Feasibility Report

Intrusion Prevention System

# Introduction

## Definitions

* Intrusion Detection System: An intrusion detection system is a device or software application that monitors the network or system activities or policy violations and produce electronic reports to a management station.
* Intrusion Prevention System: Intrusion prevention systems are network security appliances that monitor network and system activities for malicious activities. The main function of intrusion prevention system is to identify malicious activity, log information about this activity, attempt to block or stop and report it.
* Firewall: A device or application that analyzes packet headers and enforces policy based on protocol type, source address, destination address, source port, and/or destination port. Packets that do not match policy are rejected.

## Functions

Main function of intrusion prevention system is to:

* Identify intrusion
* Log information about intrusion
* Attempt to block/stop intrusion
* Report intrusion

## Methods used for Detection

* Signature based detection
* Statistical anomaly based detection

## Types of IPS

## Network based IPS

These perform packet sniffing analyze network traffic to identify and stop suspicious activities. They are typically deployed inline like a network firewall. They receive packets, analyze them, decide whether they should be permitted and allow acceptable packets to pass through. Most products use a combination of attack signature and analysis of network and application protocols. Some products allow administrator to create and deploy attack signature

## Host based IPS

HIPS are similar in principle and purpose to network based except the host based product monitor the characteristics of single host, such a monitoring network traffic, system logs running processes, file access and modification and system and application configuration changes. Host based IDPS are most commonly deployed on critical hosts such as publically accessible servers and serves containing sensitive information.

# Possible Errors

1. False Positive: Incorrectly identifying benign activity as being malicious
2. False Negative: Failing to identify malicious activities occurred

# Proposed Model

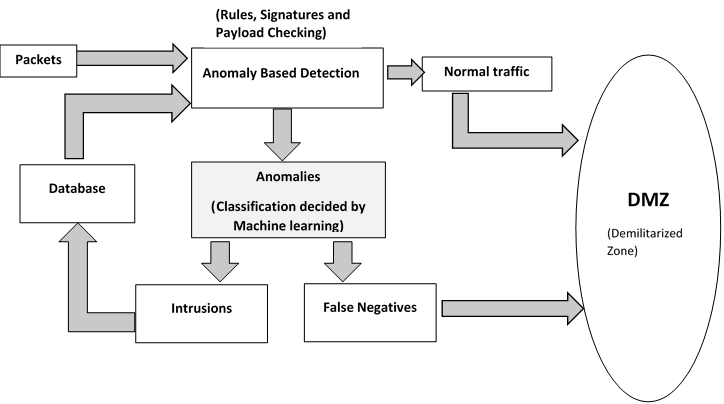


Figure 1: Proposed Architecture for IPS

* 1. Working: This IPS is an implementation of IPS over an IDS. The IPS will use Rules, Signatures and Payloads to differentiate between normal traffic and anomalies. The anomalies will then be sent to the IDS for analysis. The false negatives will be redirected to the user and the positive anomalies will be marked as intrusion attempts and added to the database of rules. To classify between false negatives and anomalies, machine learning will be implemented as shown in figure 1.

# Modules

## Inline IPS and passive IDS modes

When an IPS device is placed inline be sure it supports fail open ports. Some IPS providers offer fail-open ports on only portion their models.

## Default detection policy

Every IPS vendor should provide a detection policy comprised of most common IPS rules to help to get started. But an organization should never just rely on a default policy because it never adapts to your dynamically changing network environment

## Report, alert and dashboards

Most IPS providers offer a selection of reports, alerts and dashboards usually present in management console. Report should be flexible, alert should be offered through email syslog and SNMP and dashboard should be customized based on the user’s role in the organization.

## User identify tracking

What good is an IP address for an end user device related to the security or compliance event if you don’t know who is being attacked or who is violating a company IT policy? Instead of sifting through DHCP and active directory logs to manually cross-reference users with IP address, an IPS can place username and user identity at your fingerprints. The time it takes to tie a user to a security event can be shrunk from one hour to under a second.

## Automated tuning

Every network is different customize your IPS detection policy with rules that are relevant for your organization. If the detection policy is too small the IPS will offer inadequate protection. And if it’s too big it can overburden the IPS causing decease network throughput decrease latency. An IPS can passively profile your network and automatically recommend rules to enable and disable at a user defined interval

## Application monitoring

Most enterprise have documented acceptable use policies depicting operating system and application approved and restricted from use but few organizations have to mean the monitor and enforce them. An IPS helps IT to reduce the surface area to attack by alerting IT to the unauthorized users to operating system, application and devices.

## Network based analysis

Not all attacks come through the perimeter. Many are hand carried on mobile computing devices right from front door thus bypassing a perimeter IPS network behavior analysis technologies baseline “normal “network traffic and detect anomalies such as a spread of malware.

# Challenges

* Performance: This project aims to reduce false positives and false negatives by continuously analyzing packets for intrusion attempts in reasonable time with minimum delay to the user. Process needs to be fast and light.
* Efficiency: Efficiency of the software needs to be high. Errors need to me minimal.
* Detection Rate: Rate of processing packets after being detected should be fast.

# Technologies

## Snort

Snort is an [open source](http://searchenterpriselinux.techtarget.com/definition/open-source) network [intrusion detection](http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection) system (NIDS) created by Martin Roesch. Snort is a [packet](http://searchnetworking.techtarget.com/definition/packet) [sniffer](http://searchnetworking.techtarget.com/definition/sniffer) that monitors network traffic in [real time](http://searchcio-midmarket.techtarget.com/definition/real-time), scrutinizing each [packet](http://searchnetworking.techtarget.com/definition/packet) closely to detect a dangerous [payload](http://searchsecurity.techtarget.com/definition/payload) or suspicious anomalies. Snort is based on libpcap (for library packet capture), a tool that is widely used in [TCP/IP](http://searchnetworking.techtarget.com/definition/TCP-IP) traffic [sniffer](http://searchnetworking.techtarget.com/definition/sniffer)s and analyzers. Through [protocol](http://searchnetworking.techtarget.com/definition/protocol) analysis and content searching and matching, Snort detects attack methods, including [denial of service](http://searchsoftwarequality.techtarget.com/definition/denial-of-service), [buffer overflow](http://searchsecurity.techtarget.com/definition/buffer-overflow), [CGI](http://searchsoa.techtarget.com/definition/common-gateway-interface) attacks, [stealth](http://searchsecurity.techtarget.com/definition/stealth) [port](http://searchnetworking.techtarget.com/definition/port) scans, and SMB [probe](http://searchsecurity.techtarget.com/definition/probe)s. When suspicious behavior is detected, Snort sends a real-time alert to syslog, a separate 'alerts' file, or to a [pop-up](http://whatis.techtarget.com/definition/pop-up) window.

## SnortSam

SnortSam is a plugin for [Snort](http://www.snort.org/), an open-source light-weight Intrusion Detection System (IDS). The plugin allows for automated blocking of IP addresses on various firewalls such as Linux IP Tables, Linux IP Chains, Cisco Routers and many more.

## BASE

BASE is the Basic Analysis and Security Engine. It is based on the code from the Analysis Console for Intrusion Databases (ACID) project. This application provides a web front-end to query and analyze the alerts coming from a SNORT IDS system.

## Machine Learning Strategies

Signatures based IDSs rely on humans to create, test, and deploy the signatures. Thus, it may take hours or days to generate a new signature for an attack, which can be too long when dealing with rapid attacks. Nevertheless, in order to offer a human-independent solution to the abovementioned problem, anomaly based IDSs based on machine learning techniques provide an added advantage. Anomaly based IDSs using machine learning techniques have the ability to implement a system that can learn from data (experience) and give the decision for unseen data.

Following are some of the most widely used machine learning strategies used to classify intrusive and non-intrusive behavior:

* Neural Networks
* Bayesian Networks
* Support Vector Machine
* Genetic Algorithm
* Fuzzy Logic
* Decision Tree

A table describing the pros and cons of each strategy is shown below:

|  |  |  |  |
| --- | --- | --- | --- |
| **Sr. No.** | **Machine Learning Techniques** | **Pros** | **Cons** |
| 1. | Neural Networks | Ability to generalize  from limited, noisy  and incomplete data.  Does not need expert  knowledge and it can  find unknown or novel  intrusions. | Slow training process  so not suitable for real-  time detection.  Over-fitting may  happen during neural  network training. |
| 2. | Bayesian Networks | Encodes probabilistic  Relationships among  the variables of  interest.  Ability to incorporate  both Prior knowledge  and data. | Harder to handle  continuous features.  May not contain any  good classifiers if prior  knowledge is wrong. |
| 3. | Support Vector Machine | Better learning ability  for small samples.  High training rate and  Decision rate,  insensitiveness to  dimension of input  data. | Training takes a long time.  Mostly used binary  classifier which cannot  give additional  information about  detected type of attack. |
| 4. | Genetic Algorithm | Capable of deriving  best classification rules  and Selecting optimal  parameters.  Biologically inspired  and employs  evolutionary  algorithm. | Genetic algorithm  cannot assure constant  optimization response  times.  Over-fitting. |
| 5. | Fuzzy Logic | Reasoning is  Approximate rather  than precise.  Effective, especially  against port scans and  probes. | High resource  consumption Involved.  Reduced, relevant rule  subset identification  and dynamic rule  updation at runtime is  a difficult task. |

Table 1:Comparison of Machine Learning schemes

# 

# 6).Conclusion

Hence, considering the technologies available, the proposed project is feasible using open source tools. The idea of IPS over an IDS can be implemented using snort and machine learning can be implemented using the strategies above.