Network Intrusion Detection Using EagleX and Securepoint Nuzzler

GRADUATE PROJECT TECHNICAL REPORT

Submitted to the Faculty of
the Department of Computing and Mathematical Sciences
Texas A&M University-Corpus Christi
Corpus Christi, Texas

in Partial Fulfillment of the requirements for the Degree of
Master of Science in Computer Science

by

Jasbir S Parmar
Fall 2005

Committee Members

Dr. Mario Garcia
Committee Chairperson

Dr. Long-zhuang Li
Committee Member

Dr. David Thomas
Committee Member
ABSTRACT

An intrusion is defined as any set of actions that compromise the integrity, confidentiality or availability of a resource. Intrusion detection is an important task for information infrastructure security. The goal of an intrusion detection system (IDS) is to identify patterns of known intrusions (misuse detection) or to differentiate anomalous network activity from normal network traffic (anomaly detection).

This project is aimed at using two intrusion detection systems EagleX and Securepoint Nuzzler to identify and report patterns of known intrusions or to differentiate anomalous network activity from normal traffic. Experiments would be conducted using the same rule set on both IDS under the same conditions (network traffic) to find out which IDS can detect more intrusion pattern. Based on the results the recommendation would be made that out of these two windows based IDS which one (EagleX or Nuzzler) should be used.
TABLE OF CONTENTS

Abstract ......................................................................................................................... ii

Table of Contents ......................................................................................................... iii

List of Figures ................................................................................................................... vi

List of Tables ................................................................................................................... viii

1. Background and Rationale .......................................................................................... 1
   1.1 Defining Intrusion Detection .................................................................................. 1
   1.2 Need for Intrusion Detection Systems ................................................................... 1
   1.3 Types of Intrusion Detection Systems ................................................................... 2
      1.3.1 Host Based IDS ............................................................................................... 2
      1.3.2 Network Based IDS ....................................................................................... 3
      1.3.3 Signature Based IDS ..................................................................................... 4
      1.3.4 Anomaly Based IDS ..................................................................................... 4
      1.3.5 File Integrity Checker ................................................................................... 5
      1.3.6 Network Node IDS ....................................................................................... 6

2. Narrative ..................................................................................................................... 7
   2.1 Selected Previous Work Done in the Field .............................................................. 7
   2.2 Intrusion Detection Tools/Products ......................................................................... 8
      2.2.1 Snort ............................................................................................................... 8
      2.2.2 eTrust Intrusion Detection System .................................................................. 10
      2.2.3 PacketAlarm Intrusion Detection and Prevention System ......................... 11
      2.2.4 SecurePoint Intrusion Detection System Nuzzler ....................................... 12
2.3 Overview .................................................................................................................. 13

2.4 Description of User Interface .................................................................................. 13
   2.4.1 EagleX Main Page .............................................................................................. 14
   2.4.2 EagleX Rules/Signatures .................................................................................. 15
   2.4.3 EagleX Alerts Display ..................................................................................... 16
   2.4.4 Nuzzler Main Window ...................................................................................... 17
   2.4.5 Nuzzler Rules .................................................................................................. 18
   2.4.6 Nuzzler’s Trusted Address List ........................................................................ 19

3. Proposed System Design ............................................................................................ 21
   3.1 Main Components .................................................................................................. 21
   3.2 Project Requirements ............................................................................................ 21
      3.2.1 EagleX IDS .................................................................................................. 21
      3.2.2 Securepoint Nuzzler IDS Sensor .................................................................... 24
   3.3 Architecture of IDS .............................................................................................. 24
   3.4 Writing Rules and Generating Alerts .................................................................... 26

4. Evaluation and Results .............................................................................................. 30
   4.1 Running EagleX and Nuzzler IDS ....................................................................... 30
   4.2 Results of Comparative Analysis .......................................................................... 30
      4.2.1 Group 1 Result’s ............................................................................................ 32
      4.2.2 Group 2 Result’s ............................................................................................ 35
      4.2.3 Group 3 Result’s ............................................................................................ 38
      4.2.4 Group 4 Result’s ............................................................................................ 41
      4.2.5 Group 5 Result’s ............................................................................................ 44
4.2.6 Final Result... .................................................................46

5. Conclusions.................................................................48

Acknowledgements..........................................................49

Bibliography and References..............................................50

Appendix A: Intrusion Detection Terminology........................52

Appendix B: Default EagleX and Nuzzler Rules.....................55
LIST OF FIGURES

Figure 1.1 Host-based Intrusion Detection System ............................................. 3
Figure 1.2 Network-based Intrusion Detection System ........................................ 4
Figure 2.1 Snort IDS ....................................................................................... 9
Figure 2.2 eTrust IDS .................................................................................... 10
Figure 2.3 PacketAlarm IDS .......................................................................... 12
Figure 2.4 Network with a SecurePoint Nuzzler .............................................. 13
Figure 2.5 EagleX Main Page ......................................................................... 15
Figure 2.6 EagleX Rules/Signatures ............................................................... 16
Figure 2.7 EagleX Alerts ............................................................................... 17
Figure 2.8 Nuzzler Main Window .................................................................... 18
Figure 2.9 Nuzzler Rules ................................................................................ 19
Figure 2.10 Nuzzler’s Trusted Address List .................................................... 20
Figure 3.1 IDS Architecture .......................................................................... 25
Figure 4.1 Network based IDS Scenario ....................................................... 31
Figure 4.1 ACID Display of Intrusions Detected by Group 1 of EagleX ........... 33
Figure 4.2 Rule Categories used in Group 1 of Nuzzler IDS ............................. 34
Figure 4.3 ACID Display of Intrusions Detected by Group 2 of EagleX .......... 36
Figure 4.4 Rule Categories used in Group 2 of Nuzzler IDS ............................. 37
Figure 4.5 ACID Display of Intrusions Detected by Group 3 of EagleX ........... 39
Figure 4.6 Rule Categories used in Group 3 of Nuzzler IDS ............................. 40
Figure 4.7 ACID Display of Intrusions Detected by Group 4 of EagleX ........... 42
Figure 4.8 Rule Categories used in Group 4 of Nuzzler IDS ............................. 43
LIST OF TABLES

Table 4.1 Results of EagleX Scan for Group 1 ............................................33
Table 4.2 Results of Nuzzler Scan for Group 1 ............................................34
Table 4.3 Results of EagleX Scan for Group 2 ............................................36
Table 4.4 Results of Nuzzler Scan for Group 2 ............................................37
Table 4.5 Results of EagleX Scan for Group 3 ............................................39
Table 4.6 Results of Nuzzler Scan for Group 3 ............................................40
Table 4.7 Results of EagleX Scan for Group 4 ............................................42
Table 4.8 Results of Nuzzler Scan for Group 4 ............................................43
Table 4.9 Results of EagleX Scan for Group 5 ............................................45
Table 4.10 Results of Nuzzler Scan for Group 5 ..........................................46
Table 4.11 Final Result of IDS Comparison ...............................................47
1. BACKGROUND AND RATIONALE

1.1 Defining Intrusion Detection

Intrusion detection (ID) is a type of security management system for computers and networks. An ID system gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization). ID uses vulnerability assessment (sometimes referred to as scanning), which is a technology developed to assess the security of a computer system or network [Security 2005]. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system.

1.2 Need for Intrusion Detection Systems

The need for intrusion detection systems can be summed up by a simple principle of network security: defense in-depth. Defense in-depth is a layered approach to protecting an organization’s information systems and communications network from malicious attacks and unauthorized access to sensitive information and data. This method involves multiple, overlapping controls that assist organizations in preventing, detecting, and responding to suspected intrusions. Typically, heavy reliance is placed on protection and prevention using controls such as routers, firewalls, public key infrastructures, virtual private networks, and virus scanners. In contrast, critical detection and response functions such as those provided by intrusion detection systems are often overlooked. Intrusion detection systems act as video cameras within the network and aid in deterrence,
detection, damage assessment, and prosecution support. Without an IDS facility in place to monitor network and host activity, both attempted and successful intrusion attempts may go unnoticed, possibly resulting in irreparable damage to an organization’s network. Intrusion detection systems form a necessary layer of a defense in-depth strategy and play a critical role in a comprehensive information protection program [Paul 2005].

1.3 Types of Intrusion Detection Systems

Intrusion Detection Systems can be classified into different categories depending on either the method used to detect intrusions (anomaly, rule based) or the place where it is being used (host, network based). These different categories are discussed in the sections that follow.

1.3.1 Host-based IDS (HIDS)

A host-based IDS (Figure 1.1) analyzes several areas to determine misuse (malicious or abusive activity inside the network) or intrusion (breaches from the outside). Host-based IDS consult several types of log files (kernel, system, server, and more), and compare the logs against an internal database of common signatures for known attacks. Host-based IDS can also verify the data integrity of important files and executables. It checks a database of sensitive files and creates a checksum of each file with a message-file digest utility such as md5sum (128-bit algorithm) or sha1sum (160-bit algorithm). The host-based IDS then stores the sums in a plain text file, and periodically compare the file checksums against the values in the text file. If any of the
file checksums do not match, the IDS will alert the administrator by email or cellular pager.

![Diagram of a network system](image)

**Figure 1.1** Host based Intrusion Detection System [Stefano 2002]

### 1.3.2 Network-based IDS (NIDS)

Network Intrusion Detection Systems (Figure 1.2) are placed at a strategic point or points within the network to monitor traffic to and from all devices on the network. This monitors all network traffic passing on the segment where the sensor is installed, reacting to suspicious anomaly or signature-based activity. Traditionally NIDS were promiscuous packet sniffers with IDS filters, though these days they have to be far more intelligent, decoding protocols and maintaining state, etc. They analyze every packet for attack signatures, though under a heavy network load many will start to drop packets. SecureNet Pro and Snort are good examples of the NIDS.
1.3.3 Signature-based IDS (SIDS)

A signature-based IDS examines ongoing traffic, activity, transactions, or behavior for matches with known patterns of events specific to known attacks. As with antivirus software, a signature-based IDS requires access to a current database of attack signatures and some way to actively compare and match current behavior against a large collection of signatures. Except when entirely new, uncataloged attacks occur, this technique works extremely well. Signature databases must be constantly updated, and IDS must be able to compare and match activities against large collections of attack signatures for the IDS to work efficiently [Robert 2002].

1.3.4 Anomaly-based IDS (AIDS)

Anomaly-based IDS find attacks by identifying unusual behavior (i.e., anomalies) that occurs on a host or network. They function on the observation that some attackers behave differently than normal users and thus can be detected by systems that identify these differences. Anomaly-based IDS establish a baseline of normal behavior by
profiling particular users or network connections and then statistically measuring when the activity being monitored deviates from the norm. These IDS frequently produce a large number of false alarms because normal user and network behaviors can vary widely. Despite this weakness, the researchers working on applying this technology assert that anomaly-based IDS are able to detect never-before-seen attacks, unlike signature-based IDS that rely on an analysis of past attacks. Although some commercial IDS include restricted forms of anomaly detection, few, if any, rely solely on this technology. Main advantage of Anomaly-based IDS is that it can detect unusual behavior and thus have the ability to detect attacks without having to be specifically programmed to detect them [Mell 2002].

1.3.5 File Integrity Checker

When a system is compromised by an attacker, it will often alter certain key files to provide continued access and prevent detection. By applying a message digest (cryptographic hash) to key files, the files can be checked periodically to see if they have been altered, thus providing a degree of assurance. Upon detecting such a change, the file integrity checker will trigger an alert. The same process can be employed by a system administrator after being successfully attacked, allowing him/her to ascertain the extent to which the system has been compromised. Previously, file integrity checkers detected intrusions long after the event; however, more products have recently been emerging that check files as they are accessed, thus introducing a near real time IDS element. Example of such a system is Tripwire and Intact [Andy 2003].
1.3.6 Network Node IDS

The Network Node IDS (NNIDS) is a type of “hybrid” IDS agent which overcomes some of the limitations of the network-based IDS. The NNIDS agent works in a similar manner to the network-based IDS in that it takes network packets and performs protocol analysis and/or compares them against signature database entries. However, this “micro agent” is only concerned with packets targeted at the network node on which it resides. Because it is installed within the protocol stack of the host, it is sometimes referred to as Stack-based IDS [NSS 2004].
3. PROPOSED SYSTEM DESIGN

3.1 Main Components

The following are the main components of the proposed project:

- EagleX a windows based network intrusion detection system.
- Nuzzler a windows based network intrusion detection system by Securepoint.

3.2 Project Requirements

The software requirements for the proposed work in the field are described in this section. The comparative system design needs two network based IDS called EagleX and Nuzzler IDS to monitor network traffic which will then be acquired, analyzed and visualized using the real time data acquisition software for each IDS. To fully implement a simulated network where intrusion detection is performed also requires other network systems connected to the primary computer on which the IDS runs to detect and report the intrusion activity. Both intrusion detection systems will be installed on the same windows based computer system and then be tested against attacks which come from World Wide Web to see which IDS can detect and report more threats in the same environment and time period.

3.2.1 EagleX IDS

EagleXv2.1 is a high-performance intrusion detection system. It is a network-based, real-time intrusion detection system. It can be configured by using IP address, primary and secondary DNS server address of the system on which the IDS is to be installed. Once configured it will remember the settings and will update its setting
automatically in the future. The IDS is configured to respond to recognized signatures as it captures and analyzes network traffic [Engage Security 2003]. These responses include logging the event, forwarding the event to the IDS centre, performing a TCP reset, generating an IP log and capturing the alert trigger packets. After being installed in the network, the IDS monitors and performs real-time analysis of network traffic by looking for anomalies and misuse based on an extensive, embedded signature library. When the system detects unauthorized activity, the IDS can terminate the specific connection, permanently block the attacking host, log the incident, and send an alert to the IDS manager.

EagleX was developed using many different software each performing different yet important functions for the proper working of the IDS. As mentioned before it uses the snort engine (i.e snort rules/signatures) for the purpose of intrusion detection, it also uses apache web server, webmin, mysql database server among other software’s for its proper functioning.

*Introducing EagleX Topology*

There are five primary software packages that produce the EagleX IDS topology:

1. The Apache Web server,
2. MySQL database server,
3. IDScenter,
4. Oink Master,
5. ACID,
6. Snort,
This topology assumes that the IDS will be running on the same hardware on which the database and ACID console are running. Below is a brief description of each of the packages and their purpose in the topology.

1. Apache Web server - This is the Web server of choice for the majority of websites that are accessed on the Internet. The sole purpose of Apache is for hosting the ACID Web-based console.

2. MySQL Database- MySQL is a SQL based database for a variety of platforms and is the most supported platform for storing Snort alerts. All of the IDS alerts that are triggered from the sensors are stored in the MySQL database.

3. IDScener – IDSccenter is basically a front-end for Snort on Windows platforms. The advantage of using IDSccenter with Snort is simply much more comfort. IDSccenter helps in better understanding of the snort and also provides management features to easily configure/manage different snort features.

4. Oink Master - Oinkmaster is a simple but useful perl script released under the BSD license to help update/manage Snort rules and disable/enable/modify certain rules after each update (among other things). It will tell exactly what had changed since the last update, so that users will have total control of the rules.

5. Analysis Console for Intrusion Databases (ACID) - ACID is a Web-based application for viewing firewall logs and/or IDS alerts. This is where all the sensor information is consolidated for viewing.
6. Snort – Snort is a network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. This is the software package that is used to gather information from the network.

EagleX detects the intrusion activity from the network and sends it to the MYSQL database after generating alarms for a detailed analysis.

### 3.2.2 Securepoint Nuzzler IDS Sensor

Securepoint Nuzzler is a window’s based intrusion detection and observing application. It uses static rules and in build dynamic patterns to identify not-authorized traffic in a network segment [NUZZLER 2004]. It also features many options to observe a single computer, a group of computers or a whole network segment. Nuzzler has an important feature called observer which allow it to observe a network, ip address or a hostname. Once the intrusion is detected, an alert message is shown to the user on the screen and the alert message is stored in the log file for later evaluation/study. Nuzzler doesn’t use mysql database for storing alerts rather it has its own database created by securepoint for the purpose of storing alerts.

### 3.3 Architecture of IDS

The general architecture of any network based IDS is quiet similar. EagleX and Nuzzler both are windows based IDS and have the same underlying architecture. The general architecture of a network based IDS is represented in Figure 3.1. As seen in the system diagram, the packets from the network are captured and sent to the decoder for decoding, once decoded detection engine compare the packet information with the rules/signatures to check for the intrusion activity. Once the comparison is done and anomaly is detected
an alert is generated for the user and this intrusion activity is stored in log file for later analysis.

Fig 3.1 IDS Architecture

- Packet Decoder: The IDS packet decoder generally supports the Ethernet, SLIP and PPP mediums. The packet decoder performs all the work to prepare the data in an expedient manner for the detection engine.

- Detection Engine: The detection engine is at the heart of any IDS. It essentially is responsible for analyzing every packet based on the IDS rules that are loaded at runtime. The detection engine separates the IDS rules into what is referred to as a chain header and chain options. The common attributes such as source/destination IP address and ports identify the chain header. The chain options are defined by details such as the TCP flags, ICMP code types, specific type of content, payload size, etc. The detection engine recursively analyzes each and every packet based on the rules defined in the IDS rules file. The first rule that matches the decoded packet triggers the action specified in the rule definition.
Logger/Alerter: Logging and alerting are two separate subcomponents. Logging, logs the information collected by the packet decoder in human readable or tcpdump format. Alerts can be configured to be sent to syslog, flat file, UNIX sockets or a database. Optionally, alerting can be completely turned off during testing or penetration studies. Depending on the IDS settings some IDS log all the packets passing through the IDS in its log files while some only log the intrusion activities and does not log normal information packets.

3.4 Writing Rules and Generating Alerts

A signature specifies the types of network intrusions that the sensor will detect and report. An IDS uses signatures/rules to detect typical intrusive activity, such as denial of service (DoS) attacks. As IDS scan network packets, it uses signatures to detect known attacks and respond with actions that are defined as a response.

Understanding and writing rules is the most important aspect of the project. EagleX and Nuzzler both have separate rules and rule formats. Even though most of the rules look for same intrusion activity but still the format of these similar rules is different in EagleX and Nuzzler.

EagleX uses Snort rules for the intrusion detection purpose. Following is a sample EagleX rule:

```plaintext
alert tcp $EXTERNAL_NET any -> $HOME_NET 21 (msg:"POLICY FTP anonymous login attempt"; content:"USER"; nocase; content:"anonymous|0D0A|"; nocase;
flow:to_server,established; classtype:misc-activity; sid:553; rev:4;)
```

The rule part to the left of -> (arrow mark) constitute rule “Header” and to right of it is the “Body” part of the rule. Following is the explanation of different parts of the rule:
alert: The first word is the action to be taken if the rule matches data in the network traffic. Besides alert five other action types pass, log, active, dynamic and custom can also be used.
tcp: This is the protocol type of the rule. Tcp, icmp, udp, ip are the most common protocol types.
$EXTERNAL_NET: It is a network variable used to encapsulate list of IP address into single name. It is used for source IP address matching.
any: This mean attack can originate from any source port.
$HOME_NET: This variable represents the internal network IP address. It is used for destination IP address matching.
21: This represent the destination port number.
msg:"POLICY FTP anonymous login attempt": This is what’s written to the log file if rule matches network traffic data.
content:"USER": Content represent what rule looks for in the body part of the data checked by the IDS.
Nocase: It means content can be either upper or lower case i.e non case sensitive.
flow to_server,established; : This represents the state of connection i.e check for intrusion activity only after the connection is established with the server.
classtype:misc-activity; : This represent the severity of the attack.
sid:553; : This is the id number of the rule.
rev:4; : Rev or revision represent the number of times the rule has been revised.

A sample output of the packet captured using EagleX running on a host computer in the campus labs is as follows:
07/13-10:45:44.919135  TCP src: 10.1.46.18 dst: 211.190.238.224 sport: 1792 dport: 16629
tgts: 14 ports: 14 flags: *****S* event_id: 6

Nuzzler has its own rules and rule format. Nuzzler rules are very similar to the EagleX in the sense that they are also designed to detect the same intrusion activity that EagleX detects. Following is a sample Nuzzler rule:

<table>
<thead>
<tr>
<th>SID</th>
<th>Protocol</th>
<th>Source IP</th>
<th>Port</th>
<th>Dest IP</th>
<th>Port</th>
<th>Msg</th>
</tr>
</thead>
<tbody>
<tr>
<td>634</td>
<td>UDP</td>
<td>EXTERNAL</td>
<td>any</td>
<td>Internal</td>
<td>10080</td>
<td>Scan Amanda client</td>
</tr>
</tbody>
</table>

TTL  SEQ  ACK  Class Type
0     0     0     attempted-recon

Different parts of the rule are:

SID (634): This is the id number of the rule.

Protocol (UDP): This is the protocol type of the rule.

Source IP (EXTERNAL): It's a network variable representing the source IP address.

Port (any): This is the source port from which the attack is originated.

Dest IP (internal): This is the Network variable representing the destination IP address.

Port (10080): This is the destination port number.

Msg (Scan Amanda client): This is the message written to the log file if rule matches network traffic data.

TTL (0): This represents the time to live value of the packet.

SEQ (0): This represents the value of Sequence Number of the packet.

ACK (0): This represents the value of Acknowledgement Number of the packet.

Class type (attempted-recon): This represents the severity of the attack.
A sample output of the packet captured using Nuzzler running on a host computer in the campus labs is as follows:

DST=64.231.252.135 PROTO=TCP SPT=1903 DPT=6883 REFERENCE=Internal
Message MSG=Intrusion from address 10.1.46.18 (00-0B-DB-B7-DD-DC)
4. EVALUATION AND RESULTS

4.1 Running EagleX and Nuzzler IDS

Execution of the IDS takes place in three steps. The first step is to capture information packets from the network traffic to check for intrusion activity. The second step is to compare the captured packets with the signatures in IDS database to check for any suspicious activity. The third and final step is to keep log of any intrusion activity so that a report can be generated at later time and also to notify administrator of the network about intrusion activity.

4.2 Results of Comparative Analysis

In this project the intrusion rules/signatures were divided into 5 groups with the first 4 groups containing few particular rule sets and 5th group containing all the rule sets available with in both EagleX and Nuzzler IDS. The experiments are conducted in Nursing Computer Lab in a setup similar to one as shown in Figure 4.1. Computer System A as shown in Figure 4.1 is connected to internet on one hand and to internal computer network on the other. It also has both EagleX and Nuzzler IDS installed on it. EagleX and Nuzzler IDS are both running simultaneously on System A thereby looking at same network traffic as it passes the network. All the other computers on the network also connect to internet through computer A. Once an intrusion activity is detected by IDS an alert is generated for the user and the intrusion activity is logged in the log file of respective IDS for later analysis. Later the log text file is also converted into excel format as it make it easy to calculate total numbers of alerts generated by the respective IDS.
Figure 4.1 Network based IDS Scenario.

In each group first brief information is given about the rule sets being used in that group and then the results are displayed in the table. Description of table column headings is as follows.

- Rule Set Name: In each group different categories of rules are selected which are then used to detect intrusion on the system. Each category in turn contain the rules which are actually used for the purpose of intrusion detection.
- Number of Rules: Give the number of rules present in each category.
- Detection Period: It is the time for which the IDS is actively monitoring the system with selected rules to detect intrusion.
- Number of Attacks Detected: It gives the total number of intrusion attempts detected by the IDS during the detection period.
- Protocol Type of attacks: Each intrusion attempt detected by the IDS has a protocol type. Mostly it’s either TCP or UDP type.
4.2.1 Group 1 Result's:

Most of the rules in this group check for bad traffic or port scan activities i.e it looks for traffic that is trying to gain unauthorized access to the system.

- Bad Traffic Rules: These signatures are representative of traffic that should never be seen on any network.

- Scan Rules: These signatures are representative of network scanners. These include port scanning, ip mapping, and various application scanners.

- Finger Rules: These signatures are representative of finger scan. Finger is service used by the system and these rules are fired when someone attempts to access the finger services from other system.

- Exploit Rules: These signatures are fired when some exploit attack happen on DNS Server.

Figure 4.1 displays the ACID console of the EagleX IDS displaying the intrusions detected by EagleX. It also provide other important information like date & time when the database was queried for the results, no. of sensors used, total number of alerts, unique alerts, profile of the traffic etc. Table 4.1 shows the result of the scan for group1 rules of EagleX. Figure 4.2 shows the rule categories used for Nuzzler Group1 scan. Table 4.2 shows the result of the scan for group1 rules of the Securepoint Nuzzler IDS.
Table 4.1 Results of EagleX Scan for Group 1

<table>
<thead>
<tr>
<th>Rule set name</th>
<th>No. of rules</th>
<th>Detection period</th>
<th>No. of attacks detected</th>
<th>Protocol type of attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad-Traffic</td>
<td>14</td>
<td></td>
<td></td>
<td>TCP-&gt;1990</td>
</tr>
<tr>
<td>Exploit</td>
<td>37</td>
<td>8 Days</td>
<td>Total of 2088 attacks were detected</td>
<td>UDP-&gt;83</td>
</tr>
<tr>
<td>Finger</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Scan</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Analysis Console for Intrusion Databases

Added 1 alert(s) to the Alert cache

Queried on: Fri July 08, 2005 14:37:30
Database: snort@localhost:7788 (schema version: 106)

Sensors: 1
Unique Alerts: 241 (2 categories)
Total Number of Alerts: 2088
- Source IP addresses: 13
- Dest. IP addresses: 763
- Unique IP links 770
- Source Ports: 1552
  - TCP (1337) UDP (18)
- Dest. Ports: 385
  - TCP (378) UDP (7)

Traffic Profile by Protocol

TCP (96%)
UDP (4%)
ICMP (< 1%)
Portscan Traffic (0%)

Figure 4.2 ACID Display of Intrusions detected by Group 1 rules of EagleX
<table>
<thead>
<tr>
<th>Rule set name</th>
<th>No. of rules</th>
<th>Detection period</th>
<th>No. of attacks Detected</th>
<th>Protocol type of attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bad-Traffic</td>
<td>10</td>
<td>8 Days</td>
<td>Total of 1666 attacks were detected</td>
<td>TCP-&gt;1569</td>
</tr>
<tr>
<td>Exploit</td>
<td>67</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Finger</td>
<td>13</td>
<td></td>
<td></td>
<td>UDP-&gt;97</td>
</tr>
<tr>
<td>Scan</td>
<td>23</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4.2 Results of Nuzzler Scan for Group 1

Figure 4.3 Rule Categories used in Group 1 of Nuzzler IDS
4.2.2 Group 2 Result's:

Most of the rules in this group look for bad ICMP traffic, bad login attempts or some other local parameters defined by the users.

- ICMP Rules: These rules look for potentially bad ICMP traffic. They include most of the ICMP scanning rules and other "BAD" ICMP rules.

- ICMP-Info Rules: These rules check standard ICMP traffic. They check OS pings, as well as normal routing done by ICMP. A number of "catch all" rules that would alert on encountering an unknown ICMP types are also present.

- IMAP Rules: IMAP is Internet standard mailbox protocols. Imap rules detect any kind of buffer overflow conditions which may result in a denial of service.

- Info Rules: Info rules are used to check information like bad login attempt by the user or attempt to login with empty password.

- Local Rules: These are the rules specified by the user i.e this is the place where user defined rules are placed.

Figure 4.3 shows the ACID console of the EagleX IDS displaying the intrusions detected by EagleX. It also provide other important information like date & time when the database was queried for the results, no. of sensors used, total number of alerts, unique alerts, profile of the traffic etc. Table 4.3 shows the result of the scan for Group2 rules of EagleX. Figure 4.4 shows the rule categories used for Nuzzler Group2 scan. Table 4.4 shows the result of the scan for Group2 rules of the Securepoint Nuzzler IDS.
<table>
<thead>
<tr>
<th>Rule set name</th>
<th>No. of rules</th>
<th>Detection period</th>
<th>No. of attacks detected</th>
<th>Protocol type of attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>22</td>
<td></td>
<td></td>
<td>TCP-&gt;2891</td>
</tr>
<tr>
<td>ICMP-Info</td>
<td>92</td>
<td>7 Days</td>
<td>Total of 2950 attacks were detected</td>
<td></td>
</tr>
<tr>
<td>Imap</td>
<td>17</td>
<td></td>
<td></td>
<td>UDP-&gt;59</td>
</tr>
<tr>
<td>Info</td>
<td>25</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 4.3 Results of EagleX Scan for Group 2*

---

**Analysis Console for Intrusion Databases**

Added 11 alert(s) to the Alert cache

**Owneled on:** Wed July 13, 2005 10:16:43  
**Database:** smart@localhost 7788  
(schema version: 108)

**Sensors:** 1  
Unique Alerts: 315  
(4 categories)  
Total Number of Alerts: 2950

- Source IP addresses: 49  
- Dest IP addresses: 998  
- Unique IP links: 1835  
- Source Ports: 1930  
  - TCP (1930):  
  - UDP (11)  
- Dest Ports: 196  
  - TCP (399):  
  - UDP (7)

**Traffic Profile by Protocol**

- TCP (91%)  
- UDP (2%)  
- ICMP (1%)  
- Portscan Traffic (0%)

**Figure 4.4** ACID Display of Intrusions detected by Group 2 rules of EagleX
<table>
<thead>
<tr>
<th>Rule set name</th>
<th>No. of rules</th>
<th>Detection period</th>
<th>No. of attacks detected</th>
<th>Protocol type of attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP</td>
<td>21</td>
<td>7 Days</td>
<td>Total of 2474 attacks were detected</td>
<td>TCP-&gt;2397</td>
</tr>
<tr>
<td>ICMP-Info</td>
<td>93</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Imap</td>
<td>22</td>
<td></td>
<td></td>
<td>UDP-&gt;77</td>
</tr>
<tr>
<td>Info</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Local</td>
<td>7</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4.4 Results of Nuzzler Scan for Group 2

![Rules](image)

Figure 4.5 Rule Categories used in Group 2 of Nuzzler IDS
4.2.3 Group 3 Result's:

Most of the rules in this group look for traffic protocol, buffer overflow or pornographic material in the network traffic.

- **P2P Rules:** These signatures look for usage of P2P protocols, which are usually against corporate policy.
- **Policy Rules:** These signatures look for network traffic indicating the use of an application or service that may violate a corporate security policy.
- **Pop2 Rules:** These signatures look for an attempt to exploit a buffer overflow in the pop2 service of system.
- **Pop3 Rules:** These signatures look for an attempt to exploit a buffer overflow in the POP3 service of system.
- **Porn Rules:** These signatures look for pornographic images and text on the network traffic.

Figure 4.5 shows the ACID console of the EagleX IDS displaying the intrusions detected by EagleX. It also provide other important information like date and time when the database was queried for the results, no. of sensors used, total number of alerts, unique alerts, profile of the traffic etc. Table 4.5 shows the result of the scan for Group3 rules of EagleX. Figure 4.6 shows the rule categories used for Nuzzler Group3 scan. Table 4.6 shows the result of the scan for Group3 rules of the Securepoint Nuzzler IDS.
<table>
<thead>
<tr>
<th>Rule set name</th>
<th>No. of rules</th>
<th>Detection period</th>
<th>No. of attacks detected</th>
<th>Protocol type of attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2P Rules</td>
<td>16</td>
<td>7 Days</td>
<td>Total of 3236 attacks were detected</td>
<td>TCP-&gt;3172</td>
</tr>
<tr>
<td>Policy</td>
<td>22</td>
<td></td>
<td></td>
<td>UDP-&gt;64</td>
</tr>
<tr>
<td>Pop2</td>
<td>4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pop3</td>
<td>18</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Porn</td>
<td>26</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4.5 Results of EagleX Scan for Group 3

Analysis Console for Intrusion Databases

Added 79 alert(s) to the Alert cache

Queued on: Thu July 19, 2005 18:47:08
Database: snort@localhost:7788 (schema version: 106)

Sensors: 1
Unique Alerts: 326 (5 categories)
Total Number of Alerts: 3236
- Source IP addresses: 42
- Dest. IP addresses: 1112
- Unique IP links 1152
- Source Ports: 29946
  - TCP (2048) UDP (11)
- Dest. Ports: 433
  - TCP (425) UDP (5)

Traffic Profile by Protocol
TCP (95%)
UDP (2%)
ICMP (4%)
Portscan Traffic (6%)

Figure 4.6 ACID Display of Intrusions detected by Group 3 rules of EagleX
<table>
<thead>
<tr>
<th>Rule set name</th>
<th>No. of rules</th>
<th>Detection period</th>
<th>No. of attacks detected</th>
<th>Protocol type of attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>P2P Rules</td>
<td>11</td>
<td></td>
<td></td>
<td>TCP-&gt;2787</td>
</tr>
<tr>
<td>Policy</td>
<td>20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Pop2</td>
<td>4</td>
<td>7 Days</td>
<td>Total of 2867 attacks were detected</td>
<td></td>
</tr>
<tr>
<td>Pop3</td>
<td>26</td>
<td></td>
<td></td>
<td>UDP-&gt;80</td>
</tr>
<tr>
<td>Porn</td>
<td>21</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 4.6** Results of Nuzzler Scan for Group 3

![Figure 4.7](Image)  
**Figure 4.7** Rule Categories used in Group 3 of Nuzzler IDS
4.2.4 Group 4 Result's:

Most of the rules in this group look for Web related attacks like variable vulnerabilities in Web data, vulnerabilities in web CGI applications or vulnerabilities in web server etc.

- Web-Client Rules: These signatures look for bad traffic coming from users and attacks against web users.

- Web-Coldfusion Rules: These signatures look for an attempt to exploit a known vulnerability in a Coldfusion web server.

- Web-FrontPage Rules: These signatures look for an attempt to exploit a known vulnerability in a web server running Microsoft FrontPage Server Extensions.

- Web-iis Rules: These signatures look for an attempt to cause a denial of service of WWW Publishing Service and IIS Administration software.

- Web-Misc Rules: These signatures look for an attempt to exploit a known vulnerability on a web server or a web application resident on a web server.

- Web-Php Rules: These signatures look for an attempt to exploit a known vulnerability in a PHP web application running on a server.

Figure 4.7 shows the ACID console of the EagleX IDS displaying the intrusions detected by EagleX. It also provides other important information like date & time when the database was queried for the results, no. of sensors used, total number of alerts, unique alerts, profile of the traffic etc. Table 4.7 shows the result of the scan for Group4 rules of EagleX. Figure 4.8 shows the rule categories used for Nuzzler Group4 scan. Table 4.8 shows the result of the scan for Group4 rules of the Securepoint Nuzzler IDS.
<table>
<thead>
<tr>
<th>Rule set name</th>
<th>No. of rules</th>
<th>Detection period</th>
<th>No. of attacks detected</th>
<th>Protocol type of attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-attacks</td>
<td>47</td>
<td>7 Days</td>
<td>Total of 2270 attacks were detected</td>
<td>TCP-&gt;2165</td>
</tr>
<tr>
<td>Web-cgi</td>
<td>318</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-client</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-coldfusion</td>
<td>35</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-frontpage</td>
<td>33</td>
<td></td>
<td></td>
<td>UDP-&gt; 90</td>
</tr>
<tr>
<td>Web-iis</td>
<td>127</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-misc</td>
<td>275</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-php</td>
<td>60</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 4.7 Results of EagleX Scan for Group 4

Analysis Console for Intrusion Databases

Added 0 alert(s) to the Alert cache

Queryed on: Tue July 26, 2005 09:24:29
Database: snort@localhost:7788 (schema version: 106)

Sensors: 1
Unique Alerts: 243 ( 2 categories )
Total Number of Alerts: 2279
- Source IP addresses: 13
- Dest. IP addresses: 798
- Unique IP links 305
- Source Ports: 1642
  - TCP (1642) UDP (20)
- Dest. Ports: 392
  - TCP (389) UDP (7)

Traffic Profile by Protocol
TCP (86%)
UDP (4%)
ICMP (< 1%)
Ports Traffic (9%)

Figure 4.8 ACID Display of Intrusions detected by Group 4 rules of EagleX
<table>
<thead>
<tr>
<th>Rule set name</th>
<th>No. of rules</th>
<th>Detection period</th>
<th>No. of attacks detected</th>
<th>Protocol type of attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web-attacks</td>
<td>49</td>
<td></td>
<td></td>
<td>TCP-&gt;2056</td>
</tr>
<tr>
<td>Web-cgi</td>
<td>349</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-client</td>
<td>13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-coldfusion</td>
<td>35</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-frontpage</td>
<td>34</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-iis</td>
<td>116</td>
<td></td>
<td>Total of 2127 attacks were detected</td>
<td></td>
</tr>
<tr>
<td>Web-misc</td>
<td>310</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Web-php</td>
<td>120</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Table 4.8** Results of Nuzzler Scan for Group 4

**Figure 4.9** Rule Categories used in Group 4 of Nuzzler IDS
4.2.5 Group 5 Result’s:

This group contains all the rules which are present in both EagleX and Nuzzler IDS. In addition to rule sets used in above four group categories it contains many other rule sets. It is not possible to mention all the rule sets present in both IDS here but some of the rule sets other then those mentioned in above four groups are as follows:

- Chat Rules: These signatures look for people using various types of chat programs (for example: AIM, ICQ, and IRC) which may be against corporate policy.

- Multimedia Rules: These signatures look for people using streaming multimedia technologies. Using streaming media may be a violation of corporate policies.

- Oracle Rules: These signatures detect unusual and potentially malicious oracle traffic.

- Telnet Rules: These signatures are based on various telnet exploits and unpassword protected accounts.

Figure 4.9 shows the ACID console of the EagleX IDS displaying the intrusions detected by EagleX. It also provide other important information like date & time when the database was queried for the results, no. of sensors used, total number of alerts, unique alerts, profile of the traffic etc. Table 4.9 shows the result of the scan for Group5 rules of EagleX. Figure 4.10 shows the rule categories used for Nuzzler Group5 scan.

Table 4.10 shows the result of the scan for Group5 rules of the Securepoint Nuzzler IDS.
<table>
<thead>
<tr>
<th>Rule set name</th>
<th>No. of rules</th>
<th>Detection period</th>
<th>No. of attacks detected</th>
<th>Protocol type of attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the rules present in 48 rule sets of EagleX</td>
<td>2120</td>
<td>8 Days</td>
<td>Total of 6584 attacks were detected</td>
<td>TCP-&gt;6310</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>UDP-&gt;263</td>
</tr>
</tbody>
</table>

Table 4.9 Results of EagleX Scan for Group 5

Analysis Console for Intrusion Databases

Added 1 alert(s) to the Alert cache

Queried on: Fri August 05, 2005 16:42:10
Database: snort@localhost:7768  (schema version: 105)

Sensors: 1
Unique Alerts: 316 ( 2 categories )
Total Number of Alerts: 6584

- Source IP addresses: 16
- Dest. IP addresses: 1060
- Unique IP links 1074
- Source Ports: 3201
  - TCP (3193) UDP (26)
- Dest. Ports: 467
  - TCP (458) UDP (9)

Traffic Profile by Protocol
- TCP (96%)
- UDP (4%)
- ICMP (≤ 1%)
- Portscan Traffic (0%)

Figure 4.10 ACID Display of Intrusions detected by Group 5 rules of EagleX
<table>
<thead>
<tr>
<th>Rule set name</th>
<th>No. of rules</th>
<th>Detection period</th>
<th>No. of attacks detected</th>
<th>Protocol type of attacks</th>
</tr>
</thead>
<tbody>
<tr>
<td>All the rules present in 48 rule sets of EagleX</td>
<td>2347</td>
<td>8 Days</td>
<td>Total of 5847 attacks were detected</td>
<td>TCP-&gt;5667</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>UDP-&gt;180</td>
</tr>
</tbody>
</table>

Table 4.10 Results of Nuzzler Scan for Group 5

![Rules](image)

Figure 4.11 Rule Categories used in Group 5 of Nuzzler IDS

4.2.6 Final Result:

EagleX and Nuzzler detect variety of intrusion attacks thus helping to protect user identity and system from hackers and malicious attacks. Table 4.11 presents the overall
result of the comparison of EagleX and Nuzzler IDS. It uses results of above five groups to reach at the conclusion that EagleX is a better intrusion detection system than Nuzzler.

<table>
<thead>
<tr>
<th>Sr. No.</th>
<th>IDS Type</th>
<th>Group No.</th>
<th>Detection Period</th>
<th>No. of attacks detected</th>
<th>% more attacks detected by EagleX</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>EagleX</td>
<td>1</td>
<td>8 days</td>
<td>2088</td>
<td>25</td>
</tr>
<tr>
<td></td>
<td>Nuzzler</td>
<td></td>
<td></td>
<td>1666</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>EagleX</td>
<td>2</td>
<td>7 days</td>
<td>2950</td>
<td>19</td>
</tr>
<tr>
<td></td>
<td>Nuzzler</td>
<td></td>
<td></td>
<td>2474</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>EagleX</td>
<td>3</td>
<td>7 days</td>
<td>3236</td>
<td>12</td>
</tr>
<tr>
<td></td>
<td>Nuzzler</td>
<td></td>
<td></td>
<td>2867</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>EagleX</td>
<td>4</td>
<td>7 days</td>
<td>2270</td>
<td>6.7</td>
</tr>
<tr>
<td></td>
<td>Nuzzler</td>
<td></td>
<td></td>
<td>2127</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>EagleX</td>
<td>5</td>
<td>8 days</td>
<td>6584</td>
<td>12.6</td>
</tr>
<tr>
<td></td>
<td>Nuzzler</td>
<td></td>
<td></td>
<td>5847</td>
<td></td>
</tr>
</tbody>
</table>

Table 4.11 Final result of IDS comparison

EagleX has detected more attacks in each group than Nuzzler IDS. Table 4.11 gives the percentage (%) of more attacks detected by EagleX than Nuzzler. Percentage of more attacks detected by EagleX varies from 6.7% to 25% in different groups. By taking into account all the results mentioned above it can be concluded that EagleX has detected 15% (approximately) more attacks than its counterpart Secure Nuzzler IDS.
5. CONCLUSION

Intrusion detection is still a fledgling field of research. However, it is beginning to assume enormous importance in today's computing environment. The combination of facts such as the rapid growth of the Internet, the vast financial possibilities opening up in electronic trade, and the lack of truly secure systems make it an important and pertinent area of study.

EagleX and Securepoint Nuzzler are both signature based IDS and are very effective in dealing with intrusion activity on windows based systems. They have over 48 rule sets containing more then 2000 rules which help to protect a system from malicious attacks and identity theft. It can be clearly concluded from the data collected by running EagleX and Nuzzler IDS for extended period of time under similar network traffic conditions that EagleX can detect more attacks then Nuzzler. The percentage of more attacks detected by EagleX then Nuzzler varied from 6.7% to 25% in different groups. On an average it can be concluded that EagleX can detect 15% (approximately) more attacks then Nuzzler IDS.

Finally it can be concluded that EagleX is a better Intrusion Detection System then Securepoint Nuzzler and is recommended to be used on Windows based system over Nuzzler IDS.
2. NARRATIVE

2.1 Selected Previous Work Done in this Field

The market for intrusion-detection products, driven by reports of steadily increasing computer security breaches, has grown from $40 million in 1997 to $100 million in 1998 [BACE 1999].

With the increasing variety of IDS products, Cisco Inc., Enterasys Networks and some private organizations funded by DARPA are the very few entities that have done some research on the IDS methodologies and quantitative IDS performance measurements of these tools. A summary of some crucial research done by these companies follows.


“Testing Intrusion Detection Systems” by the National Institute of Standards and Technology ITL, and Massachusetts Institute of Technology Lincoln Laboratory [Mell 2000] explores the types of performance measurements that are desired and that have been used in the past for testing IDS methodologies. Selecting IDS according to these testing methodologies can be a better approach for organizations.

“Intrusion Detection Methodologies Demystified” by Enterasys Networks [Enterasys 2003] examines the advantages, disadvantages of different IDS methodologies and issues with each of the methodology available for uncovering devious network activity.
2.2 Intrusion Detection Tools/Products

There are different commercial tools/products, which are available in the market for the purpose of intrusion detection. Some of the most popularly used tools are discussed in the following sections.

2.2.1 SNORT

Snort is an open source network intrusion detection system, which performs real-time traffic analysis and packet logging on Internet Protocol (IP) networks. It is said to perform protocol analysis and content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes and OS fingerprinting attempts [SNORT 2004]. [see Fig 2.1] Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilizes a modular plug-in architecture. Snort has a real-time alerting capability as well, incorporating alerting mechanisms for syslog, a user specified file, a UNIX socket, or WinPopup messages to Windows clients using Samba's smbclient.

Snort has three primary uses. It can be used as:

1. A straight packet sniffer like tcpdump - Snort is a libpcap-based packet sniffer. Sniffer mode simply reads the packets off of the network and displays them in a continuous stream on the console. It prints out the TCP/IP packet headers and application data in transit on to the screen.

2. A packet logger - (useful for network traffic debugging, etc) Packet logger mode logs the packets to the disk. When Snort runs in this mode, it collects every packet it sees and places it in a directory hierarchy based upon the IP address of one of the hosts in the datagram. Once the packets have been
logged to the binary file, the packets can be read out back out of the file with any sniffer that supports the tcpdump binary format such as tcpdump or ethereal.

3. A full blown network intrusion detection system - Network intrusion detection mode is the most complex and configurable configuration, allowing snort to analyze network traffic for matches against a user defined rule set and performs several actions based upon what it sees.

Figure 2.1 Snort IDS
2.2.2 eTrust Intrusion Detection

eTrust Intrusion Detection from Computer Associates International, Inc. (CA) is a comprehensive security tool that incorporates three key capabilities of network protection, network session monitoring, and web monitoring and filtering in one product. This IDS tool helps defend against network attacks and enforce corporate security policies — meeting the needs of large, high-traffic enterprise networks [eTrust 2004].

This IDS can be categorized as a network-based intrusion detection system (NIDS). It can be placed on the network to detect and prevent attacks that are designed to affect multiple machines, such as Denial-of-Service attacks and more. eTrust IDS can be applied in a network inside the firewall or outside the firewall. Figure 2.2 shows a network system in which eTrust IDS is placed in a network inside the firewall.

![Figure 2.2 eTrust IDS [eTrust 2004]]
2.2.3 PacketAlarm Intrusion Detection and Prevention System

The PacketAlarm Intrusion Detection System identifies intrusions, makes a detailed record of them and optionally triggers an alarm through e-mail, WinPopUp, snmp or syslog. It also actively intervenes in data traffic to block hacker intrusions, worms, trojans and other attacks before they can cause any damage. PacketAlarm IDS also protects the network against network worms long before signatures for anti-virus programs can be created. This IDS is a commercial software that promises to provide maximum quality, performance and security at a minimum price [PA 2004]. This tool includes an IDS/IPS, Firewall and a vulnerability scanner.

Figure 2.3 shows the front end of the PacketAlarm IDS software system. It provides user information like the sensor is local or network based, version of present rules, license state, disk space etc. It also provides information about packets being scanned by the IDS. It gives information about most frequent IP addresses being visited by the system and IP addresses of the other systems visiting the system.
2.2.4 SecurePoint Intrusion Detection System Nuzzler

SecurePoint IDS Nuzzler is event recognition software that not only recognizes events in the network but also activities on the host and in several applications such as Firewalls. This software examines and detects security gaps present in the network. It also controls the network-traffic, analyses and detects illegal data-packets transferred on the network. Thus this software is considered as a comprehensive intrusion detection solution for large and middle sized networks [NUZZLER 2004]. Figure 2.4 show a sample network with SecurePoint Nuzzler Intrusion Detection System installed in it.
SecurePoint Nuzzler IDS can be deployed either inside the firewall or outside the firewall as shown in Figure 2.5. Both strategies have advantages and disadvantages and depending on the company needs it is deployed at one of these two places.

2.3 Overview

EagleX and Securepoint Nuzzler are two of the most well known and advanced intrusion detection systems available in the market today. EagleX uses snort rules for the purpose of intrusion detection which are the most advanced of any open source rules available on the internet today. Securepoint on the other hand has a long history in designing firewalls and other security software. Securepoint also has hardware based IDS besides nuzzler which is a free ware.

2.4 Description of User Interface

EagleX and Nuzzler are both very user friendly intrusion detection systems. Each one has its own unique interface to help user understand the working of the system.
2.4.1 EagleX Main Page

Once the EagleX is installed and configured on the system, the main page of IDS will appear on the screen. Figure 2.5 gives a screen shot of the EagleX main page. This page gives the user general information about EagleX. It gives the general configuration information about the IDS [Engage Security 2003]. Important information like snort version being used; where snort is installed on the system; where the log files of the IDS are stored; ACID (analysis console for intrusion detection) URL address is also displayed. The EagleX main page contains several options that are described next:

- **Start/Stop Snort**: This button is used to start and stop snort engine which is used for the purpose of intrusion detection.

- **View Alerts**: This button is used to the alerts generated by the intrusion detection system using ACID.

- **Reset Alarm**: This option is used to reset the alarms on the ACID console.

- **Test Settings**: This option is used to test the current settings of the IDScenter.

- **Apply**: Apply is used to apply the current settings after making changes in them.
2.4.2 EagleX Rules/Signatures:

EagleX Rules/Signatures option is available in the wizard options on the main screen. Once selected, it will display the rules/signatures window shown in Figure 2.6. It displays the rule sets used by the IDS [Engage Security 2003]. A rule set can be selected or deselected from the IDS by clearing the check mark box in front of every rule set. Every rule set in turn contain the rules which are compared with the network traffic for the purpose of intrusion detection. For each rule that exists, every packet has to be checked against it. Consequently, fewer the rules being checking against a packet, the faster the IDS can work. On the other hand, fewer the rules being checked less useful the IDS may be. Tuning is the most time consuming part of the IDS. System administrator’s can add/write a new rule, remove an existing rule or edit an existing rule using
EagleX rules/ signatures option shown in Figure 2.6.

![EagleX Rules/Signatures](image)

**Figure 2.6 EagleX Rules/Signature**

2.4.3 EagleX Alerts Display:

EagleX uses ACID (Analysis Console for Intrusion Detection) to display the alerts generated. Figure 2.7 displays the alerts generated by EagleX. ACID also provide important information like IP address from where the attack originated; number of intrusion attempts from any specific IP; number of systems from where the attacks are coming; description of the attack; description of the rule that detected the intrusion; protocol of attack (TCP/UDP/ICMP) among other things.
Figure 2.7 EagleX Alerts

2.4.4 Nuzzler Main Window

Nuzzler IDS is a product of the Securepoint Company which specializes in information security. Nuzzler is a windows based IDS [NUZZLER 2004]. Once installed and configured on the system the main window of nuzzler IDS shown in Figure 2.8 will appear. The main window contains several options/windows that are described next:

- **Start/Stop Option**: Start and Stop buttons are located on the top and are used to start and stop the working of intrusion detection system.

- **Real time Traffic**: Real time window displays the network traffic in real time as it passes the IDS.

- **Dialog Tab**: Dialog tab contains different options available in the IDS to the user for the purpose of configuring and using the IDS efficiently.
- **Packet Information**: Packet information displays the information about any particular packet passing through the network. Once any specific packet is selected in the real time traffic window, its detailed information is displayed in the packet information window.

- **Data content of packet**: This window displays the data content of the packet whose packet information is displayed in the packet information window.

- **Message List**: Message list is a very important window and displays the intrusion activity detected by the IDS.

![Nuzzler Main Window](image)

**Figure 2.8** Nuzzler Main Window

### 2.4.5 Nuzzler Rules

Nuzzler rules can be viewed by selecting “Rules” option in Nuzzler main window (Figure 2.8). Once the rule option is selected rules window appear as shown in Figure 2.9. The rule window contains the rules set currently being used by the IDS. To display rules in any particular rule set, select the rule set and click the advance button and the
ruleset window opens which displays the rules in that particular rule set [NUZZLER 2004]. Ruleset window has different options like deleting, editing and writing new rules for a particular ruleset.

![Nuzzler Rules](image)

**Figure 2.9 Nuzzler Rules**

### 2.4.5 Nuzzler’s Trusted Address List

The trusted address list is a policy table to ensure that only authorized computers are running in the internal network. For example if someone is connecting a computer to an internal network, then it will be reported as an unauthorized action. If that system is added in the trusted address list of the IDS, then from that point onwards the computer
will be recognized as trusted and data coming from it will not be checked for intrusion activities.

Figure 2.10 Nuzzler's Trusted Address List
Acknowledgements

I would like to express my deepest gratitude to Dr. Mario Garcia, Associate Professor of Computer Science, Texas A&M University – Corpus Christi, for his expertise in the area of Computer Security and Information Assurance, excellent guidance and encouragement during the period of this project work.

My sincere thanks to Dr. David Thomas, Associate Professor of Computer Science and Dr. Long-zhuang Li, Assistant Professor, Texas A&M University – Corpus Christi, for their keen interest, unending support and warm wishes that provided me the much-needed motivation in completing my project.

And finally heartfelt gratitude to all the faculty and staff of the Department of Computing and Mathematical Sciences, my colleagues and friends for their moral support.
BIBLIOGRAPHY AND REFERENCES


Appendix A: Intrusion Detection Terminology

This section includes a brief explanation of some of the terms that are commonly used with Intrusion Detection Systems [Security Focus 2003].

1. Alert

An IDS alert is a warning issued by the IDS to the system operator when it detects suspicious activity. The IDS sends alerts either locally or to a remote console in a multitude of ways.

2. Anomaly

An anomaly-based IDS examines ongoing traffic, activity, transactions, or behavior for anomalies on networks or systems that may indicate attack. The underlying principle is the notion that “attack behavior” differs enough from “normal user behavior” that it can be detected by cataloging and identifying the differences involved.

3. Bandwidth

Bandwidth is the maximum amount of data that can traverse a network segment. Bandwidth usage is a great tool to an IDS analyst, as unexpected increases can give an early warning of a DDOS attack or correlate a suspicious event.

4. Enumeration

Enumeration is when an attacker actively probes a network to discover what hosts and services are present. As this action is no longer passive it can be detected, though many networks reveal this information with minimal active probing.
5. Evasion

Evasion is the process of carrying out an attack without an IDS successfully detecting the attack. The trick is making the IDS see one thing and the target see another. One form of evasion is to set different time to live (TTL) values for different packets. Therefore, the information passing the IDS will seem harmless, however the TTL on the harmless bit is less than that which is required to reach the target host. Once beyond the IDS and nearing the target, the harmless piece is dropped leaving the harmful remains.

6. Heuristics

The term heuristics is used where artificial intelligence (AI) is used to detect intrusions. IDS that genuinely use heuristics have been around for a decade.

7. Desynchronization

Originally the term desynchronization was used for evasion methods using sequence numbers. Some IDS could be confused about what sequence number it should expect, and the resulting inability to reconstruct data effectively blinds it.

8. Exploits

For every vulnerability their is an exploit, i.e. a mechanism by which to exploit the vulnerability. An exploit can be considered the means of taking advantage of the structural weakness of the vulnerability. In order to attack a system, a hacker 'exploits' vulnerabilities in the code.

9. False Negatives

A false negative occurs when an attack or an event is either not detected by the IDS or is considered harmless by the analyst.
10. False Positives

An event that is picked up by the IDS and declared an attack but is actually harmless.

11. Honeypot

A honeypot is a system that can simulate one or many vulnerable hosts, providing an easy target for the hacker to attack.
Appendix B: Default EagleX and Nuzzler Rules

EagleX and Nuzzler come with a rich set of rules. These rules are divided into different files. Each file represents one class of rules. The source code distribution of EagleX and Nuzzler has the following set of rules:

- attack-responses rules
- backdoor rules
- bad-traffic rules
- chat rules
- ddos rules
- deleted rules
- dns rules
- dos rules
- experimental rules
- exploit rules
- finger rules
- ftp rules
- icmp-info rules
- icmp rules
- imap rules
- info rules
- local rules
- misc rules
- multimedia rules
- mysql rules
- netbios rules
- nntp rules
- oracle rules
- other-ids rules
- p2p rules
- policy rules
- pop3 rules
- porn rules
- rpc rules
- rservices rules
- scan rules
- shellcode rules
- smtp rules
- snmp rules
- sql rules
- telnet rules
- tftp rules
- virus rules
- web-attacks rules
- web-cgi rules
- web-client rules
- web-coldfusion rules
- web-frontpage rules
- web-iis rules
- web-misc rules
- web-php rules
- x11 rules