**Hardware based Intrusion Detection System**

**A Project Report**

**Presented At**

**Maharaja Surajmal Institute of Technology**



By

Amit Sharma

Nishant Kumar

Atif Ahmed

**Project Guide: Ms. Gunjan Beniwal**

# Abstract

Intrusion-detection systems aim at detecting attacks against computer systems and networks or, in general, against information systems. Indeed, it is difficult to provide provably secure information systems and to maintain them in such a secure state during their lifetime and utilization. Sometimes, legacy or operational constraints do not even allow the definition of a fully secure information system. Therefore, intrusion detection systems have the task of monitoring the usage of such systems to detect any apparition of insecure states. They detect attempts and active misuse either by legitimate users of the information systems or by external parties to abuse their privileges or exploit security vulnerabilities.

# Introduction

IDS arms any business against attacks by continuously monitoring network activity, ensuring all activity is normal. If IDS detects malicious activity it responds immediately by destroying the attacker's access and shutting down the attack. IDS reads network traffic and looks for patterns of attacks or signatures, if a signature is identified, IDS sends an alert to the Management Console and a response is immediately deployed.

The reason of developing this tool was the following:

* IDS(s) are difficult to setup
* Costs are high
* Rules implemented on the IDS can clash with services

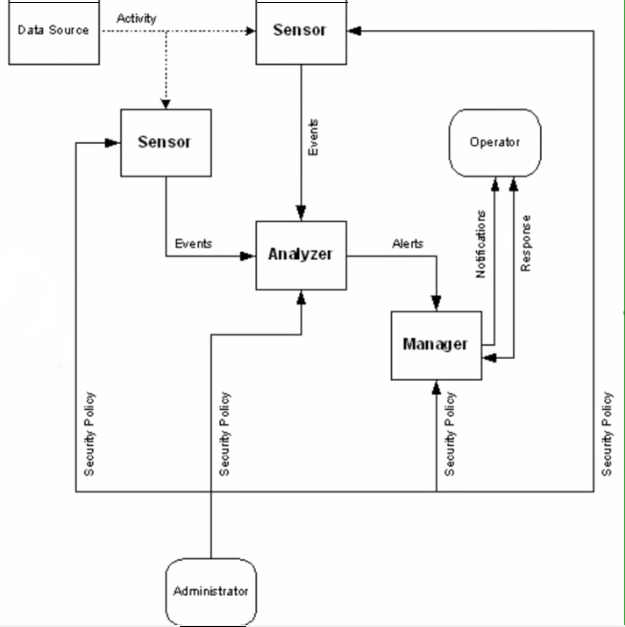


Fig.- IDS Architecture

# Objective

Main objective of this tool is to create a portable hardware based IDS which can be installed easily without any technical knowledge. Thus, empowering the common user and protecting them against the attack vectors.

# Hardware & Software

The development of the tool requires

Raspberry Pi and peripheral devices

Minibian OS

Snort

# Contribution of the Project

As development of the project is complete this can be used as a commercial plug and play module that can protect the enterprise or home network from any outside intrusions and attacks.

# Why this Project ?

Information is strategic resource, organizations spend a significant amount of their budget on managing information resources. Computer security have several security related objectives among them the three fundamental objective are: Secrecy i.e. to protect information; Incorruptibility, to protect information accuracy; lastly Access, to ensure information delivery. It is necessary to put high priority to system security, minimize loop holes and secure the computer system against intrusion. Today's standard of security implement a configured firewall along with an intrusion detection system. If an intruder is able to acquire a weakness in the network by scanning the host network, he can easy penetrate into the system and obtain valuable data. If an intruder is masking his identity for a firewall enabled service, intrusion detection systems cannot minimize the damages .

Most of the security approaches now a day’s focus on defense rather than aggressive form of a security. One of the aggressive for of defense mechanism that has come to the fore are Honeypots. It acts as a Booby trap equipment which are configured as a system weakness to attract intruders and gather all the information to eliminate future attacks thus eliminating security loop holes, these are known as Honeypots. For example honeypots like Honeyd1 are already being used to detect attackers and protect information.

The proposed architecture is based on Raspberry Pi-Honeypot using already existing tools and methods like Snort , Modern Honeypot Network (MHN) , Kippo, Dionaea , Glastopf.This architecture puts forth a simple, cost effective and an autonomous deployment in any environment.

# Conclusion

There are limited number of available IDS specially as a hardware which is cheap and easy to deploy. Most of them require an expert supervision while setting up the rules. And due to the above-mentioned reasons home users are still in a vulnerable state where and attacker can exploit the network. The tool which we are developing resolves all the issues which are suggested in the document