State-of-the-art Intrusion Detection: Technologies, Challenges, and Evaluation

Information theory Divison,
Dept of Electrical Engineering,
Linkoping University.

By

Peddisetty Naga Raju

LiTH-ISY-EX-3586-2005

Linkoping, Feb 2005.

Master's Thesis

State-of-the-art Intrusion Detection: Technologies, Challenges, and Evaluation

at Information theory Division,
Dept of Electrical Engineering,
Linköping University.

By

Peddisetty Naga Raju

LiTH-ISY-EX-3586-2005

Examiner and Supervisor: **Prof. Viiveke Fåk**

Linkoping, Feb 2005.

Defence date

24th Feb 2005

Publishing date (Electronic version)

Department and Division

Information theory division,
ISY

Linköpings universitet

Language

☒English
□Other (specify below)

□ ______________

Report category

□Licentiate thesis
☒Degree thesis
□Thesis, C-level
□Thesis, D-level
□Other (specify below)

□ ________________

ISBN:

ISRN: LiTH-ISY-EX-3586-2005

Title of series

State-of-the-art Intrusion Detection: Technology⊞

Series number/ISSN

URL, Electronic version

http://www.ep.liu.se/exjobb/isy/2005/3586

Title

State-of-the-art Intrusion Detection: Technology, Challenges, and Evaluation.

Author(s)

Peddisetty Naga Raju

Abstract

Due to the invention of automated hacking tools, Hacking is not a black art anymore. Even script kiddies can launch attacks in few seconds. Therefore, there is a great emphasize on the Security to protect the resources from camouflage. Intrusion Detection System is also one weapon in the security arsenal. It is the process of monitoring and analyzing information sources in order to detect vicious traffic. With its unique capabilities like monitoring, analyzing, detecting and archiving, IDS assists the organizations to combat against threats, to have a snap-shot of the networks, and to conduct Forensic Analysis. Unfortunately there are myriad products in the market. Selecting a right product at time is difficult. Due to the wide spread rumors and paranoia, in this work I have presented the state-of-the-art IDS technologies, assessed the products, and evaluated. I have also presented some of the novel challenges that IDS products are suffering. This work will be a great help for pursuing IDS technology and to deploy Intrusion Detection Systems in an organization. It also gives in-depth knowledge of the present IDS challenges.

Keywords

IDS, Challenges, Evaluation, State-of-the-art IDS, Evasion attacks, IDS features, zero-day attacks, Encrypted traffic.

ACKNOWLEDGEMENT

This work is a piece of gratitude to my parents. I would like to thank, Mr. Venkata Sastry for his spirit filled suggestions when I was in deep trouble waters. I am very grateful to Mr. Venkata Prasad Putcha, Prof at Kings College, London, for his esteem. I am very thankful to Mr. Raveendra Somarouthu and Balaji Yadam for my inroads to US. I am thankful to Rami Reddy and Chandra Sekhar Reddy Alla for their concern

I am thanking Prof. Viiveke Fåk for her advices during the work and for the opportunity to work on this project. I would like to thank all my well wishers and friends for their love towards me. Thanks to David Akhvlediani, my Georgian friend.

ABSTRACT

Due to the invention of automated hacking tools, Hacking is not a black art anymore. Even script kiddies can launch attacks in few seconds. Therefore, there is a great emphasize on the Security to protect the resources from camouflage. Intrusion Detection System is also one weapon in the security arsenal. It is the process of monitoring and analyzing information sources in order to detect vicious traffic. With its unique capabilities like monitoring, analyzing, detecting and archiving, IDS assists the organizations to combat against threats, to have a snap-shot of the networks, and to conduct Forensic Analysis. Unfortunately there are myriad products in the market. Selecting a right product at time is difficult. Due to the wide spread rumors and paranoia, in this work I have presented the state-of-the-art IDS technologies, assessed the products, and evaluated. I have also presented some of the novel challenges that IDS products are suffering. This work will be a great help for pursuing IDS technology and to deploy Intrusion Detection Systems in an organization. It also gives in-depth knowledge of the present IDS challenges.

Keywords: IDS, Challenges, Evaluation, State-of-the-art IDS, Evasion attacks, IDS features, zero-day attacks, Encrypted traffic.

Table of Contents

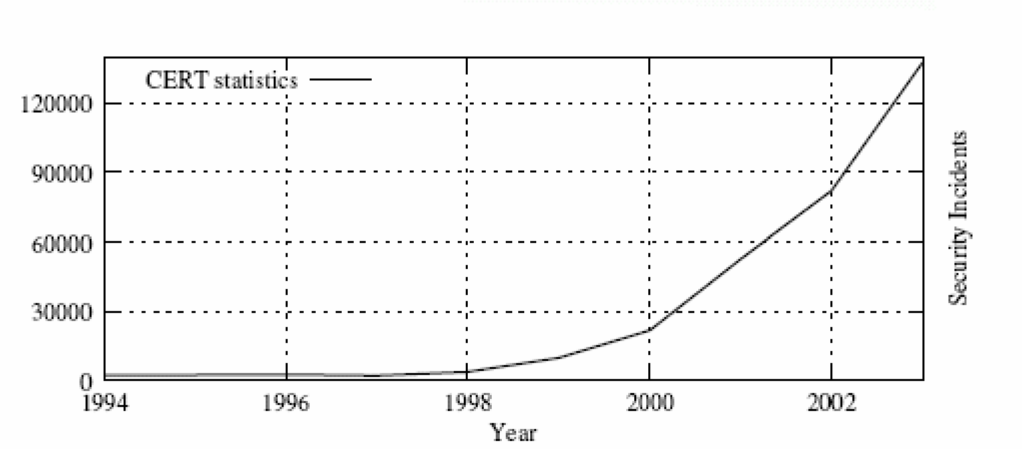
Chapter1 Introduction

Anderson, while introducing the concept of intrusion detection in 1980 [1.1], defined an intrusion attempt or a threat to be the potential possibility of a deliberate unauthorized attempt to

- Access information,
- Manipulate information, or
- Render a system unreliable or unusable.

Intrusion Detection is the process of monitoring and analysing the information sources, in order to detect malicious information. It has been an active field of research for over two decades. John Anderson's "Computer Security Threat Monitoring and Surveillance" was published in 1980 and has embarked upon this field. It was one of the earliest and most famous papers in the field. After that in 1987, Dorothy Denning published "An Intrusion Detection Model", provided a methodological framework that inspired many researchers around the world and has laid the groundwork for the early commercial products like Real Secure, Trip Wire, Snort, Shadow, and STAT etc.

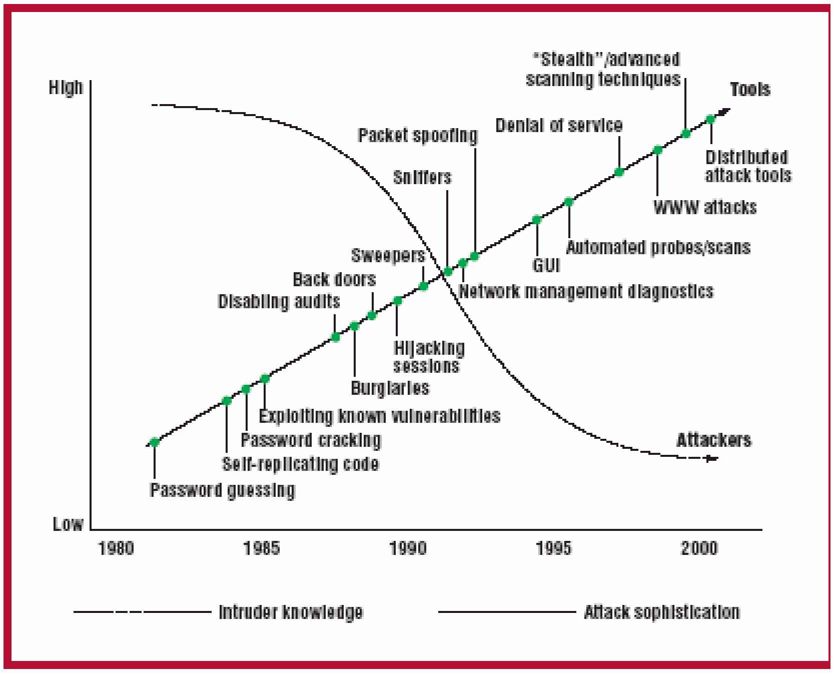
Despite some hurdles, Intrusion Detection technology has evolved and emerged as one of the most important security solutions to consider. It has several advantages and it is unique compared to other security tools. Apart from detection, it has several other benefits like archiving of the event data, allowing reports, and in combating against novel and complex attacks. All these features make ID technology to play a different role in protecting the organizations. Within its boundaries it can be considered as an important tool to protect the resources as part of the overall defence.



During 1990s, Internet has revolutionized and made the world to depend on it. Internet has given boon to the world as "World Wide Web", without it present lives are hard. With the advent of WWW, Educational Institutes, Government Organizations, Auction shops, Trading organizations, News Papers, Travel Organizations, Mail Services, Banking and almost all are now connected to the Internet and are available on-line.

Several e-commerce trading organizations have also risen during these years and became more attractive for the nefarious hackers. The evolution of Internet has also resulted in the raise of worms, viruses, DoS attacks, and several complex attacks. Connecting to the Internet is connecting to the whole world of computers, and exposing to all these kinds of malicious traffic. The above graph from CERT [1.2], explains how the number of attacks are increasing.

During 1980s, evil purpose hacking was considering as Black Art and the Intruders were experts developing their own tools. Now-a-days exploits can happen in a matter of seconds. Anyone can attack Internet sites using automated tools and exploit scripts that capitalize on well-known vulnerabilities. There are several sources for these kinds of automated tools maintained by the hacking community. These automated tools have resulted in the surging of attack complexity and the decrease of technical knowledge. The figure depicted below from CERT [1.3], gives an overview of attack sophistication versus Intruder technical knowledge.



The phenomenal growth of attacks and their complexity, and decreasing Intruder knowledge made the attacks ubiquitous. To make the networks open means exposing the networks to the attacks and misuse. So, Security has become major concern for the organizations. There are myriads of security tools ranging from Antivirus to Intrusion Prevention. Every tool has its strengths and weaknesses. No product has emerged as a security panacea. Albeit Firewalls gained lot of focus, they have their own advantages and limitations. Anti Virus products have their own strengths and limitations. The limitations of these individual products practiced in the traditional network security given origin to "Defence in Depth" approach of today's Network Security.

"Don't put all Eggs in one Basket".

The Defence in Depth approach of Network Security is similar to the above proverb. It means that; do not fight with one security tool. This approach enforces to divide the security into multiple layers and to protect each layer with the appropriate product. This approach increases the protection, allows more time to respond, and makes the attacker's job difficult by placing different barriers in between.

According to The Defence in Depth approach, Security of organizations is divided into the following layers.

1. Vulnerability Scanning & Security Policy
2. Host System Security.
3. Router Security.
4. Firewall Security.
5. Intrusion Detection
6. Intrusion Prevention.
7. Incident Response Plan.

Most of the people have a common myth that Firewalls protect the networks as a stand-alone security solution, which is not true from the above illustration. Intrusion Detection beyond the firewall is considered as the perfect fit of the organizational security approach. IDSs are installed in addition to firewalls and they carry out a check at an internal level, on the customer side of the network. They extend the Monitoring and Protection of the Networks. Firewalls are not good in detecting the Insider Threats (Both authorized and unauthorized), which constitutes the 60% of the attack landscape. These internal attacks are very expensive. For example, companies surveyed for the 1998 "Computer Crime and Security Survey" by the Computer Security Institute and FBI [1.4], reported average losses of $2.8 million from incidents of unauthorised access. This alone can explain how important it is to protect from the Insider threats and this example fosters us the impression that IDS with its ability to detect Insider threats can play a vital role in the overall security infrastructure.

ID systems can be classified primarily into two categories: Host-Based and Network-Based. In Host based, it monitors the operating system logs and Files. In Network-Based Systems they monitor the network packets in transit and analyze them. Overall, ID technology is excellent in detecting Insider threats, and is a powerful tool in Forensic Analysis.

There are several types of commercial products in the market, characterized by different monitoring, analysis, response, architecture and detection approaches. Each approach has distinct advantages and disadvantages. There are several design approaches used in Intrusion detection. These drive the features provided by specific IDS and determine the detection capabilities for that system. The wide array of intrusion detection products available today addresses a range of organizational security goals and considerations. Given this myriad range of products and features, the process of selecting products that represent the best fit for organizational goal is, at times difficult. Given the nature of modern network security threats, the most sought after question for security professionals is, which intrusion detection features and capabilities to use and which can fit their security goals of the organization and what are the challenges associated with ID technology, which is the motivation of this thesis work.

In chapter 2 of this thesis work, we will present the overview of Intrusion Detection; we present how this technology is different from Firewalls and the myths associated with ID Systems. We present comprehensive technical background on the functionality of the ID Technology. We will present a Real- world Analogy. At last we will demonstrate how an IDS can detect Buffer Overflow Attack.

In chapter 3, we will select six commercial Intrusion Detection products randomly. We will present the skeleton of the general and ideal commercial IDS. We will explain briefly about the features and their importance. Then we will match the features that are described with the products selected. This chapter will serve the second step of the selection process for IDS products after the first step of gaining the overview of ID technology preceded by setting up the requirements and goals. To give a nice view of these results, it will be presented in a tabular format. Since there are hundreds of products available, with this step users can screen out most of the products by matching their organizational environments.

In chapter 4, we will present the state-of-the-art Intrusion Detection challenges and their importance. These challenges represent the problems and issues to keep in mind before deploying IDS. These challenges will be the building block for the next chapter of Evaluation Criteria. We will present some of the more powerful attacks and their potentiality in destruction.

In chapter 5, we will develop the Evaluation Criteria, to evaluate the commercial products. This will help in selecting the better ID solution in general. This evaluation criterion will not address any specific commercial product and it will not target any specific organisation. This criterion will be useful in examining a particular feature how it works and how efficient it is.

In chapter 6, we will evaluate the selected commercial products. These results are mostly anecdotal rather than rigorous scientific testing. Due to the resource constraints, this evaluation will not be done on real-world testing. These results are obtained based on the evaluation criteria developed in the previous chapter, Evaluation criteria. These results will be based on the product data sheets and personal communication with the product manufacturers, third party evaluations, and from the survey of the IDS products in chapter 2.

Finally, we will conclude with the work carried out.

Chapter 2 Intrusion Detection Technology

In the last three years, the networking revolution has finally come of age. More than ever before, we see that the Internet is changing computing, as we know it. The possibilities and opportunities are limitless; unfortunately, so too are the risks and chances of malicious intrusions.

It is very important that the security mechanisms of a system are designed so as to prevent unauthorized access to system resources and data. However, completely preventing breaches of security appear, at present, unrealistic. We can, however, try to detect these intrusion attempts so that action may be taken to repair the damage later. This field of research is called Intrusion Detection.

2.1 Overview

Since Anderson's Paper in 1980 [2.1], several techniques for detecting intrusions have been studied. Several new methods of detection mechanisms have been introduced. Lot of research efforts were initiated resulting in more efficient Intrusion Detection Technology. In this chapter we discuss why intrusion detection systems are needed, the main techniques, present research in the field, the overview of detection methods and modes, and we present a brief description about the main Intrusion Detection Technology.

Intrusion detection is the process of monitoring the events that occur in a computer system or network and analysing them for signs of intrusions, defined as attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network. Intrusions are caused by attackers accessing the systems from the Internet, authorized users of the systems who attempt to gain additional privileges for which they are not authorized, and authorized users who misuse the privileges given to them. Intrusion detection technology strengthens the network security by contributing to one of the layers of network security.

Intrusion detection allows organizations to protect their systems from the threats that come with increasing network connectivity and reliance on information systems. IDSs have gained acceptance as a necessary addition to every organisation's security infrastructure. Albeit Intrusion Detection Technology cannot offer complete protection against the attacks, it enhances the defence-in-depth or layered approach, which is the vogue trend of Network security.

We shall review here how an Intrusion detection product is different from other network security products and why we need to use it and how it enhances the network security perimeter.

2.1.1 Firewall

Firewall is a network security device, which works on the defined and configured security policy. It is one of the security products that implement the security policy. It is also imperative that it cannot offer the complete protection against the malicious traffic. The basic difference between a firewall and an IDS is, Firewalls offer active protection against the attacks, where as IDS products can raise an alert and detect the attacks, with the passive detection only mechanism. Like firewalls, Intrusion detection products also cannot offer complete protection and cannot replace any other products.

Firewall:

1. Firewall provides the access control of the Internet traffic from inside and outside.
2. It works actively by the configured security policy and by allowing only the legitimate traffic defined by the security policy.

For example, a firewall can be configured to allow certain traffic to port 80 of the web server, and certain traffic solely to port 25 of the e-mail server. In this example it can be clearly observed that firewall does not examine the contents of the legitimate traffic.

2.1.2 Why Firewalls are not enough?

This is one of the most common questions for novice people of Intrusion detection systems. Since most of the people think that their firewall can solely protect their network, which is not true from the above-mentioned demonstration and example.

So, let us see the draw backs of firewalls, the inability of firewalls, how IDS complements firewalls and why firewall is not only enough [2.2]

- Not all access to the Internet occurs through the firewall.
- Not all threat originates outside the firewall.
- Firewalls are subject to attack themselves
- they do not examine the contents the of the legitimate traffic
- Firewalls does not offer any protection if the network is breached.
- Firewalls cannot prevent all kinds of attacks and variants of the attacks.
- it does not offer any kind of forensic analysis.

2.1.3 Several attractive reasons to acquire and use IDSs:

1. To provide the possible information about intrusions and attempts that have taken place, allowing the diagnosis improvement, recovery, and correction of causative factors.

2. To act as quality control for security design and administration, especially of large and complex enterprises.

3. To detect the purpose of attacks.

4. To prevent problem behaviours by increasing the perceived risk of discovery and punishment for those who would attack or otherwise abuse the system.

5. To detect attacks and other security violations those are not prevented by other Security measures.

2.1.4 Real-world Analogy:

In the real world, IDS are analogous to the burglar alarms in a house. Let us say the authentication control device, which is located at the entrance of the door as Firewall. It controls the access to the house by ID-card and password. There are several ways to bypass this device. Either a thief can break the window and successfully enters the house with out detecting by anybody, or a thief can spoof the ID-card and password.

In both of the above cases, a thief is undetected and there is no information what he gained, how he gained the assets, who is the thief and when did he attempted the burglary. Let us see how it is different with the burglar alarms.

Burglar alarms are activated in the house and configured to raise alarm if somebody enters. If a thief enters the house, the burglar alarm raises an alarm there by causing to alert the security guard and the owner of the house, it can inform the associated person, it can record when it has happened and further information depending on the configured policy and the processing capability of the burglar alarm.

So, the burglar alarms reduce the damage of burglary, provides extensive information and clues for the forensic investigation to take a legal action against the thieves. The Intrusion detection, which also incorporates functionally similar mechanisms, reduces the risk, helps in forensic investigation, and helps to report the events to the management.

Here we discuss some of the myths associated with the Intrusion Detection Technology.

2.1.5 What an IDS can do

- they give the clear picture on what is going on in the network and system.
- IDS can detect the reconnaissance attacks and alerts the system.
- it offers greater flexibility and integrity to the existing security infrastructure.
- they can log the sessions of activities in specified format.
- it provides and enhances the process of forensic investigation with the help of session logs, correlation of events and GUIs.
- they monitor the network or systems in real-time and do the real-time analysis.
- they can alert the security persons with the specified patterns.
- they can take active responses like altering ACL, blocking the IPs, shutting down the connections.
- they enable efficient way of reporting for the management.
- More importantly, IDS provide guidelines that assist in developing the security policy of the organization.

2.1.6 What an IDS cannot do

- they are just active, not proactive. They cannot prevent the attack.
- they are not automated, they need significant human resources for their management.
- they cannot offer complete protection for the resources. It is just an additional layer of security. It is not a panacea.

- they cannot compensate for the loopholes in network protocols.
- they cannot protect all kinds of attacks. They have limitations.
- they cannot weather to high volumes and high speeds of Internet traffic.

2.2 IDS Technology

Here we are presenting the Intrusion detection Technology in a taxonomical way. There are several types of IDSs available today, characterised by different monitoring and analysis approaches. Each approach has distinct advantages and disadvantages. All theses approaches can be described in terms of a generic process model for IDSs.

Many IDSs can be described in terms of the following components:

- Location of the IDS
- Detection Methods
- Responses
- Timing
- Architecture.

2.2.1 Location of the IDS

The most common way to classify IDSs is to group them by location of the information source where they operate. The primary information sources are, network packets, captured from network backbones or LAN segments, Operating systems and critical files. IDS can be classified as Network-based and Host Based primarily.

2.2.1.1 Network-based IDSs

The most common form of commercial intrusion detection systems is network-based. These systems detect attacks by capturing and analyzing network packets by listening onto the network segment or switch. They do this by matching one or more packets against a database of known "attack signatures", or performing protocol decodes to detect anomalies.

Network based IDS is capable of both raising alerts and terminating the connections instantaneously whenever it notices suspicious activity. "Promiscuous mode" is the most common form of operation and they monitor every packet that is in transmission of the local segment. As the sensors are limited to running the IDS, they can be more easily secured against an attack as many sensors run in stealthy mode, which makes the attacker more difficult to find the presence and location of IDS.
Advantages:

- Network-based IDS is very secure as they run in stealthy mode and it makes hard to their presence and location.
- its deployment has little impact on the network. NIDS are usually passive devices that listen onto the network wire without interfering with the normal operation of a network.

- a large network can be monitored by a few well-placed NIDS.

Disadvantages:

- Some NIDS have problems in dealing with fragmenting packets, which can cause the IDSs to become unstable and crash.
- many of the advantages of the NIDS do not apply to more modern switch-based networks.
- they have problems in dealing high speeds and high volumes of traffic.
- NIDs cannot analyze encrypted information.

2.2.1.2 Host-Based IDS

Host-based IDSs operate on information collected from within an individual computer system. HIDS employ an agent that resides on each host to be monitored. Generally most common forms of information sources for host-based IDSs are operating system audit trails, system logs and critical system files. The agent scrutinises these auditable resources looking for unauthorized changes or suspicious patterns of activity. This allows host-based IDSs to analyse activities with great reliability and precision, determining exactly which users and processes are involved in a particular attack on the operating system. With these kinds of systems the outcome can be determined unlike NIDS, as host-based IDSs can directly access and monitor the data files and system processes usually targeted by attacks.

Advantages:

- they can help detect Trojan horse or other attacks that involve software integrity breaches when they operate on OS audit trails.
- these kind of systems are unaffected by switched networks.
- Host-based IDSs with their ability to monitor events local to a host, can detect attacks that cannot be seen by a network-based IDS.
- they can process the encrypted information.
- HIDS are very good in detecting at insider threats

Disadvantages

- Host-based IDSs are harder to manage, as information must be configured and managed for every host monitored.
- Host-based IDS can be disabled by certain kinds of denial-of-service attacks.
- They are not well suited for detecting network scans or other such surveillance attacks that targets an entire network, because the IDS can only see those network packets that are received by its host.
- when dealing with OS audit trails the information can be immense, results in additional local storage on the system.
- they may be attacked and disabled as part of the attack.

2.2.1.3 File Integrity Checkers

Albeit File Integrity checkers are not a different kind of IDS, they are considered as another kind of Host-based ID systems due to their similarity in location and functionality.

They use message digest or other cryptographic checksums for critical files and objects, comparing them to reference values, and flagging differences or changes.

Attackers often alter system files, at three stages of the attack [2.3]. So, the use of cryptographic checksums is important. First, they alter system files as the goal of the attack (e.g. Trojan Horse placement), second, they attempt to leave back doors in the system through which they can re-enter the system at a later time, and finally, they attempt to cover their tracks so that system owners will be unaware of the attack.

At Regular intervals, the File integrity checkers recalculates the checksum values and compares them against the already archived. It raises an alert whenever it finds an intruder altering files that makes it a perfect technology for examining the true extent of the damage caused by a successful attack. Thus, its strength lies in forensic analysis and it is not useful where real-time analysis is essential, since its scans are periodic.

2.2.2 Detection Methods

Detection methods are the kernels of the Intrusion detection Technologies. Actually, the detection methods are the core engines in detecting the malicious activities of the information source.

They have to be developed and configured prior to monitor the associated information source. These developed detection methods function automatically, analyse the information they monitor and raises alarms whenever they detect malicious traffic. There are several different approaches for the detection of malicious traffic depending on the data to monitor. For example, to detect worms in network protocols, protocol decode is the right detection method rather than signature-based detection.

Signature-based, Traffic anomaly based, Stateful pattern matching, Protocol anomaly based, and Heuristic analysis are the vague detection methods that are in use and mentioned below.

2.2.2.1 Signature-Based Detection

Signature based detection, which is also called as Pattern Matching is primarily done using Pattern matching. The most common form of signature based detection is string matching. The main idea behind this is to detect even the known variations of the known attack patterns.

The functionality of the signature based detection methods resembles the Virus scanners, in which they can detect all known patterns of attacks. The other synonym for this method is Misuse detection. To detect the malicious events through this method requires a comprehensive database of signatures of all known attacks and their variants. The diagram depicted above can give lucid picture of signature-based detection of the worms.

The strength of signature-based detection is in detecting all known patterns of attacks effectively. The vulnerabilities of this method include:

- they are easy to elude by the zero-day attacks as it is mentioned in chapter 4.
- they need constant upgrade and maintenance.
- it is not effective at high speeds, since it has to match all the packets with all the signatures till it detects an attack, which obviously requires huge amount of computing resources.

2.2.2.2 Anomaly based detection:

This is also one of the most common detection methods and it depends on the normal profile database of the malicious events. The simplest approach to this method is ignoring everything that is "Normal" and raising alarm if it deviates from the "normal". An anomaly detector operates on the assumption that malicious events are different from normal (legitimate) actions. So they find out these differences to detect attacks. Anomaly detectors construct profiles from historical data collected over a period of normal operation. The detectors then collect event data and use a variety of measures to determine when monitored activity deviates from the norm and raises alarms.

Since the set of intrusive activities only intersects with set of anomalous activities instead of being exactly the same, it generates both false positives and false negatives. So, the primary attention must be paid on selecting the threshold levels and the selection of information sources to monitor.

Advantages:

- Anomaly detectors can produce information that can in turn be used to define signatures for misuse detectors.
- they are effective in detecting unknown attacks like zero-day attacks.

Disadvantages:

- Anomaly detectors often require extensive "training sets" of system event records in order to distinguish normal legitimate and bad traffic. For example, the installation of a new application, albeit it is perfectly legitimate.
- it normally generates huge number of false alarms for the changes in standard operations while intrusion attempts that appear to be normal may cause missed detections.
- It cannot specifically identify an attack, nor can it provide any sense of whether the attack was successful or not.

2.2.2.3 Protocol anomaly based detection

Interpreting the packet according to the protocol and analysing for intrusive attempts is called as protocol anomaly based detection. It has the advantage of detecting anomalies in packet contents very quickly than doing an exhaustive search of a signature database. This method is also very efficient in detecting attacks that are hard to analyse by the pattern-matching technique and new variations of old attacks.

The prime functionality of this technique is, incorporating the rules employed by the appropriate RFCs to monitor for malicious events. It assists in detecting certain anomalies such as binary data in an HTTP request, or a suspiciously long piece of data where it is not supposed to be, is a sign of possible buffer overflow exploit.

Advantages:

- it empowers more efficient handling of traffic and improved scalability as more signatures are added.
- it diminishes the false positives with a lucid defined and enforced protocol rules.
- it enables to detect tiny variations of exploits without having to implement separate signatures.

Disadvantages:

- If it encounters a completely novel kind of attack, it forces to develop a new signature to analyse that attack.
- it is strictly bound to the RFC rules.

2.2.2.4 Stateful Detection Method

Stateful signature based detection method stemmed from the inability of signature matching method to detect the multi-step attacks. This method ensures the perfect operation of the following

- TCP Reassembly: the ability to reassemble the TCP segments properly in the right order and without overlapping. For more information on TCP Reassembly attacks, please turn over to chapter 4.
- Tracking state: the ability to track states at the TCP layer (e.g., three way handshake, four way tear down) and IP layer.
- IP de-fragmentation: The ability to perfectly reassembling the fragments of packets in right sequence. For more information on IP fragmentations go to chapter 5.

The strengths of this method are detection of IDS evasion attacks, ability to detect multi-stage attacks, and lengthy packet attacks. The downside is, it requires more computing resources and is not reliable at very high speeds.

2.2.2.5 Heuristic Based Detection

This method uses some form of algorithmic logic to detect the intrusion attempts. This algorithm usually consists of the statistical evaluations of the type of traffic being presented. It also uses artificial intelligence, self-organising maps and neural networks. This method offers a more sophisticated algorithm for the alarms. The strength of this method lies in detecting the more complex forms of malicious traffic, while the pitfalls are, it generates too many false positives and it is more tuning intensive.

2.2.3 Response

Response is the set of actions that the system takes once it concludes the information source is malicious. Response is the capability to recognize a given activity or event as an attack and then taking action to prevent the attack or otherwise affect its ultimate goal.

The most common forms of responses falls into two major categories: active responses and passive responses. They are described below.

2.2.3.1 Active Responses

These are the kind of responses enforced by the IDS to respond to an attack. Active responses are taken immediately and automatically by the IDS. The common active responses are, collecting additional information about a suspected attack, taking immediate action against the intruder, and suspending the progress of attack.

- Collecting additional information for suspicious attacks, is useful to thwart the future attacks, to determine whether an attack is successful or not, and to assist in the forensic investigation of the attacks.
- Taking immediate action against the intruder would allow taking action against the attacker and it also notifies the attacker that the IDS has detected him. But it has some legal ambiguities about civil liability and includes more risk.
- suspending the progress of an attack is more efficient form of active response taken by the IDS. It allows halting the progress of an attack. Blocking the IP addresses, blocking ports, injecting TCP resets to terminate the connection, changing the ACL, reconfiguring routers and Firewalls are the common active responses.

2.2.3.1 Passive Responses

These are normally taken by the human administrator to respond to an attack. This process would occur after the collection and correlation of event data by the administrator. Here are the different kinds of passive responses.

- Alarms and notifications are generated by IDSs to inform users when attacks are detected. The most common form of an alarm is an onscreen alert or popup window. It can be displayed on the IDS console or on other systems as specified by the user during the configuration of the IDS.
- SNMP traps and messages generate alarms, alerts and report them to the network management systems. These allow the entire network infrastructure to respond to the attack and the ability to use common communication channels.

2.2.4 Timing

Timing refers to the elapsed time between the events that are monitored and the analysis of those events. Based on the analysis of events that have been monitored, IDS products falls into two major categories.

2.2.4.1 Post-Event audit Analysis

In interval-based IDSs, the information flow from monitoring points to analysis engines is not continuous. In effect, the information is handled in a fashion similar to “store and forward” communications schemes. Many early host-based IDSs used this timing scheme, as they relied on operating system audit trails, which were generated as files. Interval-based IDSs are predicted from performing active responses. It is also called as Batch-mode analysis and Interval-mode analysis.

This type of analysis has two key advantages:

- It addresses tremendous difficulties that organizations experience while analysing audit trails. It can reduce the costs incurred with the auditing.
- This kind of analysis allows refining of data, that is, it allows to go back to past and do historical analysis of events.

The primary pitfall of this method is, by the time it detects an attack, it would be too late to respond and protect the data, and by that time the nefarious attacker have already done the damage.

2.2.4.1 Real-Time audit Analysis

Real-time IDSs operate on continuous information feeds from information sources. This is the predominant timing scheme for network-based IDSs, which gather information from network traffic streams. In network-based IDS, this method usually operates in "promiscuous" mode and it monitors the traffic and analyse it in real-time. It does this by examining both header fields and packet contents. This method is also able to take active responses in order to prevent the progress of attack.

The palpable advantage with this method is, it can halt the attacks with out much delay, to reduce the damage. The downside of this method is it can crash at high speeds and high volumes of traffic.

2.3 IDS and its role in Forensic Analysis

"The process of identifying, preserving, analysing and presenting digital evidence in a Manner that is legally acceptable". (Mc Kemmish, 1999) [2.5].

"Gathering and analysing data in a manner as free from distortion or bias as possible to reconstruct data or what has happened in the past on a system". (Farmer & Venema) [2.4].

2.3.1 What is Forensic Analysis?

Computer Forensics is defined as the process of collecting information sources, analysing them to procure more evidence against an already happened attack in order to leverage action against an Intruder either through legal processing or through electronic. Forensic assists the organizations in procuring the evidence against a threat by collecting additional information in a similar fashion to the civil crime investigation.

Forensic analysis can be divided into four major components.

1. Procurement: This is the process of identifying the evidences, clues, traces and collecting them in a manner they will yield fruitful results in analysis.
2. Preserving: This process includes archiving the evidences to protect them from theft and keeping them safe. Preserving of the evidences is vital in order to present them to the management or authorities.
3. Analysis: It is the process of examining the data to conclude that the activity by an attacker is unauthorized, illegal and evil borne.

4. Presentation: This is the process of presenting the evidences to authorities, courts. It includes how the originator of an attacker relates to that particular attack in an easily perceivable way.

2.3.2 The Bourne of Forensic Analysis

The Forensic analysis serves the following purposes

- It enables organizations to leverage action against attackers through a legal process.
- It provides comprehensive technical knowledge; on how an attack traverse from the source of origin to the destination.
- It enables to conclude who has launched an attack, what has he compromised, what has he not compromised; at what time an attack happened.
- It enforces to prevent the further attacks from the same source and from others as well.

2.3.2 How an IDS assists Forensic Analysis

Albeit there are several different network security products exist, Intrusion Detection systems contribute extensively in the Forensic Analysis. Here we will see how Intrusion Detection Systems assists the Forensic Analysis. From our description of IDS technology, the below mentioned information can be obtained.

2.3.2.1 Host-Log Monitoring

Many of the IDS products use host logs as a source of raw events. Host logs consists of the combination of audit, system and application logs. They offer easily accessible information on the behaviour of a system. Logs generated by high-level entities can often summarise many lower level events. So, the host based IDS monitors operating system logs, application logs and audit trail events which can be treated as valuable information to prosecute an attack. So, the host based IDS serves in the forensic analysis with its logs as information about an attack.

2.3.2.2 Network Monitoring

In Network-based ID systems, they watch all the traffic and ensure that they can store all the data relevant to the communication between the attacker and victim. They archive the details including IP addresses of the originator of an attacker and victim, Port numbers of attacker and victim, the time of the attack, the protocols and services involved in it. So all these information collectively provides required information about an attack.

In addition to the host monitoring and network monitoring, IDS products incorporate several compelling features to assist the Forensic Analysis. They are

- Some of the IDS products allows the data collection and correlation process, which would improve the quality of Forensic analysis. For more information on Data Collection and Correlation, and how it plays an important role in forensic analysis, refer to chapter 4.
- IDS products have the capability to store the events in a format that offers easy

navigation and refining of data.

- Many of the IDS products allow the customisation of archiving, which enables to store desired data that is essential for forensic analysis.
- Most of the IDS products have very good reporting capabilities, allows them to present data in GUI and easily perceptible.
- They offer extensive tracing back to the attacker, which is the prime requirement to for the accountability of attack in forensic analysis.

Albeit ID systems cannot provide the comprehensive information that is required for the complete forensic analysis, the information provided by the IDS as a single product is adequate and IDS plays a vital role for the forensic analysis.

2.4 Complementary IDS tools

There are several tools that complement the functionality of IDSs and some can be used as an integral part of IDSs. Here is the brief explanation of the some of the tools.

2.4.1 Honey Pots and Padded Cell Systems

Honey pots are decoy systems that are designed to lure a potential attacker away from critical systems. They are generally placed at attractive and ubiquitous locations of a network and are designed to receive attacks. The goals associated with honey pots are

- Diverting an attacker from accessing critical systems.
- All the activities are fully logged to collect information about the attacker's intensions.
- They can be used to develop passive fingerprinting techniques and gives an insight into attackers activities.
- Keeping the attacker to stay on the system till security officer responds.

Originally, Honey pots consisted of heavily monitored, real systems or virtual systems implemented by software. The vogue systems are in their entirety and sacrificially designed to appear critical but a legitimate user of the system would not access. These networks usually separated by firewalls, which configured to allow unrestricted incoming access and limited outgoing access. Obviously any access to the honey pot can be suspicious. Sensitive monitors and event loggers are configured to detect these accesses and collect information about the attacker's activities.

Padded cells work in tandem with the traditional IDS. When the IDS detect attackers, it seamlessly transfers them to a special padded cell host. The padded cell can be constructed with interesting data designed to convince an attacker that the action is going according to his plan, and once the attackers enter the padded cell; they are struck in a simulated environment where they can cause no harm. As in honey pots, padded cells are well instrumented and offer unique opportunities to monitor the actions of an attacker.

Advantages:

- Honey pots are effective at catching insiders who are snooping around a network.
- Critical information sources can be secured by diverting the attackers.
- Allows ample time to respond to an attacker activity in honey pots.

Disadvantages:

- By using these devices, there are some legal complications.
- A high level of expertise is needed for administrators and security managers in order to use these systems.

2.4.2 Vulnerability Assessment Systems

Vulnerability systems are the modern systems emerged in the recent years to audit the networks on a regular basis. These systems assists the other network security tools like Firewalls and Intrusion Detection Systems to configure by obtaining the necessary information including what is secure, what is vulnerable etc details.

Intrusion detection systems and Vulnerable Assessment systems are turning increasingly important and are complementing each other. Vulnerability analysis tools allow security managers to reliably generate a "snapshot" of the security state of a system at a particular time.

Vulnerability analysis system process contains sampling of specified system attributes, archiving them, comparing them to the security policy and identifying and reporting the differences.

There are two kinds of Vulnerability assessment systems

- Passive Scanners, where the administrator defines a security policy on his network and the scanner audits all the machines on the network, there by producing which system violates the security policy and what needs to be done to fix the problem.
- Active Scanners, This is a pro active approach, in that it provides a number of known attacks like DoS attacks, Buffer overflow exploits, web server attacks to test the network resources. By probing with an active scanner, the administrator can obtain a clear picture on potential vulnerabilities and the ways to fix them.

Advantages

- Vulnerability analysis systems offer a way for security managers and administrators to double-check any changes that are made to the systems.
- They allow the detection of problems on systems that cannot support IDS.
- They are useful in providing security specific testing capabilities for documenting the security state of systems at the start of a security program.

Disadvantages

- Some network-based checks, especially those for denial-of-service attacks, can crash the systems they are testing.

- Network-based vulnerability analysers are platform-independent, but less accurate and subject to more false alarms.
- Host-based analysers are strictly bound to specific operating systems and applications; So they are often more expensive to build, maintain, and manage.

2.5 How an IDS detects a Buffer Overflow Exploit

In this section we present an example of attacks, Buffer Overflow. We present the code in C language and a description is also given to present novice readers and network security aspirants, how an exploit or attack looks, how it works, and how we can catch that exploit with the help of Intrusion Detection System.

Buffer Overflow exploit is one of the most common, severe and easily feasible attacks for the hackers to gain network resources. Here I would like to present the description of the attack; how it is causes the damage and what are the consequences of a successful buffer overflow attack. Buffer Overflow is mostly found in programming flaws. When a program is written, there would be some fixed memory space allocated for variables. If right amount of data is written into that memory space, it is fine. But, if there are more data writes into that memory space, the program does not know where to store the excessive amount of data. In analogous to everyday situation, but in a different manner, if we try to pour 2 liters of milk into 1 liter bottle, it will overflow. But, here the excessive data will be overwritten on the existing files. These files may be critical and it is hard to say, where the program causes it to overwritten.

Here I would like to present how buffer overflow exploit works by demonstrating with a C-programming code which runs in Linux environment to gain the root.

```
// This is buffer-overflow.c program
// Naga Raj Peddisetty.
 # include<stdio.h>
typedef char temp_buf[256];
FILE * file1;

void overflow_file()
{
   temp_buf mybuf;
  fgets(mybuf, 512, file1);
   puts(mybuf);
   }
int  main()
{
  file1 = fopen("overflow_file.txt","r");
  puts("overflow_file.txt has the following contents");
  overflow_file();
  fclose(file1);
  return 0;
}
```

The above C program when compiled on Linux, it does not give any debugging errors. Since a C compiler does not check for array bounds, the program is correct. Assume that myfile.txt file has 512 characters. But when we run the program, in addition to the desired output printed on the screen it also shows a "segmentation fault" message, since we tried to write 512 characters of file1 variable into 256 characters length of mybuf variable. Since memory is allocated for buf is 256, rest of the 256 characters will overflow to other memory segments and the existing data is overwritten. This will cause root program to crash, if some shell code is written to utilize this opportunity. Since it is a hot button and sensitive information, I do not want to disclose the shell code to crash the root here.

If we want to see what files root have, it can be viewed with this command find / -type f -perm -04000 -ls. This command will list out all the programs that root have.

Buffer overflow exploit is the most prevalent and serious attacks, since it can be easily written in C language. It is very common and it constitutes 70% of all the attacks. This will result in loss of important files, abnormal program executions, giving up root privileges, gaining the system, launching attacks from the victim host etc. By exploiting the buffer overflow, an Intruder utilizes this by executing his programs with aid of script for bad purposes. Now we shall see how an Intrusion Detection System can detect the attack.

There are two methods to detect this type of attack. If the attack is novel, the detection is through Anomaly detection method by determining if data transmissions are abnormal and out of specification, which is the indication of an attack.

If the Buffer-Overflow attack is discovered, publicized, and characterized, it can then be identified as an attack by a signature-based system. When an attack is characterized, the steps required to perpetrate the attack are described, there by creating an “attack pattern” and “signature” to detect that attack.

Chapter 3 Survey of the IDS products

In this chapter of survey we are presenting the nuts and bolts that constitute state-of-the-art commercial Intrusion Detection Products. It will be a review of several important and necessary features that describes each Intrusion detection product and its properties. These features give an overview of what an IDS has and has not. This survey also serves the purpose of comparing different products available in the commercial market. This chapter is the building block of the forth-coming chapters of IDS challenges and Evaluation Criteria for the reference of what a product constitutes of.

We have reviewed six different popular commercial products of which, four products are Network-Based and two are Host-Based. This selection of the products is random and to give the portfolio of each product. First, different kinds of components and aspects are presented and their significance is explained. Next we review whether a certain product has the specified component or aspect. Though hundreds of commercial products available in the market, for the time constraint we will list out the top six products only.

The procured information of the products based on the data sheets and product manuals. It is to be noted that certain feature that is not presented in either the product manual or data sheet, is considered as, the product cannot offer that feature.

The assessment of the products serves as a deployment guide by presenting and checking all the properties of the commercial Intrusion detection products. It can also be used to determine the state-of-the-art features of commercial products, what they lack, what the requirements to deploy are, and all the essential information about the mentioned commercial products.

3.1 Assessing the Products

First, we have selected six commercial Intrusion Detection Products randomly. Of these six products, four are network-based products and two are host-based products. These are mentioned below:

- **NetScreen IDP 500**– this is both Intrusion Detection and Prevention Network-based Product manufactured by Juniper Networks, [3.1].
- **NFR Sentivist v4.0**– this is Network-based Intrusion detection product manufactured by NFR security, Inc, [3.2].
- **Cisco IDS 4200** – this is network-based IDS and manufactured by Cisco, [3.3].
- **Secure Net** – this is a network-based IDS manufactured by the Intrusion, [3.4].
- **Tripwire** – this is a host based IDS product manufactured by Trip Wire, [3.5].
- **Intruder Alert** – this is a host- based product manufactured by Symantec, [3.6].

After the selection of this process, we have listed out the essential nuts and bolts of a general Intrusion Detection Product. We have given enough description of these properties, explained why these properties are important, and how it yields a better Intrusion Detection product.

This chapter, the survey of Intrusion Detection Products would stand as the second step for the buyers in the process of selection procedure. It gives whether particular products suits to their organizations or not, the environment the organization possess and the environment the product supports. This survey delivers the minimum requirements for the products before deploying. For example, if a product supports windows 2000 operating system, and the organization has UNIX environment, the product cannot even be considered at the early stage to deploy.

The next step after the description of essential features of the IDS products is checking all these properties in the selected products. We have listed out these answers in a tabular format by assigning the features in rows and the products in column format.

In the tables 'yes' means the attribute that we are checking in the product incorporates that attribute. 'No' means, that attribute is not incorporated in that product. 'NA' means that either information is not available or that attribute is not applicable. If any IDS differ from the mentioned features, it will be regarded, as "other" and that feature will be written in the table.

3.2 Properties of IDS

Here in this section, we list out all the properties of the general Intrusion Detection Product in a comprehensive manner. It is given in a classification form, for a better insight into what to look for in the products, why this particular feature is important and how it is relevant.

Kathleen A. Jackson at Los Alamos National Laboratory, with the support of the Global Security Analysis Laboratory at IBM's Zurich Research Laboratory, Switzerland, in 1999 has surveyed most of the commercial Intrusion Detection Products of that time [3.7]. In his comprehensive work, he has classified the properties of the Intrusion Detection Products into four major components mentioned below.

3.2.1 Characterization Component.

3.2.2 Technical Component.

3.2.3 Applicability Component.

3.2.4 Management Component.

3.2.1 Characterization

The Characterization Component can further classified into five components. The nature of IDS can be determined by following components that exists with an IDS product.

3.2.1.1 Deploying Strategy

The most two common forms of deploying IDS products are network-based or host-based. So the attributes for this aspect can be host-based or network-based or host and network-based. Some have both network-based and host-based features.

Network-based IDS products are important to monitor for all kinds of network attacks and web attacks from the outside of the internal network. For more theoretical knowledge on Network Based IDS products, please refer to Chapter2.

There has been ample information found in the chapter 2 on host based IDS. It can be found that Host-based systems are deployed on each computer in an internal network and they are good in detecting the insider threats. They are good in detecting the encrypted attacks also.

There is some kind of systems, which has both the network based and host based engines that make the hybrid system.

3.2.1.2 Detection Method

There are several different detection methods that can be found in the commercial state-of-the-art Intrusion Detection Products. For all the below mentioned detection methods, we have given enough technical description in the chapter2. Here we are going to see the importance of each detection method.

3.2.1.2.1 Stateful Pattern Recognition: Stateful pattern recognition offers slightly more sophisticated approach, since it takes the context of the established session into account, rather than a single packet. This approach makes IDS evasion much more difficult, though far from impossible.

2.1.2.2 Protocol Decode:

It is an important feature to be considered, because it minimises the chance for false positives if the protocol is well defined and enforced. Attributes are yes or no.

2.1.2.3 Heuristic Detection:

This type of signature may be used to look for very complex relationships.

2.1.2.4 Anomaly Detection

Anomaly approach is very important to detect the novel attacks. It is also good in detecting zero-day attacks.

2.1.2.5 Signature Based Detection

This is the most fundamental approach that should be considered in an IDS product in order to detect the known attacks and the known variants of the attacks.

3.2.1.3. Information source

There has been enough description on the Information sources of the IDS in the second chapter. The attributes for this aspect depend on where the IDS is located and what are its information sources, Network packets, operating system, application.

Network packets imply that, an IDS product is designed with a network sensor to monitor and process network packets and it process network protocols (e.g. TCP/IP, UDP, RTP).

Operating system means that, an IDS is designed to operate with at least one operating systems (e.g. Linux, Windows NT, UNIX).

Application means that the IDS product is designed with a feature that process the information from at least one specific application (e.g. firewalls, e-mail servers).

3.2.1.4 Timing

This aspect determines how frequent an IDS is analysing the captured information source. The attributes can be continuous (real-time) or batch mode.

In batch mode, the method of operation is static, means it analyses the audit data in store-and-forward fashion.

3.2.1.5 Response

There are two categories of Response Based IDS. They are Active response and passive response. For more information on response based IDS, refer Chapter 2.

Active Response based IDS is important to stop the progress of attack since in active response, the decision is taken immediately after processing of the audit data, if it has any suspicious behaviour or attack in it.

In passive response based IDS products, the testimonials of an attack are sent to an authorized person or system administrator to take the appropriate action. These kind of responses are mostly manual and important in dealing with most complex attacks.

3.2.2 Technical Aspects

This component is the kernel of Intrusion detection systems. The core functionality of managing, maintenance, and auditing deals in this component. There are several different technical aspects that have mentioned below. We have given a brief description on each aspect and the importance or the presence of each aspect is explained.

3.2.2.1 IDS Management

The attributes for this aspect can be any console, central console and others.

If the attribute is 'any console', it implies it is capable of managing the analysed data from any sensor or host. E.g., an user by logging into the console as root can manage the IDS functionality from any console in the network. This feature is very important in big enterprises and distributed networks.

If it is 'central console', the IDS can be managed from a specific central console only. It would be important in small organizations.

3.2.2.2 Management Capacity:

Management capacity aspect determines the capacity of an IDS management that how many sensors or hosts that it can manage and afford efficiently. This aspect can be useful in comparing an organisation capacity and the IDS product's capability. E.g., If an IDS can manage 100 sensors in a network, if an organization needs 500 sensors for the monitoring, this IDS is not suitable for that organization.

We list out how many agents/sensors that an IDS can support for this aspect.

3.2.2.3 Customization aspects:

Generally customization refers to the capability of the system administrator to configure the intrusion detection product apart from the manufacturing features. This feature would help a lot to the IDS management. When there are new attacks, instead of waiting for the manufacturers, the IDS management can easily thwart the attacks. In order to reduce false positives and false negatives, an IDS system must be fine tuned to the organizational particular needs. Mostly IDS systems are designed in general; they are not designed to a particular enterprise or an organization. So, this customization feature plays a vital role in tuning of the IDS product, which allows editing the features according to our priority and flexibility. This in turn can enhance the productivity and the ease of management. We have listed out possible features that can be customized.

Intrusion Patterns or Signatures:

This feature is useful in determining whether an IDS has the possibility of adding new patterns of attacks and misuse apart from the vendor supplied database. As new attacks are increasing everyday in both complexity and volume, there is a need for the updating and development of new attacks all the time. As hackers always try to penetrate with new kinds of attacks, this feature is very useful for the development of new intrusion patterns.

Network Protocols:

It means that apart from vendor supplied default network protocols, whether an IDS provides user configurable protocols or not. Generally vendor supplies some limited number of default protocols. If an IDS has this feature, it enables the IDS management to add, edit and modify to the existed protocols.

Response:

This feature derives whether the IDS allows editing the existed responses. It means that with this customization aspect, the IDS management can add some new kind of responses for an attack; they can delete some unnecessary responses.

Audit Record:

This feature is especially useful for host-based IDS where an IDS enabled with this feature can add some additional data for auditing.

Reports:

For every IDS, a vendor supplies some default set of reports, like text, html. It would be of great useful, if there is a provision for adding new kinds of reports. If an analysis management requires additional information about an attack, then with this feature provided, a user can report the extra details required.

Cryptography and security options:

It means that in addition to vendor supplied default set of cryptographic protocols, the IDS provides a user-configurable set of cryptographic protocols and security mechanisms. E.g., if the IDS provide DES protocol, as this protocol is obsolete and vulnerable to attacks, with this feature a user can configure the IDS with AES, which is an advanced and stronger.

3.2.2.4 Security

An IDS which is securing enterprises, first of all must secure itself from attackers. Hackers aim at compromising the enterprise resources, first tries to get rid of the barriers on the way. So self-security of Intrusion Detection products and its communication is very important. There are different kinds of places where security is needed in IDS environment. The possible aspects for security feature can be monitoring technique and Communication Security.

Monitoring Technique

There are two ways, generally an IDS monitors one is stealth mode and another is exposed with self-secure mode. Stealth mode monitoring means an IDS monitors the traffic in invisible mode. The possibility of attacking an IDS in this mode is very less.

In exposed mode with self-security mode, it is visible for anybody and it has some kind of protection mechanism for attacks on its own. Attributes for this aspect can be exposed mode and stealth mode.

Communication Security

This feature ensures the security of the communications in an IDS system, like Logging onto the management console, communication between agent and management console, communication between management console and analyzer. For example, an agent, which detects malicious code to communicate with the management console, it must either encrypt it or sign with a digital signature. Lack of protection mechanisms in the communication of IDS systems may results into social engineering (man-in-the-middle attack). It could also be possible for malfunctioning of the data.

3.2.2.5 Interoperability

Interoperability allows an IDS system to integrate with other network and security tools like Vulnerability Scanners, File Integrity Checkers, Honey pots, Firewalls and IPS. Since IDS alone is not a complete security solution, integrating with other tools is very necessary. Aspects of this feature are Common Management, Security tools.

Common Management

An IDS working along with other products like scanners, honey pots should have the capability of single management. If different products produce different kinds of results, it is hard to manage individually. Common Management can reduce the management burden by managing both the IDS and the other tools together. Attributes for this aspect can be component, compatible interface, and none.

Component means the IDS and the supporting security tools work as a single package.
Compatible interface means the supporting product works as an individual system, but it can be managed through a compatible interface. None means IDS product is not interoperable with any product

Supporting Tools

This feature determines, what are the supporting tools that an IDS can be interoperable. Here we list out the supporting tools like firewall, VA systems, etc.

3.2.2.6 Event Management

This aspect is very useful for the analysis of event data. Managing the events in a systematic and proper way leads to a better analysis and response of events.

Event prioritization:
Most of the events generated in IDS are of minor importance. As the events are generated in hundreds, responding to all the events is difficult and it wastes lot of time. It may also lead to the ignorance of important and critical attacks. So, event prioritization optimizes the response time by flagging and distinguishing the events. It yields fruitful results in responding to the events.

Full event information:
Full event information means that when an event is detected it should record all the information that may be useful in the analysis and response phase. E.g., IP address of the event source, time, date, Destination IP address etc. It is more useful in Forensic Analysis.

Event Merging:
Generally an IDS produces large number of events upon monitoring the source data. There would be lot of unimportant events, which can be ignored. Some events need to be examined. Instead of generating an alarm for every event, similar kinds of attacks can be grouped to generate a final attack. It is useful in reducing the event volume.

Additional Attack Information:
It means that an IDS system provides the additional information after the detection of an attack. This would be a brief description on the attack, the information needed to understand the context of the attack; its severity and what caused it. It also provides the recommendations to avoid such attacks and possible countermeasures for responding.

Automatic Signature Updating
Generally signature databases should be upgraded periodically with new attacks. This feature is very important for IDS with Signature based detection method.

Way of Signature updating
It gives the way of signature updating. Possible values for this feature can be ‘Web’, ‘Third party tools’ and ‘CLI’.

3.2.2.7 Response Options

Active Response Options
It is mentioned in chapter 2 that, ideal IDS should take the actions instantly with the occurrence of attacks. There are different kinds of active responses an IDS can take. They are router/firewall re-configuration, session hijacking, IP address blocking, terminating the session.

Router/Firewall reconfiguration means that an IDS can immediately reconfigure the network elements like routers, firewalls, and switches. Session Hijacking means that an IDS can seize the connection of any user on the network.

Other Response Options
IP session logging: This feature enables to store all the IP related information when an IDS detects vicious traffic.

3.2.2.8 Implementation

This feature derives the form of an IDS implementation. It determines how the IDS is implemented to suit the organisations environment. The attributes can be S/W (software), H/W (hardware), Both (means software and hardware).

3.2.2.9 Customer Support

For any IDS, a vendor provided customer support is important. For the deployment, training employees, for the upgrading of signatures, to fix the vulnerabilities, support plays a crucial role. Any good IDS, with a poor customer support fails in the market. There are different kinds of aspects like product knowledge, response of the vendor falls into this category. Attributes for both of the aspects are high, medium, poor.

Product Information:
Product information gives the detailed knowledge about the product for the customer. This aspect determines how the user is getting information through the vendor provided website, how easy it is to navigate for the support. It also gives the deployment, assessment and managing information regarding the IDS. High means that the product information is easily available and complete information is available. Medium means that the full information is not available; vendor should be contacted somehow for help. Poor means that the information about the product is not at all available.

Response of the vendor
This feature determines the concern and promptness of the vendor. It is based on how quick the vendor is in providing the necessary information regarding configuration, vulnerability patches and signature updating. The attributes are high, medium and poor. High means that response of the vendor is very quick. Medium means that response is ok, with bit delay, poor means that response of the vendor is zero and vendor is not providing any kind of help.

24x7 Hotline
It means that vendor is providing the customer support all the time with out any time constraints.

3.2.2.10 Forensic Analysis

A concise demonstration has been given on Forensic Analysis, in the previous chapter. It was observed that Forensic Analysis is very important to take action against the attackers through legally and it has several other benefits as well.

3.2.2.11 Scalability

Sometimes there will be a need for increase in sensors in organisations in order to extend the monitoring of IDS and expansion of the existing networks. If an IDS is scalable with out any need for new IDS systems, it would be considered as the most important feature for the growing organisations. This feature derives how an IDS scales with increase in sensors

3.2.2.12 Attack Landscape

The primary goal of Intrusion detection is detecting the malicious traffic. There are several types of attacks that an IDS has to detect in the attack landscape. Here we are checking for the protection of the most important attacks by an IDS. All these attacks have been mentioned below.

- Sweeps or floods.
- DoS or DDoS
- Worms or viruses
- Common gateway or WWW attacks
- Buffer overflow protection
- IP fragmentation attacks
- ICMP, SMTP, POP attacks
- FTP, SSH, Telnet attacks
- TCP hijacks
- Other Attacks

3.2.2.13 Attack Notification

Intrusion detection systems alert the administrators with different kinds of notification options according to the flexibility. There are several attack notification options as listed below that an IDS can allow.

They are 'Alarm Display', 'E-mail, E-page alerts', 'script execution', 'third party tool integration', and 'Alarm Summarization'.

3.2.2.14 Administration

This feature reveals the mode of IDS administration. This can be through 'web user interface', 'Command Line Interface (CLI)', 'Remote Management'.

3.2.2.15 Reporting

Report Merging:

When an IDS collects large number of reports from different systems, the merging of reports allows a sensible way for a better visualization and effective presentation to the management. This feature allows a tangible perception of the Reports. For example, if an IDS along with a vulnerability scanner has data of both tools, it should be an efficient job to present the data merged. Without merging, the output data would be complex and it makes hard to understand, what went wrong and leads to false decisions.

Report Format

This feature determines the kind of interface that an IDS has for the presentation of reports to the IDS management. Possible attributes would be graphical user interface, customizable interface, text, HTML, XML based reports.

Interface

It gives the mode of Interface that is used in presenting the reports.

Archiving
Archiving of Reports enables the IDS to store the reports for future use.

3.2.3 Applicability

This section deals with the IDS product's ability to interpret the local environment's information including Operating Systems, Network Protocols, Applications supported and Networking Features.

3.2.3.1 Operating Systems

Client OS : Most of the Intrusion detection system products are designed to specific operating systems. It works with only that particular OS, some work with any OS. This aspect determines the target OS an IDS built. E.g., Linux, Windows versions, Unix, Macintosh etc.

Server OS: This determines what the server, the IDS system is designed with.
Sensor OS: This gives what operating System the sensor supports.

3.2.3.2 Target Applications

This feature determines the target applications for which an IDS is designed. For example some IDSs are designed for servers and some are for application servers, and some are for databases. We list out all the applications that an IDS supports.

3.2.3.3 Network Speed

This aspect gives the speed of the networks that an IDS can support. Some IDSs are designed for low speeds like 100 Mbps and some are designed for 500 Mbps.

3.2.3.4 Network Topology

There are different kinds of topologies like ring, mesh, LAN. This feature gives the network topology that an IDS is designed and supports.

3.2.3.5 Network Protocols

Different kinds of network protocols exist. This feature gives what network protocols that the IDS can monitor.

3.2.3.6 Additional features

This feature determines the extra capabilities of the IDS, apart from the original functionality. Apart from the normal functionality of detecting and monitoring of target application some IDSs detects and monitors other kinds of applications. We list out those features here.

3.2.4 Attainment

This is the final step in the IDS survey to derive how good an IDS product performs in a real-world environment, how it withstands to the real-world system failures, how well its functionality works in crucial situations, and how it meets the expectations from their advertised information. We just present these issues here, since to answer these properties it needs a real-evaluation of the products, which is not possible at this moment.

3.2.4.1 Performance

It determines the ability of IDS product to analyse the information source effectively, accurately, and in real-time. It should perform up to the expectations.

3.2.4.2 Robustness

It determines how well an IDS weathers to the system failures like power failure, crashes, etc. It gives the ability of an IDS to recover from system failures.

3.2.4.3 Accuracy

Accuracy determines how many false positives and false negatives it is producing, how accurate it is in terms of attack detection rate, signature updating, and the ability in monitoring the events.

3.2.4.4 Ease of Use

This feature determines how easy it is to operate an IDS system. It addresses issues like technical expertise needed to install the IDS, configuring the security policies, developing new signatures, modifying attack definitions etc.

Chapter 4 IDS Challenges

"Crying wolf: False alarms hide attacks;
Eight IDSs fail to impress during month long test on a production network".
- By Network World Fusion e-magazine. [4.1]
"Intrusion Detection Systems are dead; they are market failure. They cannot provide the ROI. They will be obsolete by 2005"
- By Gartner Research Report, Information Security Hype Cycle. [4.2].

How far these comments are true? It has become common to see this kind of quotes during these days. We have mentioned in our technical description of Intrusion detection systems in chapter2, there are several advantages and disadvantages of Intrusion Detection Methods. It has also been mentioned that IDS is not a complete security solution. We here discover and present the limitations more elaborately to give the true picture of IDS challenges.

Intrusion Detection Systems have been emerged during 1990s. Since then there were extensive research efforts made and enormous amount of money has been spent. But still the technology is immature. There are several aspects that have not been focused on research. We here present some of the future research aspects that should be focus on.

Despite the significant advancements in Intrusion Detection Research, the state-of-the-art commercial Intrusion Detection Products are sustaining up to the Research Results. We will present here the obstacles that are impeding the progress of Intrusion Detection and the state-of-the-art challenges faced by the Intrusion Detection Products. This chapter has been written to address the IDS challenges more elaborately and to inspire research people to resolve these challenges in order to make IDS products mature and complete.

This chapter gives the snap shot of the present commercial product's challenges and limitations. Regardless of rumours and paranoia, we here present the true challenges and problems, and we discuss how these challenges are limiting the performance of IDS. With this knowledge a buyer can have the real expectations from the IDS and he can also decide upon what are the organizational requirements and what the products can truly offer.

We will present some of the modern challenges like zero-day attacks, Encrypted Traffic, Data Collection and Correlation, and IPv6. We will discuss problems with the Evasive attacks like IP fragmentation attacks, TCP Reassembly attacks, Denial-of-service attacks. It has also been discussed about the performance challenges of IDS like High Speeds, False Alarms.

4.1 Zero-day attacks

From the observation there are two different definitions can be defined for the zero day attacks. In one definition, it can be defined as any exploit that is written for a previously unknown vulnerability. In other definition, it is new or undocumented attack for which a signature or definition has not been written. Zero day attacks exploit a known vulnerability with a new pattern of exploit (e.g., Code Red and its later version Code Red 2). The Zero day vulnerabilities are flaws in software that no one knows except the attacker.

According to commercial IDS manufacturers like Symantec the attack in between the time gap of published or known vulnerability and applied patch is called as Zero-day attack [4.3]. An important point here is when vulnerability is published to the public, everybody comes to know about it, but it is not unknown to the manufacturer. It is very hard to get it patched with in a short time but it is very easy to write the exploiting code with the known vulnerability. Since organizations take significant time to release and apply the patch for vulnerabilities, Attackers take this to their advantage and can cause much damage in between this time gap.

Zero-day attacks cause more damage to the signature based IDS tools compared to that of Anomaly based detectors. Since signatures would not be available at the time of zero-day attack detections, signature based IDSs can be easily circumvented.

According to the IT managers at InfoSec2003 in New York, zero-day attack is viewed as a major threat to data security [4.4]. They have also stressed the importance of having well-developed patching and incident-response capabilities to reduce the massacre that the attack can cause.

If zero-day attack is on the encrypted side of transmission it becomes more difficult to find out. Preventing the infrastructures from the zero-day attacks without affecting the normal legitimate traffic is another problem for IDS systems.

The chief technology officer of Redwood shores, Qualys Inc., Gerhard Eschelbeck explains the problem by his research as "Laws of Vulnerabilities" research [4.5]. In his illustration, the present life of vulnerability, the time taken by users to get patch half their systems after a vulnerability announcement is made, is 21 days for external systems and 62 days for internal ones.

In summer 2001, Code Red worm hit vulnerable systems running Microsoft's IIS software; the patch was released after 30 days, which has wreaked havoc. From ICSA Labs survey it is revealed that average cost to recover from the zero-day attacks rose from $69,000 in 2001 to $81,000.

As the amount of attacks is surging, and the time gap between vulnerability announcement and exploit is decreasing, combating against zero-day attacks is the state-of-the-art challenge for the IDS organizations despite the limitations of the detection methods.

4.2 Data Collection and Correlation

Now-a-days Network Security now is practiced as defence-in depth or layered approach, which allows security to divide into layers and protecting all the layers collectively. This approach introduced a new challenge for the intrusion detection technology; that is Data Collection and Correlation. In the layered approach of Network Security, security tools in each layer plays important role. All these tools have their strengths and weaknesses, in terms of providing security information for the collective analysis. For example, Operating systems provide only system logs; they cannot provide any information about the network traffic passing through the perimeter. In order to have collective analysis of the malicious events, there is a need for more information from all the layers of Network security.

Data Collection is the process of collecting security related information from different proprietary security products in a network perimeter. As different vendors manufacture all these products and they use different formats of data, there is lot of risk associated with the collection of the data. This process includes the collection of System Logs (port requests, port map messages, login messages, kernel messages, Daemon messages), online statistics and events about the usage of the system and the behaviour of the network connectivity, system last record (user connection and disconnected time, after authentication), from the Operating System, CGI script access attempts, monitoring information from Intrusion detection products, ACL information from the router, Firewall logs etc Products.

Data Correlation can be defined as the process of analysing different security related information sources by matching similar patterns in an event. This in turn gives more evidence of an attack and can reduce false positives. Data Correlation process reviews all the information collectively and provides a more complete and comprehensive picture of the incident. It also assists in forensic analysis of the attack and allows taking more appropriate response for the attack.

The following example gives a better insight into the importance and details of Data Collection and Correlation. We assume a model network consists of Router, Firewall, NIDS and Application server. All these products provide the following kind of information:

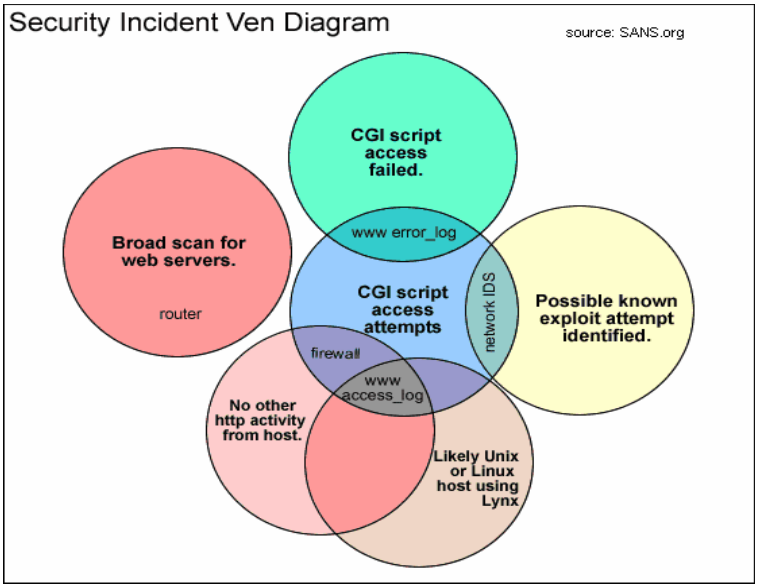
Firewall: Firewalls provide extensive logging and access control capabilities that allows visibility into network traffic passing through the network perimeter. In general firewalls gives the information about which ports are open, which ports are closed. But, we cannot determine whether an event is successful or not, just by saying an event was allowed.

Router: Routers are the first line of protection in Network security. They provide the ACLs(Access Control Lists), which determines who is allowed to access the network elements. They also assist in packet filtering with syslog type of alerts, and produce logs if they encounter any kind of reconnaissance attacks. So, they provide a certain IP address that probed the web servers, but they do not assist in giving any information regarding the objective of the attacker’s action.

NIDS: These products monitor the network traffic passing through, and generate alerts if there is any malicious or un-authorised traffic. Since NIDS can produce lot of false positives, there is a room for ignorance of some attacks, so there is a need for more information to be analysed whether an attack is a serious one or not. Still we cannot confirm whether the event is successful or not by just seeing malicious traffic. So, if we correlate the information from NIDS with other network products, there would be a scope for efficient analysis.

Application Servers: Web servers, E-mail servers, ftp servers etc provide the whole information involved with in an organization. These are the primary targets for any attackers. These servers log the data about all the transactions involved in the operation with them. They provide reasonable visibility into what had happened and the objective of an attacker. The access-logs in these servers reveal the attempts for their resources, and the error-logs reveal that the attack is successful or not.

In summary, from the above illustration each network security product provides limited amount of necessary information required for Intrusion analysis. So, the analysis of individual product's information will not be adequate and would not result in fruitful results. But, if the information from all the products collectively analyzed it can determine genuineness of the events and allows procuring enough evidence against an event.


Security Incident Ven Diagram
source: SANS.org
CGI script access failed.
www error_log
Broad scan for web servers.
router
CGI script access attempts
network IDS
Possible known exploit attempt identified.
firewall
www access_log
No other http activity from host.
Likely Unix or Linux host using Lynx

In the above diagram from Sans Institute [4.6], it can be observed that neglecting the data from even one-circle (security tool) results in a dramatic shrinkage of evidence collection about an attack. So it implies that each proprietary security tool contributes to the broad range of information collection for an attack.

We have seen how important it is to collect information from each security tool. We shall see here why it is difficult in Intrusion Detection.

1. In network security perimeter, it consists of different proprietary security products. They do not support information sharing standards between them. Each product uses it's own information structure. Formats of windows operating systems, SYSLOG, SNMP all

are different. So, this process of collecting information requires manual expertise.

2. The volume of the event data is huge. Collecting data from all the network products like servers, routers, firewalls, vulnerability scanners, IDS generates huge amount of traffic. It is impossible for a human being to analyse all the traffic.

3. Data is located at different places like local systems, some are located at distant servers and some are stored at network elements.

4. Disparate Event IDs also pose the problem in correlation. For example, an event ID in UNIX means something different in Windows.

Due to all these above-mentioned problems, data collection and correlation would be pretty difficult. Albeit there are efforts to develop standard information sharing processes for IDS data, like IDMEF and CIDF working groups, these efforts have gained little support, since each IDS manufacturer maintains commercial advantage by preventing other products from using their information. So, the correlation process still needs the human administrator to analyze and it is still a soon resolving issue.

4.3 Encrypted traffic:

"The biggest inhibitor to network IDS growth has always been Encryption. Commercial Web servers encrypt session traffic over SSL connections, effectively blinding network IDS sensors from finding hacker attacks on the wire." Stuart McClure, CTO, Found stone [4.7]

Encryption ensures the confidentiality of the data. Communications between servers and clients, e-commerce applications and any secure required communications use mostly encryption for their transmission of data. The example protocols are Secure Socket Layer (SSL), SSH, HTTPS, VPN, IPSec. Normally encryption process works as encrypting with one key at the sender and by decrypting with another key at the receiver. To decrypt the transmitted data, destination's private key is needed, which is hard to get for the third parties.

This makes the eavesdropper difficult to attack the transmitted data. If the traffic is intercepted, it doesn’t ensure the confidentiality, which makes encryption useless. If we look back to the fundamentals, an Intrusion Detection must intercept the traffic and analyze it, which is quite contrary to Encrypted traffic principles. Network Based Intrusion detection systems suffers much from the encrypted traffic, since they need more CPU power, high-profile attack target and interception of the attack.

The problem becomes worse, if a web server has two roots for both encrypted and non-encrypted websites. The attacker can connect through the encrypted version of the connection, by passing the NIDS in place without giving his credentials, and then he can use the non-encrypted version of the connection for attacking.

Growing popularity of VPNs, which use dedicated, encrypted and private connections also add to the problem of encrypted traffic. VPNs allow using private tunnels for their communication, which would be very difficult to intercept in between, and making the NIDS blind. VPNs also allow users to connect from anywhere like net cafes, public networks through tunnels to the host, which results in easy escape from being caught.

By Blinding the NIDS using encryption, attackers will successfully gain the access and control the system and critical resources with out anybody's knowledge. This makes the theory of NIDS, " an NIDS has to process each packet of the transmission as to detect and raise an alarm when an attack occurs", useless and results in attacks like SQL injection, Buffer Overflow, Unicode attack.

The increasing length of Encryption algorithms like DES, AES, RSA also adds another problem. For example, public key uses 1024 bit key, which is very slow to compute and needs lot of computation resources. Decrypting the encrypted traffic with enough resources and maintaining the throughput is one of the challenges at the forefront of the Intrusion detection research.

In fact, according to Gartner, by 2008, nearly all-trading communities will use SSL to meet diverse trading-partner requirements; Encryption will remain the bane of network-based intrusion detection technologies.

Though some of the state-of-the-art products boast of processing the encrypted traffic, there is no product that is offering the true ability to process the encrypted traffic accordingly with higher speeds. So, Increasing amount of encrypted traffic and increasing lengths of encryption algorithms remains as a challenge for the Intrusion Detection products

4.4 IPv6

In the early 1990s, the IETF (Internet Engineering Task Force) began an effort to develop the next generation of IP protocol. The prime motivator for this effort was the realization that the use of 32-bit address space will be saturated and used up, as new networks and nodes are being attached to the Internet at a brisk pace.

Here are some of the differences between IPv6 and IPv4.
1. IPv6 uses 128-bit addresses where as IPv4 uses 32-bit addresses.
2. IPv6 uses Class less Intra Domain Routing where as IPv4 uses class full.
3. IPv6 has Extensible Headers for more encryption and security features; IPv4 doesn't provide authentication and encryption.
4. No need of ARP, IGMP and RARP in IPv6. IPv4 uses IGMP, ARP and RARP.
5. The header format is simplistic in IPv6, where as IPv4 uses complex format.

Here are some of the advantages that IPv6 provide
IPv6 doesn't allow for fragmentation and reassembly at routers en-route, since the sender and receiver can perform these operations. As Fragmentation and reassembly poses extra burden on routers, this feature enhances the performance of the packet forwarding. It can also prevent systems from fragmentation and reassembly attacks.

The transport layers for example, TCP, SCTP and UDP and data link layer protocols (e.g., Ethernet) in the Internet layers perform check-sum operation. These checksums are placed in the IP packet. It implies that as the IP packets traverse through routers, checksum should be calculated for each fragmentation and Reassembly. As IPv6 doesn't allow the fragmentation and reassembly at intermediate routers, this feature will also be an important consideration.

IPv6 uses 128 bit addresses, which ensures that the world would not run out of IP addresses. Then, each particle on the planet can be allocated with an IP address. It helps the concept of Ubiquitous networking, a larger address space that is a motivation to connect everything to the Internet.

All these above mentioned advantages foster an impression that switching to IPv6 is inevitable. Either today or tomorrow, the world must switch to IPv6 from IPv4. Here I am going to present some of the hurdles that are preventing the research results of IPv6 world from successful deployment and operation.

The foremost problem with IPv6 is deploying. As the present Internet world using IPv4, transition to IPv6 is a cumber some task. While IPv6 can be made backward compatible that is, it can send, route, and receive IPv4 data grams, the widely deployed IPv4 enabled systems are not capable of handling IPv6 data grams. Though there are several options possible, like dual-stack approach, tunnelling, header translation, it is enormously difficult to change network layer protocols.

One more problem with IPv6 is with the simplified header format. IPv6 uses very simplistic header and it improves the performance of CPU, because it doesn't allow the fragmentation process during intermediate routers and it uses extension headers. So, no assembling of packets needed, which is efficient on old processors also. Since the extension headers are subjected to fragmentation, it may be possible for incorrect reassembly, which means that fragmentation attacks developed for IPv4 stacks can still pose a threat [4.8].

The Large address space also contributes to the stack of challenges faced by the IDS products with IPv6. It is defined above that ubiquitous networking results in numerous number of IP nodes in the Internet. To connect to the Internet, all these IP nodes run on some kind of operating system with TCP/IP enabled. If there is any security flaw in the operating system or with software running in this IP node, it is very unlikely to apply patch for each and every simple systems.

We have mentioned the problem with the encrypted traffic for IDS systems in section 4.3. The use of IPv6 makes further complications to IDS systems with their embedded encryption and authentication mechanisms.

Another problem with using IPv6 in IDS systems is Tunneling. Tunneling defined as private dedicated and encrypted connection using encapsulation (placing one packet in another packet). Lance Spitzner at his honetnet project wrote in his mailing list, in 1992 one of Honey net project's Solaris Honeynet was compromised. After breaking into the system, the attackers enabled IPv6 tunnelling on the system, with communications being forwarded to another country. The attack and communications were captured using Snort, however the data could not be decoded due to the IPv6 tunnelling, which blinds the capacity of IDS systems [4.9].

In final words, IPv6 has lot of useful, advanced features, which would be a great complement to the Internet. The capabilities of IPv6 make it use inevitable. But there is lot of problems to convert existing IPv4 protocol enabled networks into IPv6 networks. It still has some problems to overcome to deploy and using it in a smart and right way. So, the successful deployment and management of IPv6 is one aspect that poses a big challenge for the IDS products.

4.5 IP Fragmentation Attack or Insertion Attack

The growths of the Internet traffic at ever increase pace and more secure mechanisms influencing the attackers to discover novel attacks. An IP Fragmentation attack is also one of these kinds of attack to evade the network based intrusion detection system. The link layer protocols cannot carry packets of the same size. For example, Ethernet packets can carry no more than 1,500 bytes of data; where as packets for many wide-area links can carry no more than 576 bytes. Because each IP datagram is encapsulated within the link layer packet for transport from one router to the next router, the maximum transfer unit of the link layer places a limit on the size of the IP datagram. So, to solve this problem, an IP packet must be divided into pieces called fragments.

The primary problem with fragmentation is, it generates an extra amount of traffic in between the sender and receiver on the network. It causes the CPU to perform excessively for fragmentation. The process of assembling the fragments at the end host is called Reassembling. If every end host reassembles the fragments in the intended right sequence it is well and good. But if an end host cannot reassemble the fragments for fragments that arrive out of order, the problem of IP fragmentation attack will occur. Due to the routers placed en-route to the destination, the fragments travel through different shortest paths. So, some fragments reach the destination out of intended order. Some packets may arrive lately; some may never reach the destination. The attackers exploit this vulnerability of fragmentation, by sending fragmented packets that never reach the IDS system. As the end host allocates more resources, it will run out of memory, because the fragmented packets never completed. Another problem is, misconception that the IDS not reassembling the fragments until it gets all the fragments. One more misconception is, when IDS starts to reassemble packets as soon as it gets the last fragment. All these mistakes lead an attacker to successfully elude the IDS system in place.

It is evident that stateful IDS systems reassemble fragmented packets perfectly, but when the throughput increases, this consumes more CPU power and more resources and becomes less accurate.

For example, Ken and Gandalf published a new kind of fragmentation attack in BugTraq [4.10]. The attack was named Rose Fragmentation Attack; this attack is a combination of the SYN attack and the unknown ICMP attack. In this attack they have observed that it is possible to spoof the source address and source port as the packet would not travel up above the stack and can escape from being examined.

This attacks works, by first sending few bytes of a fragmented packet at offset 0(more fragments bit = 1) and then sending a few bytes at the end of a 64k sized packet (more fragments bit = 0). It was also derived that, if a packet is sent with random source IP address and port, tracing back to the source address is only through hop-by-hop method. Since the packet will not reach up the stack, the stack does not validate the packet, even if the receiver's port is a genuine. The attackers exploit this vulnerability by, sending lot of fragments like this to the destination. Since the IDS at the receiver end waits for the rest of the fragments to arrive, it fills with the buffer space, and genuine traffic will not enter the buffer.

The effects with this kind of attack are consumption of more CPU power, inability to process the genuine traffic, and difficulty of tracing back to the source.

It is evident that a stateful IDS system reassembles fragmented packets perfectly, but when the throughput increases, this consumes more CPU power and more resources and becomes less accurate.

So, it may be concluded that though some IDS tools are providing security against Fragmentation attacks, providing the perfect security against these kinds of attacks is still a challenge to the IDS research.

4.6 Evasion Attack or TCP Reassembly Attack

An End system can accept a packet that an IDS rejects. This paves the way to the noxious user by hiding the critical information from IDS monitoring. According to Thomas H. Ptacek and Timothy N. Newsham at Securenetworks, Inc, these are called Evasion attacks and they are the easiest to exploit and most devastating to the accuracy of IDS [4.11].

TCP stream reassembly is best example for Evasion attacks. TCP packets reassembly is one of the most difficult task for a network based IDS. The perfect reconstruction of the fragmented packets in the transmission, for IDS poses significant risk and can be termed as an important challenge.

General problems for the reassembly is reconstructing the packets that arrive out of order and proper tracking of the TCP sequence numbers of a connection. Since IDS cannot have the facility of requesting for retransmission for the packets that it misses, IDS has to reassemble packets accurately. The inconsistent timings between the IDS and the end-system are also another risk.

4.7 Denial-of-Service Attack

Denial-of-Service attacks are the most common and easily launch able attack like buffer-overflow. By definition, it is the process of refusal by a server, for its services, to its legitimate clients. This happens when attackers launch the denial-of-service attack on the servers to either crash them or occupying their whole capacity. In this attack, the main goal for attackers is to make the available services of the servers, unavailable to clients.

DoS attack can be launched by script kiddies who wants to show their excellence to their class-mates, Business competitors who wants to bring down the reputation, serious attackers who are furious with the victim and un-satisfied customers who are frustrated with business policy and services.

Generally DoS attack can be launched through different methods.
They are 1. TCP/SYN Flooding.
2. ICMP flooding.
3. UDP Port.
4. RPC flaws.

4.7.1 TCP/SYN flooding

Generally, In the Internet, connection between two hosts is established using the TCP handshake protocol. The establishment of the TCP connection requires the exchange of three packets in an interchangeable fashion by the two hosts. To explain lucidly, it works like below.

1. If we assume it in a Client-Server fashion, first client sends its SYN packet to the server to request a connection. This packet contains the port numbers of source and destination, and IP addresses of source and destination. The server receives SYN packets at its open ports, which are fixed in number.

2. The server will be ready to accept the connection and it will send its own SYN packet and ACK packet to the client. The Destination IP address and port will be the same as the source IP address and port of the SYN packet received from the client. An Important point here is the server waits for the ACK packet from the client to establish the connection.

3. The Client receives the server's SYN+ACK packet and it confirms that the server is available and there exits a path in between. In order for the connection establishment the Client sends an ACK packet to the server. Now the connection is established between client and server.

Now we will see how this TCP handshake protocol leads to the Denial-of-Service attack:

The server stores the information of the client regarding the IP address, port address etc when the client initiates the server as in step 1 from the above illustration. It also allocates some buffer space for the bi-directional transmission of data. From the step 2 of the diagram, it is also evident that the server waits till it receives the acknowledgement from the client for its SYN+ACK packet.

Attackers take this feature “the server waits” for their advantage. They spoof the source IP address by some valid or random IP address and send the connection request to the server. Since the server does not know this is from malicious users, it treats the request SYN packet as usual and it will send the SYN+ACK packet. The server reserves its resources and also waits till it gets ACK from the Requestor (Attacker).

When the server sends SYN+ACK packet to the source address of the Client, it will face problems. If there is no valid IP address, the packet will be discarded. But at the same time, server waits for the ACK, where there is nothing to send ACK. This obviously wastes the resources of the server. Since the server does not know that the client is malicious, it waits for some random time and resends the SYN+ACK packet. At this stage the connection is still pending. The client sends many number of SYN packets like this to occupy the total number of open connections that the server possesses.

For example, a web server has 50 open ports available for the connection initiation, if an attacker/client sends 50 SYN packets with fraudulent IP address, the server is fully allocates its all open ports to the client/attacker. So the legitimate/genuine user when tries to establish the connection with the server, it is unable to establish connection and its request will be denied. The server cannot offer any of its services further. This is the whole story to launch a Denial-of-Service attack on the web servers, e-mail servers, application servers, database servers etc through the TCP/SYN flooding method.

This method also results the innocent users to be victims, if their IP address is spoofed.

4.7.2 UDP Port

This method of DoS attack occurs when a connection is established between two UDP services, each of which produces output; these two services can produce a very high number of packets that can lead to a denial of service.

4.7.3 ICMP flooding

In this method the client/attacker broadcast an ICMP echo request with the source address as the destination/victim address. So all the hosts on the broadcast network reply to the ICMP echo request with ICMP echo reply to the source address of the sender, which is obviously the DoS victim. This overloads the DoS target and the target will crash.

4.7.4 RPC flaws

This method of DoS attack takes the advantage of inherent flaws in the RPC protocol. When attackers identify the vulnerabilities in RPC protocol they send specially crafted packets to the vulnerable machine to crash. This can turn into denial-of-service attack.

For example, On Nov12, 2004, the Dutch police arrested two teenagers in Netherlands. They have flooded the government websites to crash them. Their intentions were to protest against the government's social security policy. Since DoS attacks have the ability to bring down business, it is very important to detect them before they occur.

4.8 Distributed Denial-of-Service Attack

This form of Denial-of-Service attacks is different from DoS in both the functionality and size. DDoS causes collateral damage to the victim. The DoS attack is one to one target oriented; where as DDoS joins numerous numbers of intermediate hosts and the attack is indirect. Here is how it works.

We call the real attacker as Master attacker, and the intermediate hosts as agents. First, the Master attacker scans for the vulnerable, insecure computers using the loopholes in protocols and operating systems that are connected to the Internet. Then Master attacker installs the DDoS software that will be used for the real attack in the agents.

The Master attacker stores all the information about all these intermediate agents and he also take over the administrator or root privileges. The master attacker does not give any clue for the agent host owner that the agent is compromised. Also, the master attacker does not cause any harm to the agent.

Now, the master attacker waits for the time to launch the main attack on the victim. Since he has the administrator or root privileges, he will launch the attack from all these agents, which overwhelms the victim.

The most dangerous part of this attack is when master attacker tries to join numerous numbers of agents in a cycle fashion. This makes tracing of the master attacker very difficult and huge damage to the victim.

An Important problem with this kind of attack is, it is hard to find out the source IP address of the real attacker. It can be possible to find out the agents but if they are numerous, tracing back is difficult. The attractive targets of DDoS attack would be popular sites like Yahoo, CNN, eBay, and Amazon etc. The DDoS attacks on these sites results in their loss of fame, unavailability. Their share market will become down and financially it will become disaster for these organizations.

Though there are several commercial IDS products are available in the market, there is no product to thwart completely the DDoS. Detecting

4.9 Human Resources

The Intrusion detection products that we have analyzed in our survey in chapter3 are not automated products. All the present commercial products require human involvement to configure and develop signatures. The IDS products cannot block the attacker by looking at the IP address; it can not take any reaction on the attacker itself. So, to analyze the traffic, to take the reaction against the attacker, to report the analyzed traffic, to do the forensic analysis, enterprises need intellectual people.

In an anecdotal observation, it is observed that a major cost for the enterprises when they maintain IDS is, Staff. Maintaining well-qualified people for the Intrusion detection systems is a very big challenge for most of the companies and it contributes to the major part of the IDS expenses. This is also one of the hurdles that are blocking the enterprises to deploy Intrusion Detection Systems. Maintenance of Staff is the major factor that is to be considered when deploying Intrusion Detection Systems.

Recruiting Staff is also another challenge for the enterprises. Understanding the products and developing signatures and technical management of Intrusion detection requires a great amount of intellectuality. Since the IDS field is not so broad and not so old, getting the right people with right experience is considered as a challenge.

4.10 High Speeds

Gartner Research team, John Pescatore, Richard Stiennon and Anthony Allan in their "hype cycle for Information security, 2003", stated that NIDS do not work at network speeds. Most of these IDS products are unable to detect attacks in real-time, and they can not handle high speeds of internal networks [4.12].

It is known that Processor speeds are not increasing with the increasing speeds of networks. The high speeds of the networks generates huge amount of traffic with in a short span of time. The IDS product that works with lower speed than the network causes it to drop packets, and makes unreliable.

The High speeds of the network, when it contains encrypted data, make the problem for IDSs severe. It causes either more buffer space to save the data or dropping of the packets. As the NIDS products have to perform analysis on network packets, the increasing speeds of the networks poses a new challenge to the existing NIDS products. From our survey in the previous chapter it is evident that some IDS products are capable of Gigabit speeds. In reality, all these products are not truly providing such high speeds. These high speeds boasted by the IDS vendors are not genuine. It is observed that these IDS products can sustain up to 60-70% of their hyped speeds.

Broadband connectivity that links more than 30 million users and enterprise networks worldwide allows hackers to co-opt multiple systems' processing power to mount Distributed Denial of Service (DDoS) attacks that can easily saturate high speed multi-gigabit pipes and overwhelm the most powerful server and computing environments

Another bottleneck with high traffic is, analysis. Most NIDS use "signature-based", which has the property that the more signatures we add, the slower it becomes. The deep-packet inspection and state maintenance between sessions; all these kinds of tasks require very high speeds of the IDS products. To address the limitations of the processors with increasing speeds of the networks, researchers should focus on to increase the speeds of the processors and capability of IDS products.

Chapter 5 Evaluation Criteria

There are myriad numbers of commercial IDS products available in the market. Everyday several new vendors are making their inroads into the Security market and aggressively competing for market capture. Choosing perfect IDS for an organization is not a simple task. It requires careful study, analysis, and comprehensive Evaluation. The evaluation of the products depends on the security strategy and requirements of the organisation. A rigorous evaluation always yields a better product to deploy.

In chapter 4, we have mentioned several IDS challenges. Since these challenges represent the major requirements that a product should support, they are the building blocks of Evaluation criteria. So we have developed the Evaluation Criteria based on the challenges and other measurement characteristics in order to choose perfect IDS for an organization. This evaluation criterion is not intended to evaluate any particular product. It is not even targeted at any particular organization. If an organization wants to evaluate the products, based on this criterion, they have to select which measurements are relevant and not relevant for them.

This Evaluation Criteria is based on the general IDS requirements. In this part, we develop measurements like how the products are working in reality, how they are performing in pragmatic conditions, how usable they are, what are they supporting and what not. This will serve as a useful guide for the IDS deployment by delivering the state-of-the-art-requirements that a product must support.

In this chapter we list a set of measurements that can be made on IDSs. We focus specifically upon those measurements that are related to the detection and performance accuracy. We focus on the usability, management, and protection areas also.

5.1 Zero-day attack Protection

It is presented that zero-day attacks are one of the challenges that pose problem to the IDS technologies. Zero-day attacks have the potential to wreak havoc, so in order to protect resources, IDS products must protect against these attacks. As the Anti Virus products and firewalls are inadequate solutions to protect against zero-day attacks, the IDS with zero-day protection feature embedded in it is very important to the organization.

An attacker can cause maximum damage with a combination of an application exploit intermingled with a DDoS attack by taking advantage of the time gap between patch release and vulnerability announcement. These kinds of attacks are harder to defend against and increase the chance of malicious traffic penetrating the infrastructure. For example, SQL slammer worm targeted at Microsoft SQL servers created a disaster with in a short time.

So, zero-day attack protection is one of the most important features to look in the products. Since signature-based systems depend on the signature database, they are the prime victims of the zero-day attacks. In order to combat against this, signature based IDSs must be updated accordingly with the vulnerabilities announced.

The following questions can be evaluated to measure the zero-day protection property in IDS systems.

1. How frequent the signature-based IDSs are updated?.
2. How far does an IDS offer protection against zero-day attacks?
3. How much time an IDS vendor takes to release a new signature for an announced Vulnerability?
4. Is there any facility for the combined functionality of Anomaly Detection and Signature-matching in the product?
5. Does the product detect zero-day attacks alone, or with additional systems like HIDS?

5.2 Data Collection and Correlation & Forensic Analysis

The defence-in-depth approach of network security principle has become essential and important. The defence-in-depth or layered approach contains different kinds of tools like firewalls, routers, anti virus products, vulnerability scanners, honey pots, Intrusion Prevention systems and Intrusion detection systems. We have already insisted that data from all the products is very important for a productive and better intrusion analysis. An IDS product that supports data collection and correlation can be given highest priority in Forensic Analysis.

The following questions can be evaluated to measure an IDS product's ability of data collection and correlation.

1. How many other network security products that an IDS supports?
2. Is there a data collection and correlation feature in an IDS product?
3. Does an IDS product correlate the data in a manner to assist the forensic analysis?
4. How easy it is to navigate in forensic analysis?
5. Is the information archived by the product is sufficient for the forensic analysis?
6. How long it stores the data?
7. Does an IDS product process all kinds of data like Windows, Linux, UNIX, and SNMP Etc?
8. Does the product needs human involvement? Or is it automatic?
9. How does it store the correlated information?
10. Does it support a third party tool for correlation process?

5.3 Encrypted Traffic

We have stated that encrypted traffic is one of major challenges for IDS products. The present Internet traffic consists of up to 50% of encrypted traffic and the use of encrypted traffic is increasing at a rapid pace. Processing the encrypted traffic and analysing it for attacks is very important for most of the organizations.

Due to the importance of Encrypted traffic and its potential of hiding attacks in it, processing of Encrypted traffic is a great requirement for the IDS products. A better IDS has to inspect the encrypted traffic like SSH, VPN, IPSec, and SSL without any need for additional resources.

The following questions can be evaluated to measure an IDS product's ability to Encrypted Attacks.

1. Does IDS can support the processing of encrypted traffic? Does it miss any packets without inspection?
2. How it processes the encrypted data, with or without intercepting the traffic?
3. Is there any need to give cryptographic keys to IDS also?
4. Does it support IPSec, VPN, SSH, SSL protocols?
5. How it performs when decrypting the traffic? Is there any need for additional resources?

5.4 IPv6

IPv6 is the advanced version of IPv4 protocol. Due to its large address space, long header format, latest security features, and many advantages the use of IPv6 has become inevitable. Since the IPv4 protocol cannot serve the future applications of Internet, IPv6 is gaining importance and IPv6 traffic is also increasing at a brisk pace. So, the use of both IPv4 and IPv6 is very important in the state-of-the-art intrusion products.

If a product cannot support the IPv6 traffic, it will become blind to attackers using IPv6. We will evaluate the products for the successful implementations of IPv6 protocol.

The following questions can be evaluated to measure an IDS product's ability

1. Does a product support IPv6?
2. How it solves the problem of IPv6's encrypted traffic?
3. How it handles the tunnelling problem?
4. Does it allow dual-stack approach?

5.5 Attack Detection Comprehensiveness

The primary goal for the intrusion detection products is attack detection. It is imperative that no IDS can detect all kinds of attacks in the space. Better IDS should always be able to detect known, unknown, known with new variants, insertion and evasion attacks, and all types of attacks. To the least, good IDS should detect all the known attacks like the antivirus products with its signatures and it should also be able to detect the attacks that are producing on the Internet.

The inherent complexity of network traffic and numerous numbers of protocols at the Network, Transport, and Application layers provide sufficient vulnerabilities to camouflage the resources. We have also encountered that some of the attacks are not straightforward and occurs at different sessions and different stages. They change their shape and Bourne accordingly in these multi stages.

The following questions can be evaluated to measure an IDS product's ability of Attack Detection comprehensiveness.

1. How many attacks can it detect?
2. How it protects itself from attacks?

3. Is it able to detect Evasion attacks? What is its strength against DoS and DDoS attacks?
4. Can it detect buffer overflow attack and its variants?
5. How many detection methods an IDS supports?
6. Does it have hybrid detection methods?
7. Does it support all kinds of protocols in network, transport, and application layers?
8. How far it detects the attacks that are hidden in protocols?
9. How well the product can identify the attack that it has detected? Is it by labelling with common name or vulnerability name, assigning the attack to a category.
10. Is it able to determine whether an attack is a success or failure?
11. How does it detect the advanced polymorphic worms?

5.6 Detection methods and Accuracy

Detection methods are the core functionality of IDS to detect attacks. There are several different detection approaches offered by different products. Since every detection approach has its own limitations and disadvantages, the combination of different detection methods would yield better results. For example, if a signature based method cannot detect a new attack, it may be detected by the anomaly detection method.

False alarms are the wrong and undesired notifications that minimize the detection accuracy. False positives are the alerts caused by the detection engine for a non-malicious traffic and determine the accuracy of the IDS detection rate of attacks. Especially, anomaly based detection engines generates more number of false positives, due to their nature of flagging everything as alert, if the monitoring traffic is out of the specified background. False alarms make the intrusion analysis more difficult, and they hide the real attacks in them. This measurement is vital and the IDS that produce less number of false alarms would be the desired product to select.

The following questions can be evaluated to measure an IDS product's ability of Detection methods and accuracy.

1. How many detection approaches an IDS have?
2. Does it have hybrid detection methods?
3. Is there any deep-packet inspection method?
4. Does it have state-based detection method?
5. How frequently the vendor upgrades the detection methods
6. Is there a facility for customization?
7. How does it monitor the traffic?
8. How far it is able to detect the content-based attacks?
9. How many false alarms it produces?
10. Is there any mechanism to reduce the false alarms?

5.7 Processing Power of High Bandwidth and High Speed Traffic

We have already mentioned in the previous chapter that high speeds of the Internet traffic poses lot of problems to the Intrusion Detection Systems. Since Internet speeds are surging at a brisk pace, IDSs should also sustain with the high speeds. The high speeds of Internet generate huge amounts of data to process. This measurement determines the capability of IDS to weather the high bandwidths and high speeds of the Networks.

This characteristic requirement depends on the required levels of the bandwidths and speeds. Most of the products start to drop packets when they reach certain levels of traffic volume and speed. This results in attack missing and low detection rates. Sometimes, due to the overwhelming traffic, IDSs will crash. The state maintenance, deep packet inspection, encrypted traffic, parsing the huge database of signatures, and to keep up with the true real-time property, IDSs must be capable to weather high bandwidths and high speeds.

The following questions can be evaluated to measure an IDS product's ability of handling high bandwidths and high speeds.

1. What is the maximum speed that the product supports?
2. How much bandwidth can it handle without missing attacks?
3. How it scales, if it experiences excessive traffic?
4. How it performs, when it has to analyse at excess speeds?
5. How well it scales according to the increase in signatures?

5.8 Ease of Use

This is one of the most important measurements to be considered when selecting of any products. The complexity of a product prohibits the buyer from purchasing. A good usable system with out much confusion always yields better results. In IDS products, ease of use is the most essential feature. A good system must allow an analyst to quickly view the information, to quickly deploy, easily operable and easily configurable. The high technical skill requirement and complexity of the product makes users hard to operate and increases the problems in managing. A good IDS system must have user-friendly interfaces, GUIs, colours, and well-designed easily navigable features.

For example, intrusion detection systems raise flags for all attacks. But, each attack cannot be treated as severe. So, if there is a feature to prioritize the attacks, administrator can respond to an attack that is severe. He can ignore the non-important attacks.

The following questions can be evaluated to measure an IDS product's usability.

1. How much time it takes to understand the product and to create policies by the vendor's training?
2. How simple the installation phase?
3. How many policies an IDS requires?
4. How easy it is to deploy sensors and integrate?
5. How easy it is to upgrade the signatures and patches?
6. When it detects attack, does it provide more information about the attack, or just the attack name?
7. Is there any feature like recommended action when it detect an attack?
8. Is there any need of learning new language or common programming languages to customize, maintain, and operate?

9. Does it have GUIs and colours?
10. Does it give the snap shot of what is going on in the network?
11. Is there any feature to aggregate and merging the attacks?
12. How the product manager tells the product what to monitor for?
13. Is there any feature to refine the level of data?
14. How the product allows viewing the events?

5.9 Human Resources

Recruiting well-qualified employees and managing them is one of the challenges that are described in the previous chapter. In the overall picture of IDS management, the major expenditure is on human resources. Since, Human resources constitutes the large portion of the IDS budget, reducing the budget on HR is essential and very it is very important to consider before deploying. If a product is complex and requires high technical skills, it is ought to recruit highly skilled professionals, which obviously increases the budget. A product with simple management and operable with less human resources, would be the product to look for in the selection.

Some products like Cisco have great significance in the market. It would be very easy to recruit employees with Cisco experience. The following questions can be evaluated to measure an IDS product's requirement of Human Resources.

1. What kind of skills a product needs?
2. Is it easy to recruit the people to manage the IDS?
3. Does the product require any specialized skills persons? Is it easy to recruit them? Are they available on the market?
4. How many number of people does a product needs to manage?

5.10 Security

This measurement asserts how secured an IDS is to nefarious users who first tries to evade the IDS itself, how secure are the communications, and how strong the cryptographic mechanisms offered by the product. Attackers sends large amount of non-malicious traffic to overwhelm the IDS's processing power. Due to the flood of traffic, IDS starts to drop packets and be unable to detect attacks. There are different ways to attack the IDS, so protecting itself is very important. So measuring security as one characteristic demonstrates the products ability to secure itself.

The following questions can be evaluated to measure IDS product's Security.

1. What is the method of access for Administrator to the console?
2. Are the communications between the console and sensor encrypted?
3. How secure are the encryption algorithms?
4. Does the product have any back-up facility for the loss of data?
5. How resistance it is to attacks?
6. Are all the communications authenticated and encrypted?

5.11 Alerting and Attack Response

This is one of the measurements that strongly demonstrate a products capability to protect the resources. For IDS, after detection of an attack, it must alert the responsible person and should take a proper action to block the malicious traffic and to take action against the attacker.

A product with flexible alerting system allows sending alerts anywhere. Multiple Alerting options increase the flexible in managing the IDS. Active responses are important in taking appropriate and real-time action against the Intruder. This decreases further damage of the attack.

The following questions can be evaluated to measure an IDS product's ability in Alerting and Attack Response.

1. What are the methods of alerting?
2. Does it alert for every event? Or does it correlate the alerts?
3. Does it merge the attacks before alert?
4. How it responds to an attack?
5. Does it have any feature to block the attack immediately after the attack happens?
6. How long it takes to respond to an attack?
7. What are the response options?
8. Is there any way to customize the response options?

Chapter 6 Evaluation Results

In this chapter, we have found the evaluation results for four network security products that have been assessed. We have omitted the two host-based IDS products; Tripwire and Intruder Alert. Since the evaluation criteria developed mainly focuses on the network based IDS products, Applying this criteria to the host-based would be irrelevant.

The four products that have been evaluated are Cisco, NFR, Secure Net and Net Screen IDP. These results can be treated mostly as anecdotal, since we have found these results based on the product sheets, data manuals and third party evaluations. The third party organizations that we have got the information had done the evaluation in the real-world. In this facet, these results can also be considered rigorous.

6.1 Zero-day attacks

Cisco: we know that signature based Intrusion detection systems suffers prevalently from the zero-day attacks. Cisco uses an array of detection methods including pattern matching, protocol analysis, and anomaly detection. Moreover, Cisco's signatures are updated every two weeks. Albeit anomaly detection method can protect the zero-day attacks to some extent, it does not have any special facility to protect against zero-day attacks. But, Cisco works VPN/security management Solution (VMS) delivered with HIDS can offer protection against the zero-day attacks with its CSA.

Net Screen: This product does not mention anywhere that it protects zero-day attacks. Its signatures are also updated weekly, and it does not have any special feature to protect against the zero-day attacks.

NFR Sentivist: It has only signature based and protocol anomaly based detection method, which are not so strong against zero-day attacks. But, NFR offers moderate protection against zero-day attacks by looking for the vulnerability and not the exploit to catch mutations.

Secure net: It relies more on the very advanced protocol decode engine and network grep engine. These detection approaches make the novel attacks hard to happen. Since Secure Net is not depending totally on signature based detection method, which is not strong against zero-day attacks, Secure Net is convinced to protect zero-day attacks.

6.2 Data Collection & Correlation and Forensic Analysis

Cisco: From NSS.co.uk Cisco's Cisco works SIMSv.3.1 product supports the correlation of events in one of its four management's options. It supports data collection and correlation of event data generated from different other network security products. It allows manual correlation of events from different sensors at a basic level. But it does not process different kinds of data mentioned in the evaluation criteria like Linux, UNIX, windows. Gartner in its report revealed that Cisco IDS does not support any network products other than Cisco. So, it can be concluded that Cisco offers event correlation at a basic level only when the event data generated from Cisco products.

IDS device manager when detects an attack and raises an alarm is sent to the event monitoring host, where the IDS event viewer(IEV) writes it to an ASCII event log and to a MySQL database. The logged data depends on how the sensor is configured to monitor. The Cisco Threat Response also helps in forensic analysis by investigating in a three-phase approach by enabling the administrator to make decisions.

Net Screen: Net screen does not allow for any kind of correlation of events either manually or automatically. The ability to apply filters and drill down to more detail views within the Log viewer and Log Investigator makes it a useful tool for the forensic investigator, but due to the lack of correlation feature, it provides very less details to enhance the investigation process.

NFR Sentivist: NFR product does only alert correlation, but there is no event correlation to help forensic analysis and to reduce false alarms. For forensic analysis, NFR is not the choice. It provides little information about an attack. Conducting forensic analysis is also difficult. But NFR product integrates with popular firewalls to prevent future attacks.

Secure net: For those, who are looking for a best forensic IDS product, Secure Net is the best product. It correlates the events, supports multiple formats of data, multiple dimensional arrays, and full memory protection. The main event data resides in the much larger relational data base, which allows more detailed forensic tools. It also allows the administrator to view and store the event data in a customizable way and for a long time. It takes 24 hours of time for events to appear in the main forensic analysis module from the local cache, which is not a desired feature.
Also, the detailed recording of events for forensic analysis has a negative impact on the performance of the sensor. Apart from the small niggles, SecureNet assures as a best Forensic product with its event correlation capability

6.3 Encrypted Traffic

Cisco: Most of the NIDS offers very less protection against the encrypted attacks. Cisco's NIDS also does not specify any kind of feature to process the encrypted traffic. But Cisco HIDS delivered with the extra cost of VMS can process the encrypted traffic, but it is hard to say whether it can completely detect the attacks in encrypted traffic. The Cisco HIDS supports SSH, SSL/TLS protocols.

Netscreen: Netscreen IDP uses backdoor detection method, which can detect all backdoor attacks, both known, and unknown, even if the data is encrypted.

NFR Sentivist: NFR is not able to process the encrypted traffic. It can be vulnerable to encrypted attacks, since it does not have any special mechanism to detect them.

Securenet: SecureNet does not have any special mechanisms like SSL proxy. There is no information regarding its capabilities to process encrypted traffic. From the data sheet, it can be observed that the protocol decode engine is able to decode the SSH protocol, but not any other encryption protocols.

6.4 IPv6

Cisco: Cisco NIDS does not support the Ipv6 protocol. It can support only the Ipv4 protocol.

Netscreen: Netscreen IDP does not support Ipv6 protocol. It supports only Ipv4 protocol.

NFR Sentivist: One of the most salient feature with NFR is it supports the Ipv6 traffic, which in turn helps to detect the tunnelling exploits for example.

Securenet: SecureNet is not able to support IPv6.

6.5 Attack detection comprehensiveness

Cisco: Cisco offers protection against all kinds of attacks like floods, DoS, www attacks, Buffer overflow, IP fragmentation attacks and TCP hijacks. It is also excellent in protecting against the most important evasion attacks TCP stream reassembly, Unicode deobfuscation , IP fragmentation reassembly. Cisco NIDS was successful in protecting against all kinds of evasion attacks tested by NSS.co.uk. Cisco Threat Response (CTR) uses a just-in-time investigation of the targeted host to determine if the attack was successful or not.

Netscreen: Netscreen from its array of eight detection methods detects all kind of attacks. It detects Backdoor attacks, SYN flood attacks, DoS attacks and Layer 2 attacks, IP spoofing, all kinds of insertion and evasion attacks, and it has Network Honey Pot. An important aspect with Netscreen is, it can also prevent attacks when it operates inline.

NFR Sentivist: NFR is able to detect most of the attacks; known attacks, stealth attacks, anomalous behaviour, first strikes, DoS floods, and polymorphic attacks. It detects the IP fragmentation and reassembly attacks, reassembles TCP streams, it tracks sessions to identify disguised attacks and detects the tunnelling exploits by supporting Ipv6. NFR recognizes all five types of IP fragment reassembly. It reassembles TCP streams, and tracks sessions to detect multi-stage attacks. It detects port scanning and host scanning as well.

Securenet: SecureNet is able to detect IP fragmentation attacks, TCP Reassembly attacks, Port scanning, and all most all of the insertion and evasion attacks. It tracks full 3-way handshake of TCP and four-way TCP tear down. It supports a wide range of protocols to detect single packet attacks and attacks that are prevalently wild and intentionally malicious.

6.6 Detection methods and accuracy

Cisco: Cisco uses array of detection methods to accurately detect all the attacks. It uses the combination of Stateful protocol pattern recognition, Protocol Parsing, Heuristic Detection and Anomaly detection. It updates the signature database depending on platform and urgency. Cisco allows customizable attack definitions and to create policies. It provides the deep packet inspection capability at gigabit rates with its 4250 sensor option but not with the 4235 sensor. It is very slow to scale to large number of signatures.
When it comes to the accuracy Cisco is very good in reducing the false alarms by correlating events. It allows defining the filters for a sensor to enable and disable alarms that have specific hosts and networks as their source or destination. It is also secure against the random fragmented attacks by the user-defined reassembly options. NSS revealed that Cisco works well in reducing the false positives.

Netscreen: NetScreen IDP is unique in all of the products evaluated. It has an array of eight detection methods and has the ability to operate in-line which can be considered as very important property. The detection methods are stateful signature, protocol anomaly, traffic anomaly, backdoor detection, IP spoofing, SYN flood detection, Layer2 and denial-of-service detection and Network Honeypot.

Attack objects are used in IDP rules which can be updated weekly. The attack objects are categorised and grouped according to severity first and target application/platform second, but not by either of it. It is possible to have any number of security policies, but only one security policy is activated at each sensor. Different sensors can have different security policies. The Netscreen IDP allows customizing the signatures. To reduce the false positives, it provides the direct access between the event and the security policy that triggered. But NSS has found that Netscreen sometimes produces more alerts than strictly necessary.

NFR Sentivist: NFR has advanced signature and stateful protocol analysis for many network-based protocols. It does not have detection methods like heuristic detection; traffic anomaly detection enabling it detects all types of attacks. Since NFR enables to develop our own signatures, the detection accuracy is high. But NFR produces huge amount of irrelevant alerts, where real attacks can hide.

Securenet: SecureNet supports Stateful Signature detection, Protocol Decode, and Network Grep engine. PDS nexus is the signature distribution mechanism. In the stateful detection method, heuristics are used in every aspect of the state engine to compensate for fragmentation that is typical of most networks. It allows defining two signatures for a single policy. It has full implementation of the most common protocols allows Netscreen product to acquire more knowledge and reduce false positives. SecureNet ensures accurate detection even when packets are dropped and streams are fragmented. But protocol analysis of this method has high propensity for false positives, though its performance is high. What makes SecureNet a rare beast is, Hybrid architecture, allowing protocol decode and network grep in a single package.

6.7 Performance at High Bandwidth and High speed traffics:

Cisco: NSS proved that Cisco IDS performance was very good across the board. Detection rates are also very high; it meets the expectations of a 200 Mbps device. The scaling capacity of the signature data base is not good, with increase of signatures. The sensors will crash after it reaches the 50,000 open connections. It ideally suits to monitor multiple Fast Ethernet segments or T3 connections.

Netscreen: Netscreen IDP allows high availability configuration mode to provide failure protection, in load balancing mode, all sensors in the cluster share network traffic equally, in hot standby mode a primary sensor handles all traffic, while the second sensor stands by. If primary sensor fails, network traffic is redirected to the secondary sensor. This flexibility in configuring the sensors makes Netscreen to perform better at high speeds. By default it allows 100,000 open connections. Though Netscreen is up to its performance in normal conditions, its performance is reduced in very high TCP connection rates.

NFR Sentivist: The sentivist sensors are available for gigabit and full duplex 100 Mbps Ethernet networks which ensures the maintenance of state. NFR has also options for highly available networks, enabling continuous monitoring of high availability or fail over networks. Sentivist sensors can be configured to automatically redirect their data to an alternative Sentivist Sensor in the event of failure, ensuring continuity of alerting and event recording.

Securenet: The manager system of SecureNet has an internal event cache that is optimized for insertion rate to ensure that no events are lost when the IDS experiences High Bandwidths. SecureNet claims that the secureNet Provider manager has been load tested to accommodate up to 50 sensors on a single processor system when sensors are tuned to produce an average of two events per second. Dual and quad processor systems with additional memory can be used to support more sensors or sensors with higher event rates. NSS certified SecureNet as one of the most flexible and powerful real-time event monitoring tools they have seen, and will go a long way towards helping the administration control and analyze effectively the huge amount of data that is likely to e generated by a Gigabit IDS.

6.8Ease of Use:

Cisco: The IDM user interface is very intuitive and easy to use. The signatures can be grouped according to different implementations of different detection methods. This feature enables the Cisco IDS very flexible and readily extensible with custom signatures. The tuning of the built-in signatures is very difficult with out the pre-knowledge of the signatures. It allows the enabling of all signatures in just one click. It has both command line and GUI utilities

Albeit the event viewer is not the most intuitive interface for resorting, expanding and collapsing entries it is very flexible and powerful tool. With the turnkey appliance approach the installation tasks are also minimal and command line interface implemented by the Cisco makes the sensor to have a familiar look and feel with Cisco experience. By providing a quick way to switch between detail and summary views, Cisco stands as a flexible product to use.

Netscreen: It uses graphical user interface for interacting with the IDP system, it can be managed remotely as well. It was proved by NSS that Netscreen offers very high degree of flexibility in deploying the sensors, since it can be deployed in router, bridge, or proxy ARP modes. The installation of the product is very straightforward and takes no more than five minutes.

Netscreen's user interface allows each administrator to configure the UI with his own preferences, which remains consistent from different locations. The centralised management system makes it easy to configure, update, and maintain the IDP system from a single administration point and myriad of sensors can be managed with a single, logical security policy. The UI contains seven components which give a more clear view of the traffic and it also allows customizing with the desired features. The logged entries contain an easy accessibility with the relevant information like log viewer, session viewer and security policy editor in just one-click. The signature editor also contains reference tab that provides links to outside information about the attack, such as the attack CVE number and description. It allows customizing the log data and also enables to export data to use in other applications through a CLI. Finally Netscreen is easy to install and easily manageable.

NFR Sentivist: According to NetworkWorldFusion, Installation of NFR is a breeze. Signature developing capabilities, and tuning is quite easy. It has a simple management for many sensors. But the Forensic capabilities make it difficult to find what we want. NFR is best, if an organization intends to develop its own signatures. NFR has solid event filtering feature. It has a great facility to apply the rules for events, at a single push to all sensors. Another shortcoming with NFR is, it does not provide additional information about an attack, and like what port addresses were attacked. Refining of the data is also very difficult.

Securenet: SecureNet provider is a three-tier management system designed for scalable enterprise and service provider deployments. Filtering is done with a simple GUI on the manager. The relational database is completely open, giving unrestricted access to manage, extend, and manipulate the data and database. The administration interface to the entire system is through windows-based GUI with flexible and intuitive interface to monitoring, reporting and forensic capabilities. Software and Signature distribution is done with simple-drag-and-drop actions. It allows customization of the protocol decode engine from the scratch.

The configuration and monitoring tools are divided into three utilities, which can be used different personnel in a company. The administration interface is excellent allowing the administrator to apply filters based on engine type, priority, signature group, exploit class

6.9Human Resources:

Cisco: It is well known that Cisco is the market leader in networking products and it is most common. So, Cisco products have an edge over other products in terms of recruiting human resources and it is very easy to find people with enough experience over Cisco products. From NSS testing it is evident that Correlation process and developing customized signatures from the scratch requires significant technical knowledge.

Netscreen: though the customization process is straightforward, it requires significant knowledge to develop signatures and to develop customized views and responses. The Netscreen product is easily manageable and the policy management is also very straightforward. But, it can not correlate events which results in increasing labour costs for the forensic investigation. So, NetScreen requires significant technical knowledge and significant expenditure on labour.

NFR Sentivist: NFR product through it has a great flexibility in signature developing; it requires human intervention to conduct the forensic analysis. NFR provides a powerful development environment for its proprietary N-code language. It means that, NFR does not require people with great experience for signature developing, since it is a cake-walk.

Securenet: Securenet uses SNP-L language which is quite similar to the C programming language for development of protocol decode engine. The strong correlation feature supported by this product is also not automated. Though the Securenet product offers some of the excellent administration and management features, it requires significant Human resources.

6.10Security:

Cisco: The communication between the sensor and IDS device manager is through a secure encrypted TLS link using Netscape and Internet Explorer web browsers to perform various management and monitoring tasks. The promiscuous operating mode makes the IDS more secure for its own attacks. A user must log in to Cisco IDS successfully before system access is granted and it also seperates the access by defining the roles. Only users with full access have complete control over the database. It also allows setting cryptography on or off.

Netscreen: Netscreen IDP encrypts and authenticates all the communication between management server, user interface and the sensor.

NFR Sentivist: NFR is a tamper proof system. The sentivist sensor software and operating system run from the product CD. The standard UNIX services, shells, and drivers have been removed to make the system resistant to attack. All the communications between system components are encrypted.

Securenet: All communications within the SecureNet architecture are authenticated and encrypted. It encrypts all communications via the WBI (web user interface) through

HTTPS. It protects itself even when attackers try to evade the system. All the signatures operate in a "sandbox" environment to protect sensor from self targeted attacks.

6.11 Alerts and Attack Response

Cisco: Cisco IDS has a number of active response capabilities. It sends alerts via console messages, e-mail, pages, scripting and reports. It can terminate the active sessions using TCP resets, blocks the connection instantaneously by changing ACLs at the router, switch or firewall. Cisco IDS has both built-in and customizable alarm classification based on the severity level which would result in the classification of responses and make the administrator job easy. It also allows customizing the response options which is an excellent feature to consider.

The IDS event viewer is a Java based application that enables the administrator to view and manage alarms for up to three sensors. It enables to view alarms in real time or via imported log files. It is possible to export data from the IDS event viewer tables to an ASCII file for analysis via third party applications. The IDS event viewer ships with five default views by source address, destination address, sensor ID, signature name, or severity. It also enables to add notes to a particular alarm and to recommend certain action for that alarm. Not all the alarms provide the context data.

Netscreen: The salient feature with Netscreen is, the sensor can take predefined action and prevent the malicious traffic, if it is configured as in-line and it can act as an active gateway, unlike the traditional passive sniffing IDS. When it operates in passive sniffing mode, it can not prevent the traffic. Alerts are stored in a proprietary database, 50,000 logs per second. Netscreen IDP increases the transmission rate to send logs to management when it detects an attack.

The actions of Netscreen after detection of an attack are: ignoring the connection, dropping packets, dropping connections, closes either client or server. But it does not take any action against the connection. It also has a great feature of blocking of future occurrences of IP addresses of attackers. The notification options are logging, alarms, tracking session data, SNMP trap, syslog message, e-mail, script. The backlog is action and alert options can only be set at the individual rule level, not on a global policy wide basis.

NFR Sentivist: In NetworkWorldFusion testing, NFR produced huge pile of irrelevant alerts and had to paw through them manually, to figure out what had happened. It also misses some of the attacks. NFR displays only 1000 alerts which take significant time to print on the screen. NFR is not strong in Alert Filtering, it generates excessive alerts. It supports easily reprioritizable alerts and defines presentation. It alerts through e-mail, or on a pager, and, at the user's discretion, can initiate automated responses. Automated response is a useful feature by NFR. The sentivist enterprise console includes alert consolidation, alert correlation across multiple sentivist servers, real-time graphing and alert filtering directly from the main alert screen. The automatic responses initiated by NFR include notifying IBM tivoli and HP openView enterprise management systems, generating SNMP traps, resetting the TCP session, and initiating firewall actions.

Securenet: SecureNet has different alert options such as SMTP messages for pages, mobile phone or e-mail. Messages can be customized by sensor to include any type of information available in the alert. SNMP traps can be sent for both intrusion events and the health and status of the appliance. Administrator has flexibility in sending the alerts to Web, Linux or Windows clients. Apart from these alert options, there are active responses like TCP Reset and TCPdump. The interface for the alerts is a familiar look, almost like Outlook express. The screen provides access to Monitoring, Reporting, and Forensics functions. Alerts can be filtered by sensor, location, signature group or signature name, and then applied on a per-client basis. One more important aspect with Securenet is the use of client filter views, which allow the administrator to designate the network packets that are of interest, whilst filtering out those packets that are not. When it comes to the reporting features, it has two options. One is simple reporting and detailed Forensic Analysis.

Chapter7 Conclusions

Now, Intrusion Detection Systems have state-of-the-art detection methods. They are unique in monitoring, analysing, alerting, reporting, archiving and reporting. Intrusion Detection systems play a vital role in the defence-in-depth approach of the modern Network Security. Behind the Firewall, ID System enhances the security and is a great aid in Forensic Analysis.

Most of the commercial products support the advanced features like Stateful Detection of attacks, deep-packet inspection, active responses, and signature management. The products have wide range of features. They have overcome several problems like switches, customization, signature development etc.

Despite the advancements and substantial research efforts, general IDS is struggling with some problems like Encrypted traffic, Ipv6, Insertion, Evasion and Denail-of-service attacks, High Speeds& Volumes. To assist the Forensic Analysis they are some problems in Data Collection and Correlation.

Different detection methods have different advantages and different disadvantages. So the Hybrid Detection methods would be a better solution. Although there are several challenges associated with the IDS, some of the evaluated products have resolved some of the mentioned challenges. It means that the challenges don’t last forever, they can be resolved. The state-of-the-art commercial products support some of the challenges through their product alone, some products supports with an extra cost separate system. So, embedding these extra cost separate systems into the IDS would be a nice idea. Since HIDS is good in Insider threats, it would be a great solution to incorporate HIDS into NIDS.

- ► For zero-day attacks, Cisco and Securenet are better.
- ► For Data collection and correlation SecureNet is the best, despite tiny niggles. Cisco is also good.
- ► For Encrypted traffic, No product is good as a stand alone application. But Cisco supports moderately with seperate SSL proxy.
- ► For signature development from the scratch, NFR is the better product.
- ► For signature management SecureNet is the better product.
- ► IPv6 is supported only by NFR product.
- ► SecureNet is very good to detect the insertion, evasion attacks.
- ► All the products are performing moderately at high speeds.
- ► For accuracy, Cisco and SecureNet are better.
- ► All products are satisfying the ”ease of use” measurement with small niggles.

It can be concluded that Intrusion Detection Technology is maturing. With significant research efforts it will play a great role in combating against the most complex attacks. It would be wrong to expect it as a complete security solution. In its entirety, it will play a major role and it is certainly emerging.

Chapter 8 Bibliography

1.1 Anderson, 1980, Computer security threat monitoring and surveillance. http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf.

1.2 Statistics from CERT, http://cert.org.

1.2 Julia Allen, Alan Christie, William Fithen, John McHugh, Jed Pickel, Ed Stoner's State-of-the practice of Intrusion Detection Systems. Attack sophistication Vs. Intruder technical knowledge. http://www.cert.org/archive/pdf/99tr028.pdf.

1.4 Computer Crime and Security Survey by the Computer Security Institute and FBI, 1998. http://www.pbs.org/wgbh/pages/frontline/shows/hackers/risks/csi-fbi2000.pdf.

2.1 Anderson, 1980, Computer security threat monitoring and surveillance.

http://seclab.cs.ucdavis.edu/projects/history/papers/ande80.pdf

2.2 Rebecca Bace, An Introduction to Intrusion Detection and Assessment for Systems and Network Security Management, http://downloads.securityfocus.com/library/intrusion.pdf

2.3 Peter Mell, NIST and Rebecca Bace, Infidel, Inc, NIST special publication on Intrusion Detection System. http://csrc.nist.gov/publications/nistpubs/800-31/sp800-31.pdf

2.4 Farmer, D., & Venema, W. (1999). *Internet Security Auditing Class handouts*, [www]. Available: http://www.porcupine.org/auditing/ [2001, 10 January 2001].

2.5 McKemmish, R. (1999). What is **Forensic** Computing? *Trends and Issues in Crime And Criminal Justice* (118). *Microsoft Responds to Security Issue*. (Press release)(2000). Redmond: Microsoft.

3.1 Net Screen IDP, http://www.juniper.net/products/intrusion/.

3.2 NFR Sentivist4.0, http://www.nfr.com/solutions/sentivist-ids.php.

3.3 Cisco, http://www.cisco.com/warp/public/cc/pd/sqsw/sqidsz/prodlit/ids4f_ds.htm.

3.4 Secure Net, http://www.intrusion.com/support/documentation/ReadMe/SecureNet-Sensor-2.5-Readme.txt

3.5 Trip Wire, http://tripwire.com
http://enterprisesecurity.symantec.com/products/products.cfm?ProductID=171&EID=0

3.7 Kathleen A. Jackson, 1999, Distributed Knowledge Systems Group Computing, Information, and Communications Division, Los Alamos national Laboratory, Los Alamos, New Mexico, USA. Intrusion Detection System (IDS) product survey. LA-UR-99-3883.

4.1 Network World Fusion, article http://www.nwfusion.com/techinsider/2002/0624security1.html.

4.2 Gartner Research Report, Hype Cycle for Information Security.

http://security1.gartner.com/story.php.id.54.s.1.jsp.

4.3 Protecting against "zero day" attacks, march 2004, Article ID : 3450. http://enterprisesecurity.symantec.com/article.cfm?articleid=3450&EID=0.

4.4 InfoSec 2003: 'Zero-day' attacks seen as growing threat http://computerworld.com/securitytopics/security/story/0,10801,88109,00.html?SKC=news88109.

4.5 Gerhard Eshelbeck, CTO and VP Engineering, Qualys; The Laws of Vulnerabilities. http://www.qualys.com/docs/laws_of_vulnerabilities.pdf.

4.6 What is the Role of Security Event Correlation in Intrusion Detection? by Steven Drew. http://www.sans.org/resources/idfaq/role.php.

4.7 Breach View SSL White Paper, http://www.gilian.com/IDS_Enhancements/pdfs/BreachView_SSL_White_Paper.pdf

4.8 Intrusion Detection Systems and IPv6, by Arrigo Triulzi, http://documents.iss.net/whitepapers/IPv6.pdf.

4.9 Oleg Kolesnikov, and Wenke Lee, Advanced Polymorphic Worms: Evading IDS by Blending in with normal traffic. www.cc.gatech.eduzSz~okzSzwzSzok_pw.pdf/advanced-polymorphic-worms-evading.pdf.

4.10 Ken and Gustav Publication of an article at Bug Traq. http://www.securityfocus.com/archive/1/359144/2004-03-29/2004-04-04/0.

4.11 Thomas H. Ptacek and Timothy N. Newsham at securenetworks, Inc. Insertion,
Evasion, and Denail-of-Service attack: Eluding Network Intrusion Detection Systems. http://www.insecure.org/stf/secnet_ids/secnet_ids.pdf.

4.12 Gartner Research Report, Hype Cycle for Information Security. http://security1.gartner.com/story.php.id.54.s.1.jsp

Appendix A

Feature	Cisco IDS	NFR Sentivist	TRIP WIRE	
Deploying				
Network-based	Yes	yes	No	
Host based		NA	YES	
Both				
Information source				
Network-packets	Yes	yes	No	
Operating Systems	No	NA	yes	
Applications			servers	
Others			Files	
Detection Method				
Stateful pattern recognistion	yes	yes	No	
Protocol parsing	Yes	yes	no	
Heauristic analysis	Yes	yes	Yes	
Anomaly detection	Yes	yes	No	
Hashing Algorithms	No	No	yes	
Timing				
Real-time	Yes	yes	yes	
Batch Mode	No	no	no	
Response				
active	Yes	yes	Yes	
Passive	No	no	No	
Technical Aspects				
IDS management	centralized	Centralized	Centralized	
Management capacity	medium	N/A	high	
Customization				
Intrusion patterns	yes	yes	Yes	
Network protocols	No	yes	No	
responses	Yes	yes	yes	
Audit record	No	na	yes	
reports	Yes	yes	yes	
Security options	No	no	yes	
Security				

Monitoring Technique	Stealthy	stealthy	na
Communication Security	Yes	yes	yes
Interoperability			
Common management	No	yes	no
Firewalls	Yes	yes	no
Vulnerability scaners	Yes	no	no
Honey Pots	na	no	no
Other security tools	no		yes
Event Management			
Event prioritization	yes	yes	yes
Event full information	yes	yes	yes
Event merging	yes	yes	yes
Vendor Attack DataBase	yes	yes	No
Automatic Signature Updation	yes	yes	Yes
Monitoring Event merging	no	no	yes
Signature Updation	Web	web	Command
Replication of Data	No	No	Yes
Active Response			
Router/firewall/switch reconfiguration	Yes	yes	No
Session hijacking	Yes	no	No
Session Termination via TCP resets	Yes	yes	No
IP session Logging	Yes	no	No
Automated Responses	No	yes	yes
Third Party integration	yes	yes	yes
Restore files	No	No	yes
Implementation			
Soft ware			yes
Hard ware		yes	
both		yes	

Support			
Vendor response	high	high	ok
24x7 Hotline	yes	yes	no
Product information	good	good	ok
Forensic analysis	yes	yes	yes
scalability	high	high	medium
Attack Protection			
Sweeps or floods	Yes	yes	No
DoS or DDoS	Yes	yes	No
Worms or Viruses	Yes	yes	Yes
WWW attacks	Yes	yes	Yes
Buffer overflow	Yes	na	No
IP fragmentation attacks	Yes	yes	No
ICMP,SMTP,POP attacks	Yes		No
FTP, Telnet, SSH attacks	Yes		No
TCP hijacks	Yes	yes	No
Integrity of files	No	No	Yes
IDS evasion Protection			
IP fragmentation reassembly	Yes	yes	No
TCP stream reassembly	Yes	yes	No
Other Protections			Na
Attack Notification			
SNMP traps	No	yes	yes
Alarm Display	Yes	yes	No
E-mail, E-page alerts	Yes	yes	yes
Script Execution	Yes	no	
Third party tool integratiom	Yes	yes	
Alarm summarization	Yes	yes	
syslog	No		yes
Reporting			

Interface	Console	Console	WEB
Format	Text , graphs	Real-time graphs	XML and HTML
Archiving	No	No	yes
Merging	yes	yes	yes
Customizable	yes	yes	yes
Adminstration			
Web user interface	yes	yes	no
console	yes	yes	yes
Remote Management	yes	no	yes
Applicability			
Client OS	Windows NT, 2000,XP.	Linux,Solaris,Windows 2000 or Windows XP	All OS
Server OS	Windows, solaris	Linux,Solaris	Na
Sensor OS	Windows, Solaris	No need of OS	na
Target Applications	Web servers, application servers	E-mail Servers, Web Servers, DataBases	All servers
Network speed	80 Mbps-1000Mbps	100mbps-gigabit	Na
Network Topology	T1/E1,T3,Switched Networks,	Ethernet full duplex	Na
Network Protocols	ICMP,Ipv4,TCP,UDP,IEEE 802.1q,DNS,FTP,RPC,SSH	All Ethernet Protocols	na
Additional applications		Supports Ipv6	na
Management and Acquition			
Performance	High	high	high
Robustness	high	high	high
accuracy	high	high	high
Employee education	medium	no	no

Appendix B

Feature	Intruder Alert3.6	Intrusion SecureNet	Netscreen-IDP	
Deployment				
Network-based	NA	Yes	Yes	
Host based	Yes	No	No	
Both				
Information source				
Network-packets		Yes	Yes	
Operating Systems	Yes	No	No	
Applications	Yes	No	Yes	
Others	File systems, audit logs			
Detection Method				
Stateful pattern matching	No	Yes	Yes	
Protocol parsing	No	Yes	Yes	
Heuristic analysis	Yes	Yes	Yes	
Anomaly detection	Yes	Yes	Yes	
Hashing Algorithms	No	No	No	
Timing				
Real-time	Yes	Yes	Yes	
Batch Mode	No	No	No	
Response				
Active	Yes	No	Yes	
Passive	No	Yes	Yes	
Technical Aspects				
IDS management	Centralized	Any WBI	Centralized	
Management capacity	100 agents	10 sensors	Unlimited	
Customization				
Intrusion patterns	Yes	No	Yes	
Network protocols	NA	Yes	No	
Responses	Yes	No	No	
Audit record	No	No	No	
Reports	No	Yes	Yes	
Security options	No	No	No	
Security				

Monitoring Technique	Self security	Stealthy	Stealthy
Communication Security	No	Yes	
Interoperability			
Common management	Yes	No	Na
Firewalls	Yes	No	Na
Vulnerability scanners	No	No	Na
Honey Pots	No	No	Na
Other security tools	Tivoli, BMC Patrol		Na
Event Management			
Event prioritization	Yes	Yes	Yes
Event full information	No	Yes	Yes
Event merging	Yes	Yes	Yes
Vendor Attack Data Base	Yes	Yes	Yes
Automatic Signature Updation	Yes	No	Yes
Monitoring Event merging	No	Yes	No
Signature Updation	Web	From nexus	Yes
Replication of Data	No	No	No
Active Response			
Router/firewall/switch reconfiguration	No	Yes	Yes
Session hijacking	No	Yes	No
Session Termination via TCP resets	No	yes	Yes
IP session Logging	No	No	Yes
Automated Responses	Yes	No	No
Third Party integration	Yes	Yes	No
Restore files	No	No	No
Implementation			
Soft ware	Yes		Yes
Hard ware		Yes	
both		Yes	

Support			
Vendor response	Ok	Ok	Ok
24x7 Hotline	No	No	No
Product information	Poor	Ok	Good
Forensic analysis	Yes	Yes	Yes
Scalability	High	High	Ok
Attack Protection			
Sweeps or floods	No	Yes	Yes
DoS or DDoS	No	Yes	Yes
Worms or Viruses	Yes	Yes	Yes
WWW attacks	No	Yes	No
Buffer overflow	No	Yes	Na
IP fragmentation attacks	No	Yes	Yes
ICMP,SMTP,POP attacks	No	Yes	Yes
FTP, Telnet, SSH attacks	No	Yes	No
TCP hijacks	No	Yes	Yes
Integrity of files	Yes	No	No
New attacks	yes	No	Yes
IDS evasion Protection			
IP fragmentation reassembly	Na	Yes	Yes
TCP stream reassembly	Na	Yes	Yes
Other Protections	Prevents unauthorized activity	Protocol Decode, Network Grep	No
Attack Notification			
SNMP traps	No	Yes	Yes
Alarm Display	Yes	No	Yes
E-mail, E-page alerts	No	Yes	Yes
Script Execution	No	No	No
Third party tool integratiom	Yes	Yes	No
Alarm summarization	No	Yes	No
Syslog	No	No	Yes

Reporting			
Interface	Console	MS Access	GUI
Format	Line and bar charts	Charts and graphs	Pivot tables, graphs
Archiving	No	Yes	Yes
Merging	No	Yes	No
Customizable	No	Yes	Yes
Adminstration			
Web user interface	No	Yes	Yes
console	Yes	Yes	Yes
Remote Management	Yes	Yes	No
Applicability			
Client/Console OS	Windows NT, HP-UX, Sun Solaris	Windows2000 Professional with Office2000Pro	Windows
Server OS	AIX, HP-UX, Solaris	Windows2000 Server, MS-SQL2000 Standard	Windows
Sensor/Agent OS	AIX, Digital UNIX, HP-UX, Windows NT, 2000.	NA	Windows
Target Applications	Web servers, Data Base servers, Files	Enterprises, Defence, Governments	Servers, business, enterprises
Network speed	Na	3 Mb/s- Giga Bit	100Mbps
Network Topology	Na	Fast Ethernet, Giga Bit Coverage	Fast Ethernet, Giga Bit Speeds
Network Protocols	Na	All popular	All popular
Additional applications	System and accounting file	Na	Na
Management and Acquition			
Performance	Ok	Ok	Ok
Robustness	Ok	Ok	Ok
Accuracy	Ok	Ok	Ok
Employee education	No	Limited	Limted