Shri Vile Parle Kelvani Mandal's
DWARKADAS J. SANGHVI COLLEGE OF ENGINEERING
Approved by AICTE and Affiliated to the University of Mumbai
Department of Electronics & Telecommunication Engineering

DCE MINI PROJECT REPORT ON INTRUSION DETECTION SYSTEM

GROUP MEMBERS:
SANJEET KRISHNA 60002160050
ATULYA KUMAR 60002160054
CRISPIN LOBO 60002160056

TEACHER INCHARGE:
PROF VISHAKHA KELKAR
PROF ARCHANA CHOUDHARI

CERTIFICATE

This is to certify that M/S. _____, SAP ID _____ of TE EXTC 1: has submitted their Mini Project for Data Compression and Encryption for the Academic Year 2018-2019.

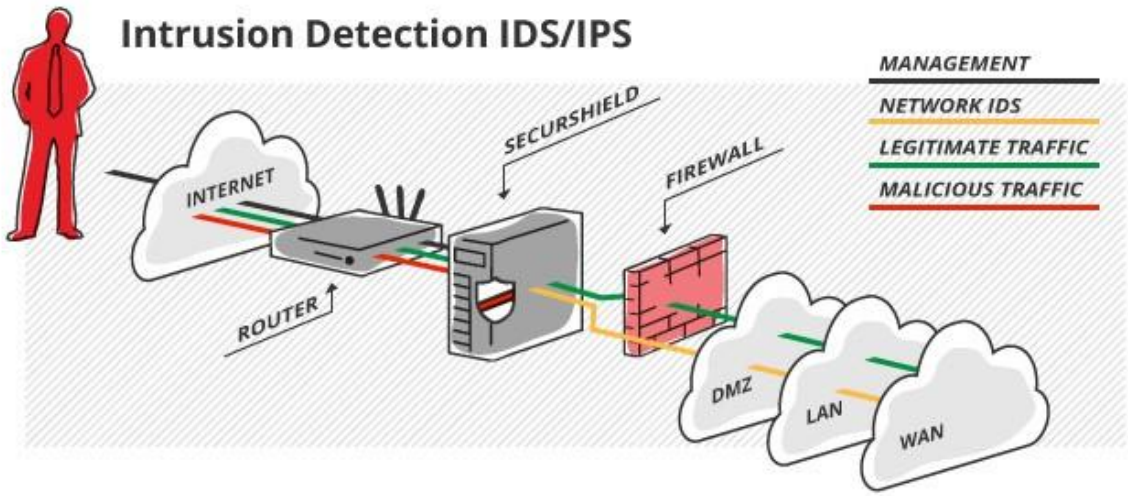
Guide

Examiner

Head of Department
EXTC Department

Introduction:

Intrusion detection is a technique of detecting unauthorized access to a computer system or a computer network. Intrusion prevention, on the other hand, is the art of preventing an unauthorized access of a system's resources. The two processes are related in a sense that while intrusion detection passively detects system intrusions, intrusion prevention actively filters network traffic to prevent intrusion attempts.



An intrusion detection system (IDS) is a system used to detect unauthorized intrusions into computer systems and networks. Intrusion detection as a technology is not new, it has been used for generations to defend valuable resources.

When designing an IDS, the mission is to protect the data's

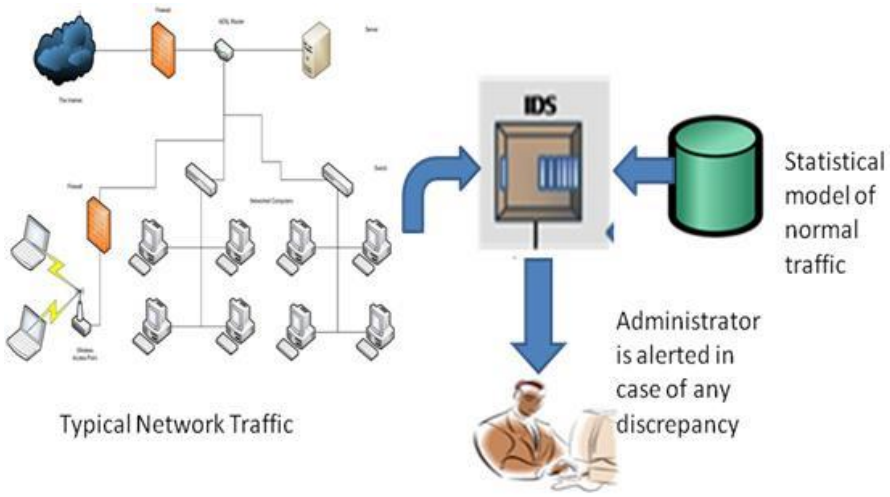
- **C**onfidentiality- read
- **I**ntegrity- read/write
- **A**vailability- read/write/access

Three models of intrusion detection mechanisms:

1. Anomaly-based detection
2. Signature-based detection
3. State Protocol Analysis

1. Anomaly based Detection –

Anomaly based systems are “learning” systems in a sense that they work by continuously creating “norms” of activities. These norms are then later used to detect anomalies that might indicate an intrusion.



Advantages:

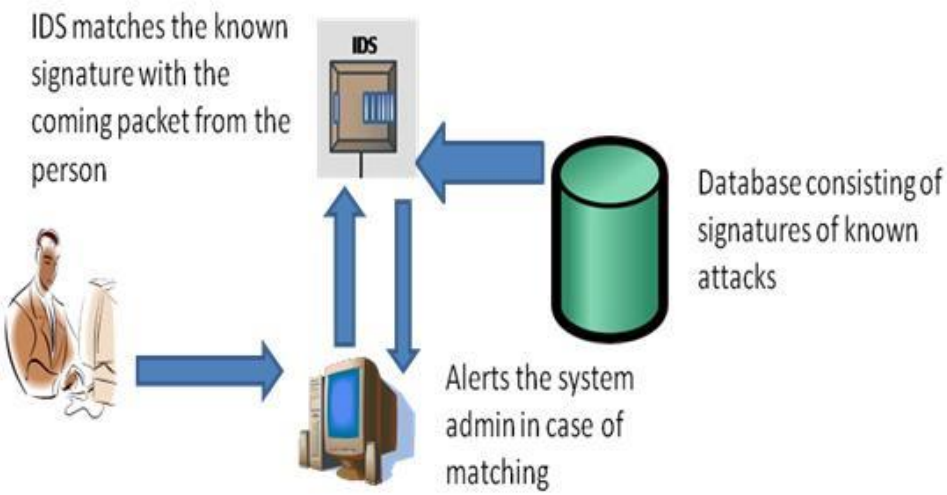
- Conducts a thorough screening of what comes through
- “Learning system” i.e. observes and checks deviation of normal network

Disadvantages:

- False alarms due unpredictable behavior of user and network.
- Painstaking slow

2. Signature based Detection -

- The misuse detection concept assumes that each intrusive activity is representable by a unique pattern or a signature so that slight variations of the same activity produce a new signature and therefore can also be detected.
- Identification engines perform well by monitoring these patterns of known misuse of system resources.

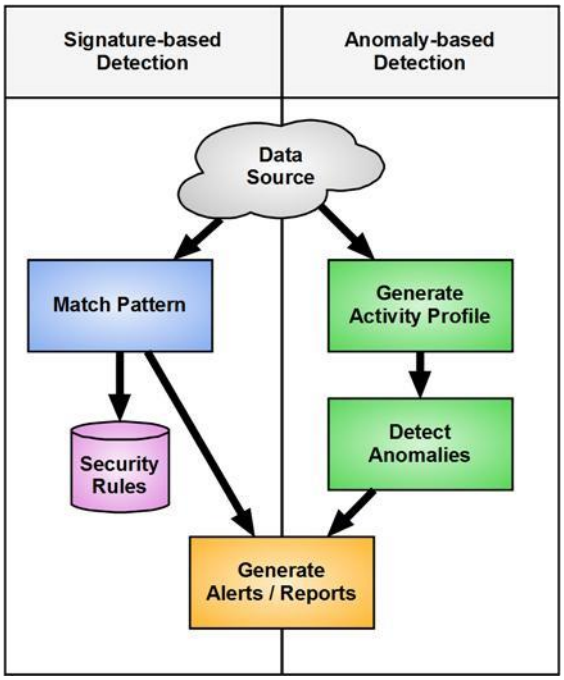


Advantages:

- Very accurate
- The systems are fast since they are only doing a comparison between what they are seeing and a predetermined rule.

Disadvantages:

- Can detect only known attacks, therefore cannot identify new attacks efficiently.
- Constant updating of attack pattern is required.



3. State Protocol Analysis

- Unlike the previous methods this protocol relies on Vendor developed universal profiles
- The stateful protocol analysis means the IDPS is able to check the network, applications and protocols that are pre defined in them. It can identify unexpected sequence of threats in form of commands.

Disadvantages:

- Extensively resource demanding

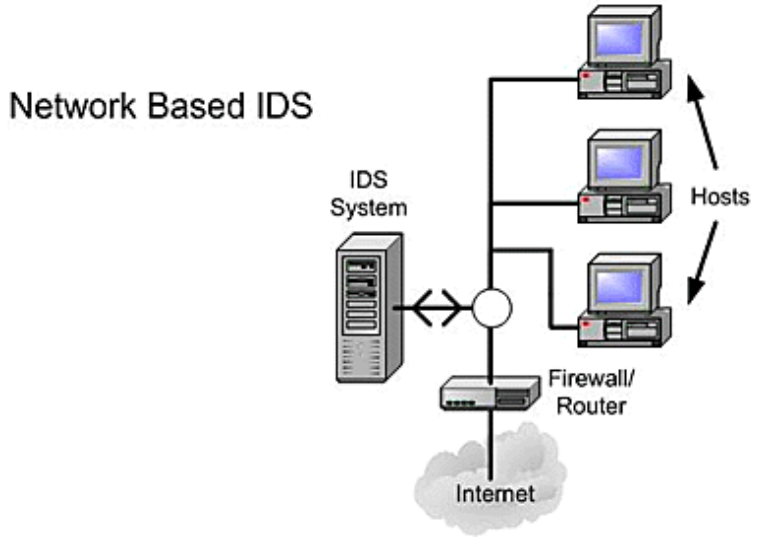
Types of Intrusion Detection Technologies

Intrusion detection systems are classified based on their monitoring scope:

1. Network-based intrusion detection
2. Host-based detections.

Network-Based Intrusion Detection Systems (NIDS)

- NIDSs have the whole network as the monitoring scope. They monitor the traffic on the network to detect intrusions.
- NIDs detects attacks by capturing and analyzing packets and indicates if there is any malicious data present
- It can be installed in servers, workstations, personal computers etc



Advantages

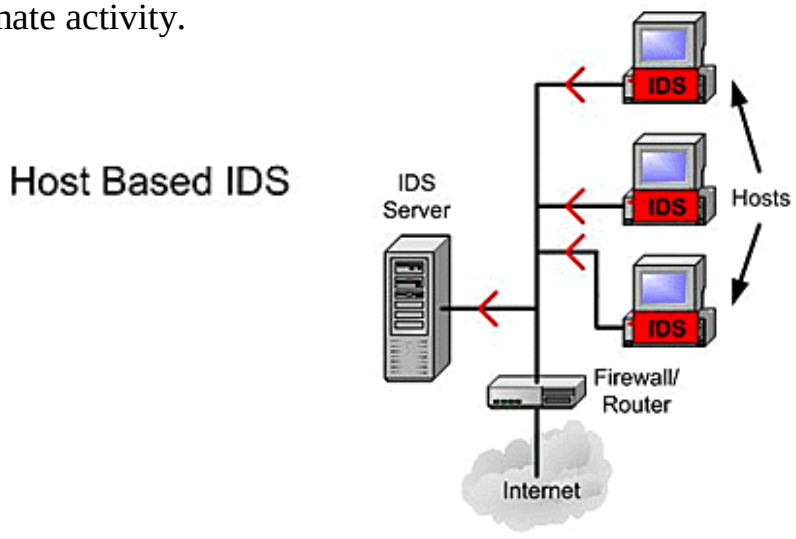
- Can monitor a large network
- Listens to the network but doesn't interfere in the network
- NIDs can be made invisible to the attackers
- Uses live network data for real time attack detection
- It is operating system independent

Disadvantages

- Cannot analyse the network if it is in encrypted format
- Usually only detects the initial level of attack rather than the whole process
- The busier the network gets the harder it is to monitor

Host-Based Intrusion Detection Systems (HIDS)

- Host-based intrusion detection is the technique of detecting malicious activities on a single computer.
- A host-based intrusion detection system, is therefore, deployed on a single target computer and it uses software that monitors operating system specific logs including system, event, and security logs on Windows systems and syslog in Unix environments to monitor sudden changes in these logs.
- When a change is detected in any of these files, the HIDS compares the new log entry with its configured attack signatures to see if there is a match. If a match is detected then this signals the presence of an illegitimate activity.



Advantages

- Helps detect Trojan horse or other attacks that creates a software integrity violation
- HIDS analyse most of the encrypted network traffic
- It is able to detect the nature of attack completely

Disadvantages

- They are difficult to manage as they are installed individually on all hosts
- HIDs might need separate storage space on the host system to store logs and other network data
- They are not suitable for detecting network denial of service and scan attacks because it does not have control over the overall system. It only checks those packets received by individual host.

Implementing an Intrusion Detection System

An effective IDS does not stand alone. It must be supported by a number of other systems. Among the things to consider, in addition to the IDS, in setting up a good IDS for the company network are:

- Operating Systems. A good operating system that has logging and auditing features. Most of the modern operating systems including Windows, Unix, and other variants of Unix have these features. These features can be used to monitor security critical resources.

- Services. All applications on servers such as Web servers, e-mail servers, and databases should include logging/auditing features as well.

- Firewalls. A good firewall should have some network intrusion detection capabilities.

- Network management platform. Whenever network management services such as OpenView are used, make sure that they do have tools to help in setting up alerts on suspicious activity.

A Real intrusion detection system