ASSIGNMENT NO. 8

* Aim

Use the snort intrusion detection package to analyze traffic and create a signature to identify problem traffic.

* Theory

Intrusion Detection System defined as tools, methods, and resources to help identify, assess or report unauthorized or unapproved network activity. It can also detect insider attacks, violations made and other threats.

Components of Intrusion Detection System

It consists of management console and sensors. Management console is the management and reporting console. Sensors are agents that monitor hosts or networks on a real time basis. IDS has database of attack signatures. In case it finds a match, it reports the activity to management console. The sensor can then take different actions.

Types of Intrusion Detection Systems

There are broadly two types. These are

1) Host Based Intrusion Detection System

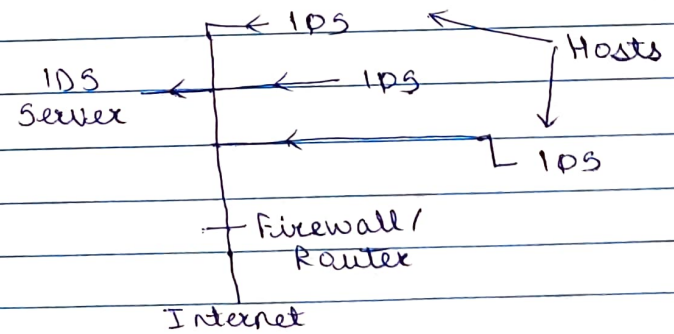
It monitors and analyzes the internals of a computing system as well as the network packets. It monitors all dynamic behaviour. It can also help to detect which program accesses what resources.

Monitoring dynamic behaviour

Many computer users have encountered tools that monitor dynamic system behaviour in form of anti-virus packages.

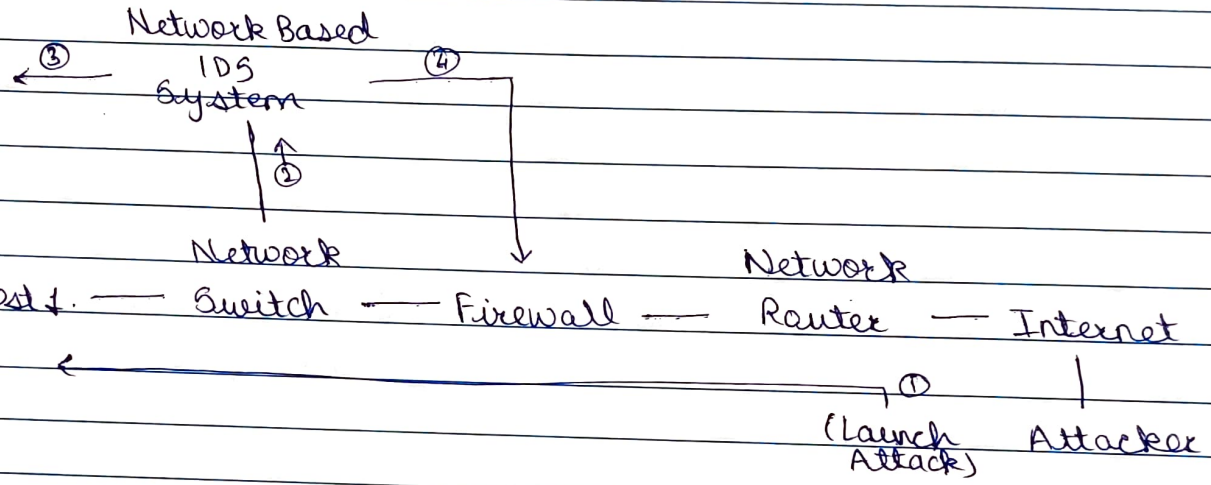
These spend a lot of time looking at who is doing what inside a computer and whether a program should have access to particular resource of system.
The principle operation of HIDS depends on fact that the successful intruders will generally leave a trace of their activities and will establish their 'ownership' at times. In theory, computer users have ability to detect any such modifications.
Ideally a HIDS works in conjunction with NIDS, in order to find out about whether a network intruder has been successful or not at a targeted host. Most successful intruders, on entering a target machine, apply best security technique practices to secure the system they have infiltrated, leaving only their backdoor open, so that other intruders can not take over.

Technique: In genral, HIDS uses a database of system object it should monitor. It could also check appropriate regions of memory. During the communication establishment phase and while transferring data requested by client, the hosts' server and client exchanges a passphrase to verify their identity. Based upon that object is created. For each question, HIDS will usually remember attributes and create checksum of some kind and store it in database.



-Host Based IDS

2) Network Intrusion Detection System
It identifies intrusions by examining network traffic and monitors multiple hosts. It gains access by connecting to hub, network switch configured.



3) Hybrid Intrusion Detection System
HIDS combines one or more approaches. Agent data is combined with network information. Example is Prelude.

Passive System v/s Reactive System
In passive system, IDS sensor detects a potential security breach, logs the information and signals an alert on console.
In reactive system, the IDS responds to suspicious activity by resetting the connection it believes to be suspicious or by reprogramming.
Though these both relate to network security

Signature based vs Anomaly Based Detection
This detection technique uses specifically known patterns

to detect malicious code. These specific patterns are called signatures.
Anomaly dection is a technique designed to detect abnormal behaviour in a system.

* Conclusion
Thus we have studied Intrusion Detection System and it's types.

* FAQs

Que1: What is Intrusion Detection System?
→ It is a monitoring system that detects suspicious activities and generates alerts when they are detected.

Que2: What are different types of IDS?
→ Network IDS, Host IDS, Protocol-based IDS are few examples

Que3: What is Host Intrusion Detection System?
→ It is a system that monitors the computer infrastructure on which it is installed, analyzing traffics, etc.

Que4: Why is IDS required in today's computing environment?
→ It is necessary system to monitor and alert attacks on cloud.

Que5: Are there any tools to visualise the data from IDS?
→ A tool to visualise data from IDS is CyberVTI: Cyber Visualisation Tool for Intrusion Detection.