch. Now developed by Cisco.
- It is free open-source software.
- It can also be used as a packet sniffer to monitor the system in real time.
- The network admin can use it to watch all the incoming packets and find the ones which are dangerous to the system.
- It is based on library packet capture tool.
- The rules are fairly easy to create and implement and it can be deployed in any kind on operating system and any kind of network environment.
- The main reason of the popularity of this IDS over others is that it is a free-to-use software and also open source because of which any user can able to use it as the way he want.
- Ref: https://www.snort.org

SNORT: Features

- Real-time traffic monitor
- Packet logging
- Analysis of protocol
- Content matching
- OS fingerprinting
- Can be installed in any network environment.
- Creates logs
- Open Source
- Rules are easy to implement

SNORT: Basic Usages

innovate achieve lead

- **Sniffer Mode –**
  To print TCP/IP header use command **./snort -v**
  To print IP address along with header use command **./snort -vd**
- **Packet Logging –**
  To store packet in disk you need to give path where you want to store the logs. For this command is**./snort -dev -l ./SnortLogs**.
- **Activate network intrusion detection mode –**
  To start this mode use this command **./snort -dev -l ./SnortLogs -h 192.127.1.0/24 -c snort.conf**

SNORT: Installation Steps (Linux)

- **Step-1:** wget https://www.snort.org/downloads/snort/snort-2.9.15.tar.gz
- **Step-2:** tar xvzf snort-2.9.15.tar.gz
- **Step-3:** cd snort-2.9.15
- **Step-4:** ./configure –enable-sourcefire && make && sudo make install

SNORT: Demo Video

- Network Intrusion Detection and Prevention System - Kali Linux - Cyber Security

  https://www.youtube.com/watch?v=vLVdfAJ1Tr4

-

Demo

- Network Intrusion Detection using Snort
  https://www.youtube.com/watch?v=iBsGSsbDMyw
- Intrusion Detection Systems
  https://www.youtube.com/watch?v=VPLSIsRegFI
- Network Intrusion Detection & Prevention Systems
  https://www.youtube.com/watch?v=hEgWPWIuq_s
- Suricata Network IDS/IPS
  https://www.youtube.com/watch?v=S0-vsjhPDN0

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?

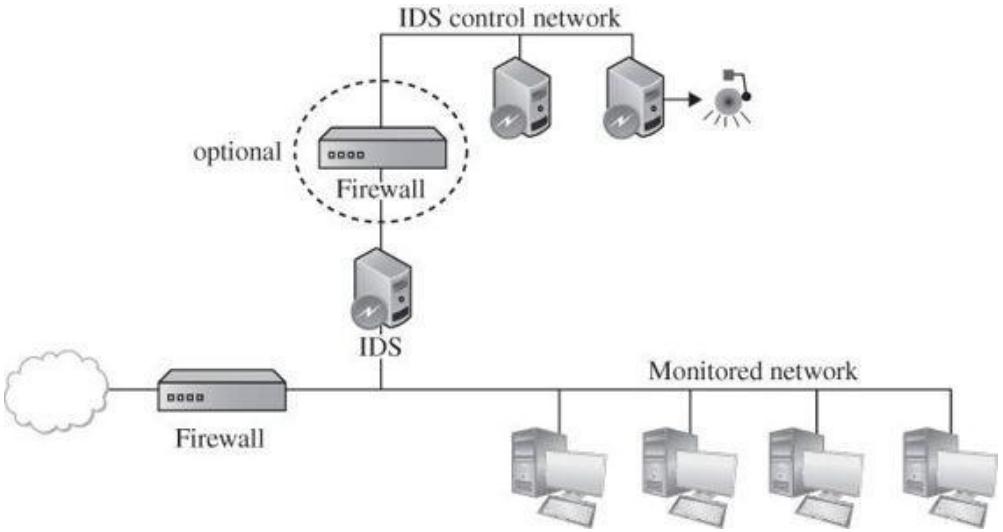
Anomaly Based IDS

- 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