Intrusion Detection System

Marmagna Desai *

March 12, 2004

Abstract

This report is meant to understand the need, architecture and approaches adopted for building Intrusion Detection System. In recent years IDS has emerged as special technique to protect computers or networks, proactively. Hence the variety of attacks on the system/network are in huge numbers, the approaches to detect any attack are also in great variance. Though this report covers all major approaches and tries to explain method of "System Call Interception" used to build Anomaly Detection based Host based IDS. The goal of this report is to manifest most important features about the presentation made on [one of the most interesting topic] IDS.

1 Introduction

Intrusion Detection Systems attempt to identify unauthorized use, misuse and abuse of computer systems and alert proper individuals upon detection. The feature which distinguishes IDS from majority of security scanners or virus detection tools is the *REAL TIME* response and proactive steps taken when system is compromised. The usage of IDS can be varied depending on the Security Policy and needs of an institution. IDS can protect Network boundary or System-Server. IDS tools detect whether the Network or System is under attack or breached thus they form an integral part of Security System. When IDS is used in conjuncture with Security Policies, Data Encryption, Vulnerability Accessing, Authentication and Access Control mechanisms; it can promise Secure Network or System.

Recently there are many different approaches developed in the area of IDS. The mail classifications are based on the way IDS detect the attack or the entity IDS protect or the point of presence of IDS. The first category provides two major techniques : Misuse Detection and Anomaly Detection. The later part of classification is broad. HIDS, NIDS, NIDES, IDS and DIDS are some of the major implementations of IDS. The other major class of IDS is intrusion detection **Expert** systems. This approach is modern and it is not strict implementation of any one kind of IDS technique. Expert Systems are combination of Anomaly Detection, Misuse Detection and Network/Host based approaches.

As background, section 2 of this report presents an overview of NIDS, HIDS and Expert Systems. The main differences and appropriate scenarios are discussed in this section. In section 3 IDS techniques are explored. Anomaly Detection is the major consideration of this report. Hence the a unique way to implement this approach is annotated. Where System-Call interception and method of delaying malicious process on the System by delaying process schedulers is annotated as simplified implementation algorithm of Immune system Approach. Though this technique is strictly based on Host Based IDS, the idea is quite promising in Network based scenarios too. The IDS architecture in general is discussed beyond in section 4. Before this report conclude with, it presents some of the general requirements of and Ideal IDS.

2 Probe Techniques

This section defines some of the major probing techniques and state major advantages, disadvantages and features of them.

2.1 NIDS : Network IDS

Network based IDS monitors packets on network connection and attempts to discover an attempt to break in to system/network. Hence this type of IDS requires to set the NIC of the system to be in promiscuous mode. Packet sniffing is done at TCP or IP level and the header and payload of the packet is intercept before it is passed to IP or TCP software. A typical example of an activity performed by such IDS is a system that monitors for a large number of TCP connection request (SYN) to many different ports on a target machine, thus discovering if someone is attempting TCP port scan. A NIDS can installed at the target system where it watches its own traffic or at independent machine monitoring promiscuously all network traffic.

*101282813 - Computer Science, UoW

The major advantage of monitoring network traffic is the attacks which are destined to exploit network connections and services are detected. Most of NIDS work in Real Time. Hence they can detect a misuse over a network connection and generate an alarm based on Statistical Behavior model or Signatures. The other advantage of this technique is there is no processing impact/overhead on monitored system. Also network level attacks can be detected for a range of systems on a segment. The only major disadvantage of this systems is they can not detect any malicious packet which is encrypted. Also NIDS are not capable to analyze the payload in order to protect user data and processes. Finally, as network complexity and capacity increases, the performance requirement of NIDS can be prohibitive[idsieee]

2.2 HIDS: Host IDS

Host based IDS are systems which operates on operating system level and provides intrusion detection and protection to system from malicious activity. HIDS consult several types of log files such as kernel, system, network, firewall, server etc. and compares the logs against an internal database of common signatures of known attacks[Misuse Detection]. The approach of anomaly detection can also be adapted in HIDS where the module should be built as kernel extension, which will monitor the kernel process trees created by each user and identifying abnormal activity by comparing with internal database of normal activities. Regardless of the approach of detection HIDS acts at System level. This property of HIDS generates positive and negative aspects. This leads to comparison of HIDS and NIDS. Before comparing both techniques its important to summarize the advantages and disadvantages of HIDS. They operate in Encrypted environment, the attack can be mounted over a network or within a segment, encrypted data can be attached with the packet. In such situation, HIDS will monitor only the end effect of the attempt on operating system. Hence Encryption does not stop HIDS to detect attacks. Secondly HIDS is cheap and easily maintainable solution to security problem. Though HIDS has many negative features such as any kind of HIDS is highly O/S specific and it puts heavy load on the system. Hence for less powerful system this type of IDS is not applicable.

2.3 HIDS vs NIDS

It is a time to compare both systems!!

Function	HIDS	NIDS	Comments
Protection on LAN	****	****	Both System Protect User on LAN
Protection off LAN	****	-	Only HIDS protects User when he is OFF LAN
Ease of Administration	****	****	Equal from Central Admin Perspective
Versatility	****	**	HIDS are more Versatile
Price	***	*	HIDS more affordable if right product is chosen
Bandwidth Requirements	0	2	NIDS used LAN bandwidth. HIDS does NOT.
Cross Platform Compatibility	**	****	NIDS is more adaptable to Heterogeneity.
Central Management	**	****	NIDS more centrally managed.
Disable Risk Factor	*	****	NIDS failure rate is much Higher.
Local Machine Registry Scan	****	-	Only HIDS can do this type of scans.

2.4 Next Generation ID Expert System

As discussed in above section, IDS can be broadly classified in Host based and Network based implementations. Though both approaches have significant disadvantages. The necessity of reducing these flaws in practical IDS provided the birth of Expert Systems in IDS arena. Expert systems takes better from both worlds! Instead of exploring more about the expert systems this report gives some interesting features of Next Generation IDS developed by System Design Laboratory of SRI International.

NIDES: NIDES performs real-time monitoring of user activities on multiple target system connected via Ethernet.[SRI] This system has its own node to perform analysis and detection on the audit trails of user activity over network. It uses both techniques of Misuse Detection and Anomaly Detection to identify malicious signature which is knows as attack and also the novel pattern which can be instantiated by intruder *i.e. Anomaly.* The former is strict Rule-Based analysis where as the Anomaly Detection models the user behavior as profile and creates statistical model for each profile. The alarms generated by two analysis are screened by resolver component, which filters and displays warnings as necessary through the NIDES host X-windows interface.[SRI]

Greater details are necessary for Resolver component which is the key part of any Expert System. This part of system is responsible for identifying False positives and False Negatives from the alerts generated by two different approaches of analysis. Hence resolver has the forensic intellect to generate report in most efficient way. It can also automate report generation process by sending alerts to list of email recipients. Some user-configurable filters are also provided in NIDES. Filtered alerts are not reported but they will be logged for future references.

NIDES includes some of the useful facilities such as archiving and testing. Archiving can be done on the audit records, analysis results and alerts which have been gathered in the history. Where as Testing allows a security officer to experiment with new statistical parameters or new rulebase configuration before committing

them to running on NIDES. NIDES can run in Realtime or in Batch mode. It can monitor many heterogenous machines over a network.

Thus NIDES can be views as the best possible implementation of the IDS approaches we have in our knowledge yet there are many future prospectives and challenges in this direction.

3 Detection Approach

There are mainly two approaches to follow to build any IDS. Either probing method[*NIDS, HIDS*] uses one of the approaches or the combination of both. This section of the report explains them in detail with examples.

3.1 Anomaly Detection

Anomaly detection is mainly used in HIDS. At the heart of any IDS lies the ability to identify intrusions. This identification can be based on defining non-intrusions and classifying all other attempts as intrusion or the other way round. This approach follows the first way, which models normal behavior of the user or system. Any event which violates this model will be identified as anomaly and considered to be suspicious. The example of this can be given as follows:

Any normal process owned by non-root user entity is not allowed to access any executable file under /sbin directory on UNIX system. And hence any such process will not execute such executable as /sbin/init. Now, Anomaly Detection implementation creates a behavior model for such user. And also maintains database of system calls generated by /sbin/init. Thus when such process will perform a pattern similar to the stored pattern of system call for /sbin/init, the detection module will alarm Anomaly for that user. This event can be logged and also alerts can be generated.

The above example is over simplified example of behavior model for users. In practice this involves so many problems. The major are False positives. False Positive alerts are generated when a legitimate user or process behaves different than modeled pattern. In this case the user/process is legitimate and the activity is also harmless. But due to limited definitions of normal behavior system will detect such activity as anomaly and hence intrusion! The example of such case is given as follows:

False positive example can be given with respect to same example discussed. Let the system model system-call pattern for /sbin/init process for a root user. Now root user is allowed to modify this process according to his wish. Root can build a kernel module which extends /sib/init to do something extra than the usual process. In this case, whenever a Root will execute modified version of /sbin/init the IDS will find different pattern than it has modeled for Root for init. Now there is no way for IDS to determine the intension of the user to execute such different patterns. And this will generate a False alarm.

The modeling in this approach has been implemented in various ways. The next part of this section will discuss some of them.

Statistical Modeling: This was initiated by [Denning], it described number of statistical characterizations of events. Some of them are as follows:

- **Threshold Measure:**This scheme applies set or heuristic limits to event occurrence or event counts over an interval.[IDSIEEE] With respect to the example discussed, if the Root user performs different patterns more than a limit the system will detect as intrusion.
- **Mean and Standard Deviation:**By comparing event measures to a profile mean and standard deviation, a confidence interval for abnormality can be established.[IDSIEEE] This can be viewed as an extension to Threshold measure, where threshold value for such different pattern is calculated based on the Means and SD.
- **Clustering Analysis:**This is non-parametric method which relies on representing event streams as a vector, examples of which are then grouped in to classes of behaviors using some clustering algorithms. These cluster represents the user behaviors or patterns based on which Anomaly can be detected.

Immune System Approach: In this approach application's behaviors are modeled as sequence of system-calls in various conditions such as normal, abnormal, error condition etc. This approach was developed at University of New Mexico, which provides an efficient way to deal with intrusion just as immune system deals with intrusions on human body. This implementation builds a kernel module which has such sequences of system-calls for particular user in most possible situations. This module is responsible of comparing anomalous sequence of system-call generated by user or process. Upon identifying anomaly it can take preventive actions. The UNM approach inserts a predefined amount of delay in system-call execution between system call dispatcher and schedular. If the sequence is identified as normal then the module by-pass control to schedular and normal execution is processed. This approach reduces the false positive by adopting delay mechanism in sequence calls.

The general fact is assumed that majority of security breaches are resulting in abnormal system call execution by kernel level processes. And hence the focus is on the system calls. Though this approach is not effective to build Network Level attacks, it provides quite efficient implementation of System Level(Host)intrusion detection.

3.2 Misuse Detection

Misuse detection attempts to model abnormal behavior. The abnormal behavior is defined as any occurrence which indicates system abuse. Since in this approach the system abuses are defined so clearly which has narrow scope, these systems are highly accurate. The number of false positive and negatives are very less compare to anomaly detection. The abnormal behavior is represented in a pattern called signature. Each known attack should be defined in an accurate signature particular to system, architecture and networking topology. Hence ideally system administrators and hence IDS system itself should be aware of all possible known vulnerabilities and signature of them. Note that the users who slowly modify their activity so that their profiles contain abusive activity are nearly impossible to detect with anomaly detection method.

Hence as summary, this approach analysis information it gathers and compares it to large databases of attack signatures. Essentially the system built on this approach looks for known attack signatures. Though these systems are only as good as the database of the signature is. Hence the major disadvantage of these systems is they are prone to novel attacks. And hence regular update of attack signatures and highly maintenance cost are some of the hindering factors of this approach. Still due to high accuracy it is useful in an environment where the number of possible attacks are limited and the size is maintainable.

4 IDS Functional Blocks

Up to this point major approaches and techniques of IDS are discussed. But this section is more general with respect to its applications and concepts. In general any IDS resides in three different category:

- **Monolithic:** Which has single application acting as complete IDS. Here the architecture is very simple but at same time this approach can not identify with the attack made by distributed events seem to be normal when analyzed with respect to one single system.
- **Hierarchic:** This architecture has evolved in order to identify distributed attack made in networked environment. Here IDS's centralized module co-relates data available from different nodes and analyze logically to detect intrusion.
- **Agent Based:** It is purely distributed in nature. There will not be any centralized control over analysis and data source/sink. This architecture is highly scalable and adapted by many modern IDSs.

Intrusion Detection Systems have evolved from monolithic batch-oriented systems to distributed real-time network of components. In recent systems, a number of common functional building blocks can be distinguished:

- **Sensors:**These modules form the most primitive data gathering components of an IDS. They will be implemented in highly system specific fanion, they track network traffic, log files or system behavior - translating raw data into events usable by IDS monitors.[IDSIEEE]
- **Monitors:**They are main processing components of an IDS, they receive events from Sensors. These events are then correlated against the IDS behavior models, potentially producing model updates and alerts. Alerts, events in themselves, indicate occurrence significant to the security of a system, and may be forwarded to higher level monitors or Resolvers.[IDSIEEE]
- **Resolvers:**Resolver components receive suspicious reports from Monitors and determine the appropriate response - logging, changing the behavior of lower level components, reconfiguring security mechanisms and notifying operators.[IDSIEEE]
- **Controllers:**They are facilitating component configuration and coordination and are most significant in distributed ID systems, where manually starting, updating and configuring network wide series of components will be impossible. In addition controllers provide single point of administration for an IDS.[IDSIEEE]

5 Requirements

This section states some of the general requirements of an ideal IDS systems. They are also major challenges in present development of an IDS.

- **Accuracy:** The accuracy for IDS can be measured in reduced false positives and false negatives. Though false positives are permissible upto certain extent false negative are NOT allowed in any IDS since the implementor will not at all desire to miss potential attack by his IDS. The second measure is the Protocol Analysis, this is significant to Network Based IDS. As attacks including IP spoofing, DNS hijacking and protocol poisoning are common in recent years thorough analysis of Protocols has been added to Accuracy factor of an IDS.
- **Prevention:** Realtime response and AI approaches to profile intelligence are some of the future challenges in IDS development. Today IDS needs to be reconfigurable and integrable with other security tools like firewalls, virus detection.

- **Forensic and Reporting:** IDS reports should me meaningful to security administrators. Forensic analysis is the major requirement of a successful intrusion detection. Actually greater accuracy provides more meaningful forensic and reports of an IDS.
- **Speed:**As Network based IDS needs to adapt against highly dynamic nature of network topology and traffic, the speed-performance is an issue for such tool. Host based IDS suffers more savior challenge in this area where the overhead on system is huge and needs of maintaining profile diabases is significant. Modern IDSs require Wire-Speed as performance satisfaction.

6 Conclusion

IDS is a complex area of study where lot many techniques, approaches and technologies are involved. This report is at introductory level and explores major features of an IDS. Though it will be premature to conclude any absolute opening about an IDS, this report can be concluded with some comments and facts regarding IDS:

- IDS will merge all Network components and tools which exists today, into a complete and co-operative system, dedicated to keeping networks and system stable and secure.
- Future IDSs will be more distributed in nature and will deploy more hierarchical correlation with intelligent analysis.
- Novel technologies like AI or Data-mining will be soon incorporated with IDS implementation.

7 References:

- http://www.securityfocus.com
- http://www.citeseer.com
- “Intrusion Detection Techniques and Approaches” - Theuns Verwoed and Ray Hunt [IDSIEEE]
- “Computer Systems Intrusion Detection - A Survey” - Anita K Johns, Robert S. Seilken
- http://www.insecure.org
- http://nss.co.uk