BACHELOR OF COMPUTER SCIENCE

Network Security

Intrusion Detection Systems

Kenneth Thilakarathna

UNIVERSITY OF COLOMBO SCHOOL OF COMPUTING

Intended Learning Outcomes (ILOs)

The lesson introduces you to Intrusion Detection Systems (IDS) by going through its need, currently used common Intrusion Detection methods and technologies.

After completing this session, related activities, and assignments, you should be able to:

- **LO-01** Describe security threats, mechanisms, protocols and services in computer networks
  - **LO-01-01** Explain importance of Intrusion Detection Systems for an organization
  - **LO-01-02** Explore further knowledge on intrusion detection.

Intended Learning Outcomes (ILOs)

- **LO-02** Analyze and evaluate the implementation and functioning of network applications and decide on their suitability from the security point of view.
  - **LO-02-01**Analyse and evaluate Intrusion Detection Systems' requirements
- **LO-03** Design and implement applications that provide or use security services in computer networks
  - **LO-03-01** Design network to place Intrusion Detection Systems
  - **LO-03-02** Deploy a basic IDS

Lesson Plan

- Why Intrusion Detection Systems are needed?
- What is an IPS?
- Network based IDS/IPS and Host based IDS/IPS
- IDS/IPS placement
- Network based IDS/IPS details
- Host based IDS/IPS details
- IDS/IPS attack detection methods
- Advantages and disadvantages of IDS/IPS types based on the location
- Actions based on IDS response
- `snort`, an Open Source IDS

Who is an intruder?

A person or program who attempts to have unauthorised access to a system or sub system or ... to damage, get unauthorised information, disturb, etc.

Person can be both outsider or insider

program can be a virus, warm, exploit, or even a software accessing a provided service may be through an API.

Why Intrusion Detection Systems (IDS)?

- Detect intruder or malicious attacks. Could be both internal or external.
- Document existing and trends of threats to an organisation.
- Mechanism for detecting information security policy violations to certain extend.
- Provide a source to take preventive mechanisms either automated or manual.

Real world IDS examples

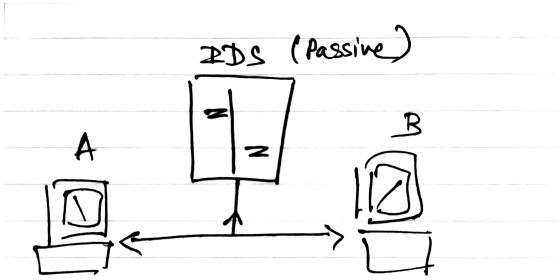
- Car alarms
- Fire detectors
- Surveillance systems

What is an IPS ?

Intrusion Detection and Prevention System / Intrusion Prevention System.

While IDS only detect intrusions passively, IPS can prevent intrusions actively.

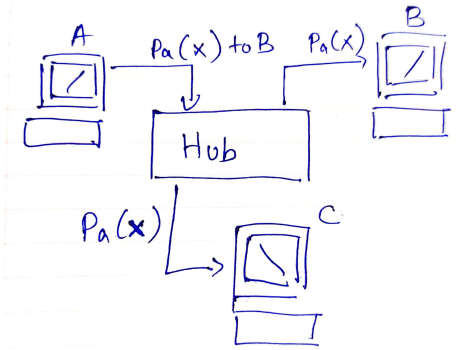
What does it mean by passive?



Scanned with CamScanner

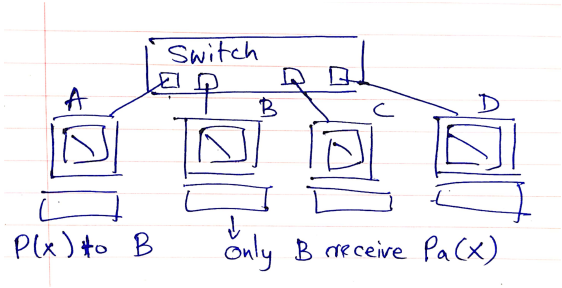
How IDS sniff packets?

Hubs



Scanned with CamScanner

Switch



Scanned with CamScanner

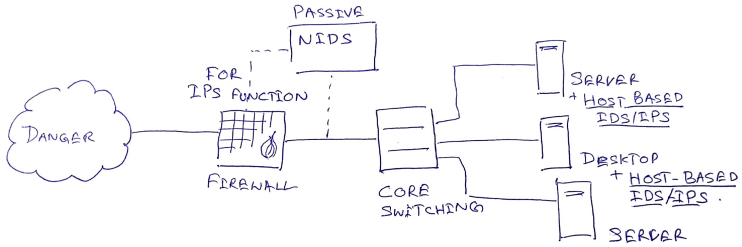
How IDS sniff packets in packet switched environment?

- Port mirroring (passive)
- Tapping (passive)
- In line (active)

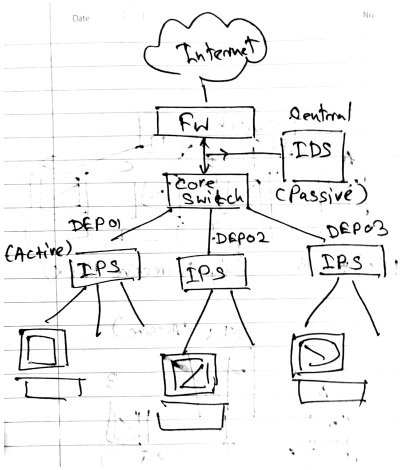
IDS / IPS classification based on position

- Network based
  - Active - In-line : e.g. Snort + IPTables
  - Passive : e.g. Snort
- Host based
  - Active - In-line : End point protection solutions.
  - Passive : OSSEC

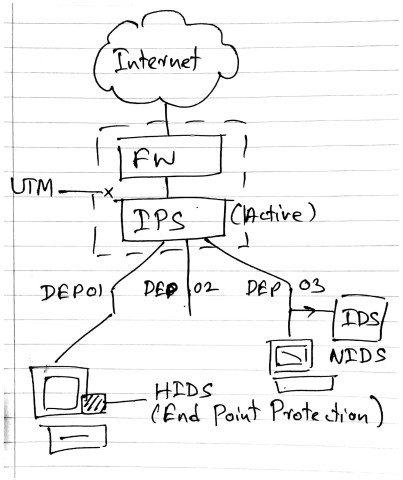
Example positioning of NIDS and HIDS



Positioning



Positioning



Attack identification

- False negatives
- False positives
- True negatives
- True positives

Network based IDS/IPS

Installed at a place where it can watch the network traffic going in and out of a particular network.

Could be a computer (software IDS) or network appliance.

Generally look for attack patterns to identify intrusions (Signatures).

- Protocol verification
- Payload verification (content)
- Communication pattern matching for intrusive activities

Network based – Software IDS

- Less cost compared to appliance
- Can upgrade hardware easily
- Limited amount of features
- Available as freeware or open source solutions – e.g. snort
- May need expert knowledge to install and use

Network based – IDS appliance

- Expensive compared to software solutions
- Optimised for the task and performance
- Less OS related vulnerabilities
- More features and fine grained solutions
- Easy deployment compared to software solutions
- Cater high availability requirements at hardware level

Host based IDS/IPS

- Deployed on a computer/server which will monitor activities within only that server
- Generally can be defined as change detection based on a baseline system
  - File changes
  - CPU/memory or other resource utilisation
  - Monitoring logs
  - etc.
- Technologies overlap – Anti Virus Guards also do tasks of HIDS such as monitoring dynamic behaviour – e.g. System state changes due to virus activity

IDS/IPS attack detection methods

Signature based

- Based on known attack pattern database
- Cannot detect new attacks or attacks due to zero day vulnerabilities
- Faster

Anomaly based

- Comparatively resource intensive
- Need some time to setup as there is a training/learning process
- May generate many false positives
- Possibility is there to detect new types of attacks or attacks due to zero day vulnerabilities

Advantages of Network based IDS/IPSs

- Fewer devices can be used to monitor a large network thus ease of management (depends on the network design)
- NIDS is generally a passive device thus could be implemented/deployed in existing network without much interruptions. However, when it comes to IPS, there could be interrupts but of course there are automated bypass mechanisms which allows the device to be bypassed upon a failure.
- Less vulnerable for direct attacks

Disadvantages of Network based IDS/IPSs

- Since, vast volume of network traffic will pass through the device may fail to recognise attacks at some rare situations
- Require access to all traffic to apply the protection entirely. Attacks may be formed from different networks that IDS may not have access to which will go undetected.
- Cannot detect if an attack was successful or not
- Will have a tough time with fragmented packets
- Cannot analyse encrypted protocols if encryption keys are not provided.
- If active NIPS is used, the network performance will depend on the performance of NIPS.

Advantages of Host based IDS/IPS

- The traffic that are encrypted over network passed undetected by NIDS may be available to analyse as the system is deployed locally in the host machine
- Can detect inconsistencies based on the log files or configuration file changes which is not possible in NIDS
- Processing power available is more compared to NIDS

Disadvantages of Host based IDS/IPS

- Number of deployments will make the management difficult
- Vulnerable for direct and host attacks
- Non host devices under attack cannot be detected
- Can be intrusive to the performance of the host machine

Actions based on IDS/IPS Responses

- Triggering alarms or notifications
- Invoke:
  - Additional data collection
  - Network modification e.g. directing traffic to an Honeypot
  - Defined preventive measures
  - Triggering an incident management process

Components of Snort - Open Source IDS

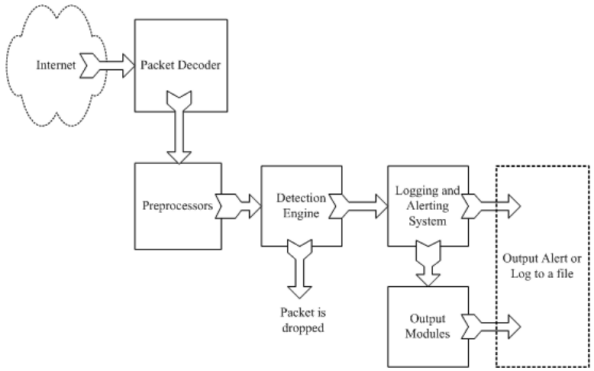


Figure: Ref: Intrusion detection systems with Snort - Rafeeq Ur Rehman

Components of Snort - Open Source IDS cont ...

Decoder

- Get the packets from different types of network interfaces and direct it to preprocessor or detection engine.

Preprocessor

- Defragmentation of packets (Max Transfer Unit in Ethernet defaults to 1500 bytes)
- re-assemble TCP streams
- Decode HTTP URI

Detection engine

- Most important part of the system
- Could be rule based or anomaly based

Components of Snort - Open Source IDS cont ...

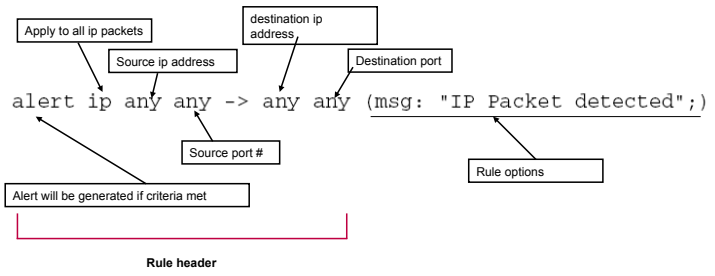
Logging and alerting

- Based on the detection and decision of detection engine, this module would generate alerts or logs.

Reporting/Output module

- This will help analyse the logs and alerts, trigger alarms based on identified attacks etc.)
- Generates reports, statistical information, etc.

Snort rule




```
alert tcp $TELNET_SERVERS 23 -> $EXTERNAL_NET any (msg:"TELNET
  Attempted SU from wrong group"; flow:
from_server,established; content:"to su root"; nocase;
  classtype:attempted-admin; sid:715; rev:6;)
```


Activity @ Home - Assignment

Install Snort and write rules to cater following requirements.

- alert for "Zoysa" keyward within the HTTP packets.
- alert if 10.0.2.15 tries to connect using HTTP
- alert abnormal SSH terminations from 10.0.2.15
- alert any port scanning attempt by 10.0.2.15 and log them into a file called portscan.log
- alert for telnet attempts by 10.0.2.15
- alert for UDP packets trying to query a DNS server
- alert if anyone has tried to access www.ucsc.cmb.ac.lk

Submit the rules