ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

Intrusion Detection Approach &Tools

Umang G. Waghmare, Dr. G.P. Bhole
Student, Professor
Computer Engineering & Information Technology Department, VJTI College, Mumbai, Maharashtra, India

Abstract*— Wireless Networks have become important technology in the last few years due to the rapid growth in wireless devices. Communication in wireless network takes place over an open medium that is accessible to all users. Wireless medium is available to both legitimate network users and malicious users. Because of the nature of open medium they are more prone to attack. .Because of this, the conventional theories or ways of guarding the network with firewall and encryption is no longer enough and efficient. It is essential to look for new mechanisms to secure wireless network, WIDS (Wireless Intrusion Detection System) is one of them. Intrusion Detection System (IDS) is capable of identifying the attacks, by monitoring the system constantly and look for the suspicious behaviour in the network. Here in this paper we focus on the various IDS tools their working and features/flaws comparing them on the basis of their working criteria, approach towards detection, their reliability for users and organisations as shown in table II.

Index Terms—**Intrusion Detection Tools, Intrusion Detection Systems, Network Security**

I. INTRODUCTION

A field in computer networks that involves securing of computer network infrastructure is Network security which has become more important to personal computer users, organizations, and the military. As the internet is growing, security became a major concern. Knowing the attack methods, allows for the appropriate security to emerge. Many businesses secure themselves from the internet by means of firewalls and encryption mechanisms. The entire field of network security is vast and in an evolutionary stage. In order to understand the research being performed today, background knowledge of the internet, its vulnerabilities, attack methods through the internet, and security technology is important and therefore they are reviewed. Therefore, the traditional way of protecting networks with firewalls and encryption software is no longer sufficient. We need to develop new architecture and mechanisms to protect the wireless networks and mobile computing applications.

Now a day's wireless communication between mobile users is becoming more popular, which is due to recent technological advancement in mobile computers and wireless communication devices, such as wireless modems and Wireless LANs. There are various security requirements to be handled in wireless network such as confidentiality, availability, integrity. The availability and services in ad-hoc network is an important issue to be handled. Because the nodes in wireless ad-hoc network are not necessary to be stationary, they can be mobile so they can act as node or a router that can forward packet from one node to another. Ad-hoc networks can be deployed in places with no infrastructure. This is useful in disaster recovery situations and places with non-existing or damaged communication infrastructure. Because nodes can act as router so the task of forwarding the packet can lead to some malicious actions this issue has to be handled. There are various attacks on the wireless ad-hoc network that must be handled. Some of them are related to the reliability of the wireless communication. As reliability is one of the main concerns in the wireless communication so reactive steps should be taken to detect and reduce them. This work looks at some of these problems and tries to evaluate some of the current tools used to deal with the reliability issues.

II. BACKGROUND

A. *What is an IDS?*

Intrusion Detection Systems (IDS) is a security monitoring system that will gather and analyze data from various areas within a system or network to identify/detect possible intrusions and/or misuse [9]. A security break occurs when there is an unauthorized access to your systems. This unauthorized access is done by illegitimate users. This unauthorized access can be further divided into two primary categories, intrusions and misuse. Intrusions occur when the security breach originates from outside the organization whereas misuse is an attack that originates from the inside, i.e. employees, intruders, etc. This unauthorized access can be for stealing proprietary data or utilizing

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

your systems to play resource intensive role-playing games. Intrusion Detection Systems perform a wide array of functions, which include:

- Monitoring and analyzing both user and system activities,
- Analyzing system configurations and vulnerabilities,
- Assessing system and file integrity,
- Ability to recognize patterns of typical attacks,
- Analysis of abnormal activity patterns, and
- Tracking user policy violations

Traditionally, IDS systems were divided into two classes – network-based and host-based IDS [1]. These two classes of IDS are different from each other which is shown in table I.

B. *Network Intrusion Detection System*

NIDS monitor the network and attempt to detect attacks happening on systems. An attacker attempts to break into system .NIDS utilize rough network packets as its data source for its analysis. A basic example of a monitoring technique is a system monitoring TCP connection requests (SYN) to a wide range of ports on a target machine to determine if someone is attempting a port scan. A NIDS can run on a host machine, while sitting on there it monitors all incoming and outgoing network traffic to that machine or on an independent machine, promiscuously monitoring network traffic. The system can be configured to analyze traffic passing through a network segment to point out patterns which may indicate an attack. These systems provide real-time event monitoring to host. NIDS, generally, are less expensive than but are very different in nature. The NID sensor generally does not monitor activity at the host level. A few reliable network-based intrusion detection systems are described in [1].

C. *Host Based Intrusion Detection System*

Host-based IDS (HIDS) [1], [2], [3] monitor event, and security and system logs at the operating system level. When any of these important file change, the IDS compares the new log entry with attack signatures to see if there is a match. If there is a match, the system will respond with administrator alerts to initiate response procedures. This technology continues to develop, but managing HIDS is simpler. Agents can be installed on multiple hosts and monitored from a central console. HIDS can be critical in determining whether or not an attack was successfully launched. The HID data can also be used should legal matters arise and the altering of data needs to verified.

Table I. Differentiation of NIDS & HIDS

NIDS	HIDS
Monitors network & attempts to detect attacks happening on network	Monitors event & system logs at operating system level.
Near Real time response	Responds after suspicious entry
Not suitable for encrypted & Switches network	Well suited for encrypted & switches environment
Does not perform normally detection of complex attacks	Powerful tool for analyzing a possible attack because of relevant information in database
High False positive rate	Low false positive rate
Better for detecting attacks from outside	Better for detecting attack from inside
Detects network attack, as payload is analyzed	Detects local attack before they hit network

D. *Approaches to ID [4]*

There are multiple approaches to perform intrusion detection. The basic methods are statistical-based intrusion detection (SBID) and rule-based intrusion detection (RBID).

- ***Statistical-Based Intrusion Detection System (SBID) [4]***

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

SBID system identifies security violations by systematically analyzing audit trail data. The system will compare log activity with predicted attack files. This eliminates the need to manually sift through log files to try and identify unusual network traffic or system activity. The system automates this process and will perform this analysis in a structured manner. For this analysis to be effective there must be a preexisting classification of system or user activity that is considered to be normal. This characterization is usually called a profile. This profile is based on a series of events found in system audit data and can be used to configure expected behavior. User profiles can be customized to each user and are maintained dynamically. This allows the user's profile to change as the user's behavior changes. Administrators should be able to review these profiles to ensure that they make sense for their organization. This method of using profiles is not used by RBID's. Statistically significant deviations above the predefined profile are considered intrusion attempts.

- ***Rule-Based Intrusion Detection (RBID) [4]***

RBID systems are considered expert systems that will analyze extensive log files to differentiate between intrusive and normal day-to-day behavior. The system is centered on the assumption that it is possible to identify intrusion attempts based on a specific sequence of user activity that typically resembles activities that lead to system compromises. RBID expert system properties will initiate pre-defined rule sets when log data and system files indicate what appears to be unauthorized activity. These rule sets will attempt to compare patterns in audit data to patterns customarily seen during a penetration attempt. Systems can be configured to alert specified individuals if a penetration is in process or has occurred. The systems can provide details surrounding the alert as well as user specific information of the suspected intruder.

E. IDS Tools

- ***AAFID:***

AAFID is a distributed monitoring and intrusion detection system that employs small stand-alone programs (Agents) to perform monitoring functions in the hosts of a network. AAFID stands for Autonomous Agents for Intrusion Detection, a distributed intrusion detection system. In this architecture, nodes of the ids are arranged in a hierarchical structure in a tree [5]. AAFID is not by itself a network-based intrusion detection system.
Distributed Monitoring The feature of AAFID is that it is a distributed monitoring system which uses number of host for monitoring.
Provides the infrastructure for distributing monitoring It uses number of host for monitoring the network. Some agents may implement network monitoring functions, while others may implement host monitoring functions.
Implemented in Perl 5, which makes it easier to run it in different platforms [6].

- ***AIDE:***

AIDE (Advanced Intrusion Detection Environment) is a file and directory integrity checker. AIDE is an intrusion detection program. It creates a database from the regular expression rules that it finds from the config files. Once this database is initialized it can be used to verify the integrity of the files.
File & Directory Integrity Checker The feature of AIDE is that it is a file and directory integrity checker.
It has several message digest algorithms There are number of message digest algorithms which are used to check the integrity of the file such as: md5, sha1, rmd160, tiger, crc32, sha256, sha512, whirlpool (additionally with libmhash: gost, haval, crc32b) [7].
Supports File Attributes The entire usual file attributes can also be checked for inconsistencies. File has attributes which can also be supported by AIDE which are File type, Permissions, Inode, Uid, Gid, Link name, Size, Block count, Number of links, Mtime, Ctime and Atime.[7]
Simple Database It consist of plain text configuration files and database for simplicity of the files specified in AIDE.conf, AIDE's configuration file. This is mainly useful for security purposes, given that any malicious change which could have happened inside of the system would be reported by Aide.
Powerful regular expression It requires regular expressions which are required to create the database .It support to selectively include or exclude files and directories to be monitored.
Easy Monitoring It is stand alone architecture which is helpful for easy client/server monitoring configurations.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

- ***Deception Toolkit:***

The Deception ToolKit (DTK) is a toolkit designed to give defenders a couple of orders of magnitude advantage over attackers. In a sense that the attacker get deviated from attacking. It uses deceptions as a counterattack to defend the system

Uses deception to counter attack The deception is intended to make it appear to attackers as if the system running. DTK has a large number of widely known vulnerabilities.

DTK's deception is programmable, but it is typically limited to producing output in response to attacker input in such a way as to simulate the behavior of a system which is vulnerable to the attacker method.

Use to create honey pot services sprinkled across servers. Keep attackers wondering if they are hitting a real service or honey pot .It has highly configurable responses and notifications which make it difficult for attackers to go undetected

.

- ***HostSentry:***

HostSentry is a host based intrusion detection tool that performs Login Anomaly Detection (LAD) [7].

Login Anomaly Detection (LAD) This tool allows administrator to spot strange login behavior and quickly respond to compromised accounts and unusual behavior. It works by monitoring interactive login sessions to the computer system and spotting unusual behavior or activity that indicates an intrusion.

Trace suspicious user's activity It also looks for the suspicious user activity, unknown user logins and suspicious login domains, taking measures against compromised accounts and unethical user's behavior.

Incorporates a dynamic database and actually "learns" the user login behavior. This behavior is then utilized by modular signatures to detect unusual events. Login Anomaly Detection It uses a dynamic database and modular signatures to detect misuse and report or react to the events in real-time.

- ***IMSafe:***

ImSafe is a new tool, known as Host-based IDS but the first one to truly implement pure.

Anomaly Detection at the process level The idea behind anomaly detection is that you don't know what an attacker may do to corrupt your system, but you know how your system is supposed to behave in a normal situation. An anomaly detector is simply comparing the actual state of the system with its own knowledge of how the system should behave. Anomaly detection by analyzing audit trails of system calls. Fast detection of Buffer Overflow Attacks through call origin heuristic mechanism

Monitors specific applications: The applications that are potential targets (eg: ftp server). ImSafe traces the system calls of those processes and try to predict the next system call with a certain probability. If the predictions fail to be correct, then an alarm is raised. Monitor multiple processes of one single application at a time .React in real-time to an attack by executing the script of your choices

Monitor the sequence of system calls made by a process; these sequences are stored in a data-base using a tree data structure. It has a high volume of false positive.

- ***Snort:***

Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks. It supports wide range of operating systems such as XP, Linux, and Solaris etc.

Performs The snort has wide range of functionality some of them are it can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks. It allows raw packet data analysis. This allows for examination of a packet down to the payload to determine what caused the alert, why the something caused the alert, and whether action needs to be taken.

Snort uses a flexible rules language Rules are very flexible, easily written, and easily inserted into the rule base. Snort's detection system is based on rules which are based on intruder signature. A rule may be used to generate an alert message, log a message, or, pass the data packet. Snort rules are written in an easy to understand syntax. Most of the rules are written in a single line. Rules are usually placed in a configuration file, typically snort.conf. Snort rules operate on network (IP) layer and transport (TCP/UDP) layer protocols. However there are methods to detect anomalies in data link layer and application layer protocols.

It can use honey pots to find out what intruders are doing and information about their tools and techniques. It has a database of known vulnerabilities that intruders want to exploit. Snort is currently the most popular free network intrusion detection software. The advantages of Snort are numerous. .

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

Snort's flexibility, ease of configuration, and raw packet analysis makes it a powerful intrusion detection tool.

III. CONCLUSION

In this paper we have examined 6 open source ids tools which can detect network and host based attacks. These tools are user friendly and can give appreciable result. These tools are capable to detect known and new attacks on various platforms e.g. Linux, UNIX based platforms, Windows, etc. using statistical and rule based approach as described in table II. By using IDS tools we are able to detect and notify the user that the system is under attack which is the first step towards preventing attacks. By detecting the attack Ids tool helps the user to take further steps to prevent the attack that is why use of Ids tools is growing now a day. Thus the use of the Ids is must along with the firewall.

REFERENCES

[1] Oleg Kachirski, Ratan Guha "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks", Proceeding of the IEEE Workshop on knowledge media Networking (KMN'02) 2002. "Published"

[2] J. Haines, L. Rossey, R. Lippmann, R. Cunningham, "Extending the DARPA Off-Line Intrusion Detection Evaluations", Proceedings of DARPA Information Survivability Conference & Exposition II, Volume: 1, 2001, pp. 35-45. "published"

[3] Y. Zhang and W. Lee, "Intrusion Detection in Wireless Ad-Hoc Networks", Proceedings of the 6th Annual International Conference on Mobile." Published"

[4] Dennis Mathew "Choosing an Intrusion Detection System that Best Suits your Organization", SANS Institute "Unpublished"

[5] http://en.wikipedia.org/wiki/AA

[6] http://www.securityfocus.com/tools/57

[7] http://aide.sourceforge.net/

[8] Importance of Intrusion Detection System(IDS) [International Journal Of Scientific & Engineering Research, Volume 2, Issue1, January-2011] "published"

[9] Intrusion Detection A Brief History & Overview: Richard A. Kemmerer, Reliable Software group Computer Department University Of California Santa Barbara. "unpublished"

AUTHOR BIOGRAPHY

Umang G. Waghmare is pursuing masters in computer science with specialization in network infrastructure management system (NIMS) from VJTI, Mumbai, India. He has completed B.E from RCERT Chandrapur, India in 2010.

Dr. G.P. Bhole is Associate professor in VJTI, Mumbai. He has done M.E in electrical engineering and PhD in electrical engineering. He has 20 years of teaching experience.

APPENDIX

Table II. Comparison of IDS tools

Tools/ Features	Approach	NIDS	HIDS	Monitoring	Platform supported	Attack Detected	Suitability
AAFID	Statistical	YES	Yes	Distributed	Windows NT, Linux, FreeBSD, Open BSD	DOS, File System Attacks	Suitable for detecting suspicious activities in distributed environment in small, medium ,large scale organisation in linux , unix based, and windows platform
AIDE	Rule	No	Yes	Stand Alone	Solaris, Linux, Free BSD, Open BSD, MAC OS	File & Integrity Checker	Suitable for checking integrity of file & directory, mainly useful for security purposes and can be used in small, medium, large scale organisations, is suitable in linux and unix based system.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 2, Issue 4, July 2013

DTK	Statistical	No	Yes	Stand Alone	Free BSD, Open BSD Linux, MAC OS	Resources Exhaust, Port Scanning	Works as a deception to attackers and is suitable in linux and unix based systems. It suits in single user environment.
Host-Sentry	Statistical	No	Yes	Stand Alone	Linux, Free BSD	Unknown user Logins, Suspicious User Activity, Suspicious login Domain	Suitable for detecting login anomaly detection, trace suspicious user activity, monitors interactive login sessions, and reports or reacts in real time in linux. It suits in environment where authentication and authorization is main concern.
ImSafe	Statistical	No	Yes	Stand Alone	Linux, Free BSD, Open BSD	Buffer Overflow Attack	Suitable for buffer overflow attacks and react in real time, for monitoring sequences of system calls, in linux and unix based platforms. It suits in small scale organisation.
Snort	Rule	Yes	No	Stand Alone	Linux, Window, Solaris, Free BSD, MAC OS.	DOS & CGI (Common Gateway Interface) Attacks, Intrusion Attacks, port Scans, SMB (Server Message Block) probes layer3 and above attacks.	Suitable for detecting CGI attacks, SMB probes, OS fingerprinting attempts, performs protocol analysis in Linux, as well as in windows. It is suitable in small, large organizations.