A Review of Log Based Intrusion Detection and Prevention System

Aastha Goswami[#1], **Deepak Singh Rajput**[*2]

[#]*Research Scholar, Computer Technology & Applications*
Gyan Ganga College of Technology, Jabalpur (M.P.),
Rajiv Gandhi Proudyokigi Vishwavidyalaya, Bhopal(M. P.), India
[*]*Professor, Computer Science & Engg.*
Gyan Ganga College of Technology, Jabalpur (M.P.), India
[1]*aasthagoswami02@gmail.com*
[2]*deepakrajput16@gmail.com*

Abstract— **In the recent years, Intrusion Detection materializes the high network security. Thus tries to be the most perfect system to deal with the network security and the intrusions attacks. Monitoring activity of the network and that of threats is the feature of the ideal Intrusion Detection System. Intrusion Detection System is classified on the basis of the source of Data and Model of Intrusion. There are some challenges faced by the Intrusion Detection System. In order to detect these malicious activities, organizations deploys Intrusion Detection and Prevention Systems (IDPSs) in their corporate networks. They generate huge amount of low quality alerts and in different formats when an attack has already taken place. Thus Alert and event correlation is required to preprocess, analyze and correlate the alerts produced by one or more network intrusion detection systems and events generated from different systems and security tools to provide a more concise and high-level view of occurring or attempted intrusion.**

Index Terms—**Intrusion Detection and Prevention, IDPS, Intrusion Alert, Network Security**

I. Introduction

Today, every business is depending on network. Mostly, because of business needs, enterprises and government agencies have developed sophisticated, complex information networks, incorporating technologies as diverse as distributed data storage systems, encryption techniques, remote and wireless access, and web services. For hackers, these well-travelled paths make networks more vulnerable than ever before and with relative little expertise, hackers have significantly impacted the networks of leading brands or government agencies. Cyber-crime is also no longer the prerogative of lone hackers or random attackers. Today disgruntled employees, unethical corporations, even terrorist organizations all look to the internet as a portal to gather sensitive data and instigate economic, social and political disruption. With networks more vulnerable and hackers equipped to cause destruction, it’s no surprise that network attacks are on the rise. In order to robustly protect enterprise and government networks against the complete spectrum of threats and vulnerabilities, all three methodologies of intrusion detection must be employed at a time i.e. Signature Detection, Anomaly Detection, and Denial of service Detection. Also, Intrusion Detection System (IDS) must do more than detect attacks: it should enable accurate detection to prevent attacks from reaching and damaging critical network resources and data. Without this range of detection methods and the performance to accurately prevent attacks many IDS products are no more than a digital Maginot line. From this, it’s clear that enterprises and government agencies need to step up and deliver innovative solutions that effectively protect their networks from malicious attacks and misuse.

Intrusion Detection Systems (IDS), though a new field of research, has attracted significant attention towards itself and presently almost every day more researchers are engaged in this field of work. The current trend for the IDS is to make it possible to detect novel network attacks. The major concern is to make sure that in case of an intrusion attempt, the system is able to detect and to report it. Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defence that protects information systems. There are several reasons that make intrusion detection a necessary part of the entire defence system. First, many traditional systems and applications were developed without security in mind. In other cases, systems and applications were developed to work in a different environment and may become vulnerable when deployed Intrusion detection complements these protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks.

II. ATTACKS DETECTED BY DIFFERENT TYPES OF INTRUSION DETECTION SYSTEM

Scanning Attack: Scanning attacks can be used to assimilate information about the system being attacked. Using scanning techniques, the attacker can gain topology information, types of network traffic allowed through a firewall, active hosts on a network, OS and kernel of hosts on a network, server software running, version numbers of software etc. Using this information, the attacker may launch attacks aimed at more specific exploits. The above was gathered by launching a stealth SYN scan. This scan is called stealth because it never actually completes TCP connections. This technique is often referred to as half open scanning, because the attacker does not open a full TCP connection. The attacker sends a SYN packet, as though you he were opening up a real TCP connection. If the attacker receives a SYN/ACK, this indicates the port is listening. If no response is received, the attacker may assume that the port is closed.

© 2016 JCT. All Rights Reserved

Denial of Service Attack:

There are two main types of denial of service (DoS) attacks: flooding and flaw exploitations. Flooding attacks can often simply implement. For example, one can launch a DoS attack by just using the ping command. This will result in sending the victim an overwhelming number of ping packets. If the attacker has access to greater bandwidth than the victim, this will easily and quickly overwhelm the victim. As another example, a SYN flood attack sends a flood of TCP/SYN packets with a forged source address to a victim. This will cause the victim to open half open TCP connections - the victim will send a TCPSYN/ACK packet and wait for an ACK in response. Since the ACK never comes, the victim eventually will exhaust available resources waiting for ACKs from a nonexistent host.

Penetration Attack:

Penetration attacks contain all attacks which give the unauthorized attacker the ability to gain access to system resources, privileges, or data. One common way for this to happen is by exploiting software flaw. This attack would be considered a penetration attack. Being able to arbitrarily execute code as root easily gives an attacker to whatever system resource imaginable. In addition, this could allow the user to launch other types of attack on this system, or even attack other systems from the compromised system.

2.1 DIFFERENT PROTOCOL ATTACKS:

ICMP is used by the IP layer to send one-way informational messages to a host. There is no authentication in ICMP which leads to attacks using ICMP that can result in a denial of service, or allowing the attacker to intercept packets. There are a few types of attacks that are associated with ICMP shown as follows:

ICMP DOS Attack:

Attacker could use either the ICMP Time exceeded" or "Destination unreachable" messages. Both of these ICMP messages can cause a host to immediately drop a connection. An attacker can make use of this by simply forging one of these ICMP messages, and sending it to one or both of the communicating host s. Their connection will then be broken. The ICMP redirect message is commonly used by gateways when a host has mistakenly assumed the destination is not on the local network. If an attacker forges an ICMP "Redirect" message, it can cause another host to send packets for certain connections through the attacker's host. [2]

Ping of death:

An attacker sends an ICMP echo request packet that's larger than the maximum IP packet size. Since the received ICMP echo request packet is larger than the normal IP packet size, it's fragmented. The target can't reassemble the packets, so the OS crashes or reboots.

ICMP nuke attack:

Nukes send a packet of information that the target OS can't handle, which causes the system to crash.

ICMP PING flood attack:

A broadcast storm of pings overwhelms the target system so it can't respond to legitimate traffic. ARP: ARP maps any network level address (such as IP Address to its corresponding data link address. Some ARP attacks are given below:

ARP flooding

Processing ARP packets consumes system resources. Generally, the size of an ARP table is restricted to guarantee sufficient system memory and searching efficiency. An attacker may send a large number of forged ARP packets with various sender IP addresses to cause an overflow of the ARP table on the victim. Then the victim cannot add valid ARP entries and thus fails to communicate .An attacker may also send a large number of packets with irresolvable destination IP addresses. When the victim keeps trying to resolve the destination IP addresses to forward packets, its CPU will be exhausted.

User spoofing:

An attacker may send a forged ARP packet containing a false IP-to-MAC address binding to a gateway or a host. The forged ARP packet sent from Host A deceives the gateway into adding a false IP-to-MAC address binding of Host B. After that, normal communications between the gateway and Host B are interrupting. In DoS attack target hosts are denied from communicating with each other, or with the Internet. Connection Hijacking and Interception Packet interception is the act in which client can be victimized into getting their connection manipulated in a way that it is possible to take complete control aver .

UDP: UDP uses a simple transmission model without implicit handshaking dialogues for providing reliability, ordering, or data integrity. Thus, UDP provides an unreliable service and datagram may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. Some UDP attacks are describe below:

UDP flood attack:

Similar to ICMP flood attack, UDP flood attack sends a large number of UDP messages to the target in a short time, so that the target gets too busy to transmit the normal network data packets.

Fraggle - A fraggle attack is similar to a smurfing attack with the exception that the User Datagram Protocol (UDP) is used instead of ICMP.

Teardrop - A teardrop type of DoS attack the attack works by sending messages fragmented into multiple UDP packages. Ordinarily the operating system is able to reassemble the packets into a complete message by referencing data in each UDP packet. The teardrop attack works by corrupting the offset data in the UDP packets making it impossible for the system to rebuild the original packets. On systems that are unable to handle this corruption a crash is the most likely outcome of a teardrop attack.

© 2016 JCT. All Rights Reserved

III. CATEGORIZATION OF INTRUSION DETECTION

An intrusion detection system (IDS) reviews all arriving and outbound network activity and recognizes guarded patterns that indicate a network or system attack from someone attempting to break into or compromise a system. Various classifications [5] of the Intrusion Detection System are possible as per the different criteria. Initially the categorization can be done as follows as shown in figure.

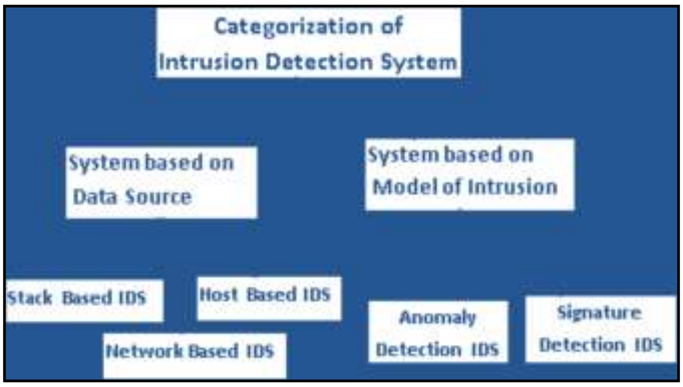
Categorization of Intrusion Detection System
System based on Data Source
System based on Model of Intrusion
Stack Based IDS
Host Based IDS
Network Based IDS
Anomaly Detection IDS
Signature Detection IDS

Fig 1. Categorization of intrusion detection system

A. Stack based Intrusion Detection System (SIDS)

It is latest technology, which works by integrating meticulously with the TCP/IP stack, allowing packets to be watched as they traverse their way up the OSI layers. Watching the packet in this way allows the IDS to pull the packet from the stack before the OS or application has a chance to process the packets.

B. Network Based Intrusion Detection System (NIDS):-

Network based Intrusion Detection System (NIDS) monitors the traffic as it flows to other host. Monitoring criteria for a specific host in the network can be increased or decreased with relative ease. NIDS should be capable of standing against large amount of network traffic to remain effective. As network traffic increases exponentially NIDS must grab all the traffic and analyze in a timely manner.

C. Host Based Intrusion Detection System (HIDS):-

Host based Intrusion Detection System (HIDS) keeps record of the traffic that is originated or is projected to originate on a particular host.. HIDS controls the privileged access of the host to monitor specific components of a host that are not readily accessible to other systems.. HIDS has limited view of entire network topology and they cannot detect attack that is targeted for a host in a network which does not have HIDS installed.

D. Anomaly Based Intrusion Detection System:-

Anomaly based Intrusion Detection System examines ongoing traffic, activity, transactions and behaviour in order to identify intrusions by detecting anomalies. It works on the notion that attack behaviour‖ differs enough from ―normal user behaviour‖ such that it can be detected by cataloguing and identifying the differences involved. The system administrator defines the baseline of normal behaviour. Anomaly-based IDS systems are very prone to a lot of false positives .Anomaly-based IDS systems can cause heavy processing overheads on the computer system.

E. Signature Based Intrusion Detection System:-

Signature based Intrusion Detection System use a set of rule to identify intrusions by watching for patterns of events specific to known and documented attacks. It is typically connected to a large database which stocks attack signatures. These types of systems are able to detect only attacks ―known‖ to its database. Thus, if the database is not updated with regularly, new attacks could slide through. Signature based IDS‘s affect performance when intrusion patterns match several attack signatures. In such cases, there is a noticeable performance lag. Signature definitions stored in the database need to be specific so that variations on known attacks are not missed. This can lead in building huge databases which eat up a chunk of space.

IV. KEY FEATURES OF INSTRUSION DETECTION SYSTEM

Key feature of intrusion detection system is ability to provide a view of unusual activity and issue alerts notifying administrators and/or a block suspected connection. Prevent intrusion with firewall, network port security, systrace (process jail). Simulation software, Monitoring data, security logs or action on network. Analyze to ascertain whether it is an attack. Detect attack or intruder using some scheme. Report Intrusion to system administrator. Act on or defend computer system and possibly repel the attack.

A. Host-Based Intrusion Detection

Specific and have more detailed signatures. They can reduce false positive rates. They can determine whether or not an alarm may impact that specific system. They are application specific. Operates in encrypted environment. Detects local attacks before they hit the network. Powerful tool for analysing a possible attack because of relevant information in database . Require no additional hardware. Better for detecting attacks from inside and detect attacks that network-based IDS would miss.

B. Network-Based Intrusion Detection

Can get information quickly without any reconfiguration of computers or need to redirect logging mechanism. Does not affect network or data resources. Monitor or detects in real time network attacks or misuses. Does not create system overhead. Broad in scope. Examines packet headers and entire packet. No overload. Lower cost of ownership. Better for detecting attacks from outside and detect attacks that host-based Intrusion detection would miss.

V. STRUCTURE AND ARCHITECTURE

An intrusion detection systems always has its core element - a sensor (an analysis engine) that is responsible for detecting intrusions.. Sensors receive raw data from three major information sources (Figure.1):

i. Own IDS knowledge base,

ii. Syslog and

iii. Audit trails.

The syslog may include, for example, configuration of file system, user authorizations etc. This information creates the basis for a further decision-making process. The sensor is integrated with the component responsible for data collection

(Fig.2) — an event generator. The collection manner is determined by the event generator policy that defines the filtering mode of event notification information. The event generator (operating system, network, application) produces a policy-consistent set of events that may be a log (or audit) of system events, or network packets.

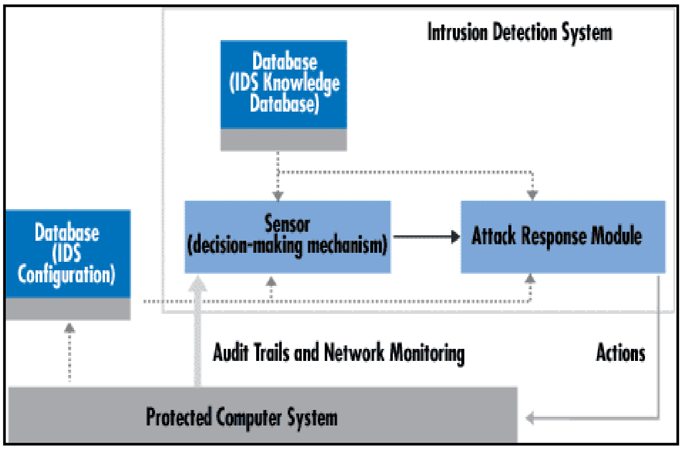
Intrusion Detection System
Database (IDS Knowledge Database)
Database (IDS Configuration)
Sensor (decision-making mechanism)
Attack Response Module
Audit Trails and Network Monitoring
Actions
Protected Computer System

Fig 2. A sample ids. the arrow width is proportional to the amount of information flowing between system components

The role of the sensor is to filter information and discard any irrelevant data obtained from the event set associated with the protected system, thereby detecting suspicious activities. The analyzer uses the detection policy database for this purpose. In addition, the database holds IDS configuration parameters, including modes of communication with the response module. The sensor also has its own database containing the dynamic history of potential complex.

A. Working of Intrusion Detection System

The working of the intrusion detection system is quite similar as that of the other programs used to prevent the computer system from dangerous threats like malware, spyware, spam and many more. The job of the intrusion detection system starts from the recording the information about the problem and check the occurrence and the nature of the threat. When the system monitors the problem and collects the data about it, then it sends this information to the administration department of the intrusion detection system which makes several preventive measures to protect the system and keep the system in the safe hands. Intrusion detection system can work in the specific manner by monitoring some important things. These important things are as follows.

1. Monitoring the activity of the network and activity of the threat in the network.
2. This system has ability to detect the viruses, malware, spyware and different form of viruses and the important thing about this it can also locate their restore point.
3. Intrusion detection system can work by observing the unauthenticated and unauthorized use of different programs of networking.

So, the whole working of the intrusion detection system based on the examination of such events of networking.

B. Ideal Intrusion Detection System

An ideal intrusion detection system [1] should address the following issues, regardless of mechanism it is based on:

1. The system must run continually without human supervision. It must be reliable enough to allow it to run in the background of the system being observed.
2. It should not be a "black box". That is, its internal workings should be examinable from outside.
3. It must be fault tolerant in the sense that it must survive a system crash and not have its knowledge-base rebuilt at restart.
4. It must resist subversion. The system can monitor itself to ensure that it has not been subverted.
5. It must impose minimal overhead on the system. A system that slows a computer to a crawl will simply not be used.
6. It must observe deviations from normal behaviour.
7. It must be easily tailored to the system. Every system has a different usage pattern, and the defence mechanism should adapt easily to these patterns.
8. It must deal with changing system behaviour over time as new applications are being added. The system profile will change over time.
9. It must be difficult to fool.

All the above listed are the features that an ideal Intrusion Detection System must have. So that the system becomes perfect to defend the attacks and the intrusions.

VI. CONCLUSION

An intrusion detection system is a crucial part of the defensive operations that complements the static defences such as firewalls. Essentially, intrusion detection systems search for signs of an attack and flag when an intrusion is detected. In some cases they may take an action to stop the attack by closing the connection or report the incident for further analysis by network administrators. According to the detection methodology, intrusion detection systems are typically categorized as misuse detection and anomaly detection systems. From a deployment perspective, they are be classified as network based or host based although such distinction is coming to an end in today's intrusion detection systems where information is collected from both network and host resources. In terms of performance, an intrusion detection system becomes more accurate as it detects more attacks and raises fewer false alarms. Future advances in IDS are likely to continue to integrate more information from multiple sources (sensor fusion) whilst making further use of artificial intelligence to minimize the size of log files necessary to support signature databases.

REFERENCES

1. Modi CN, Patel DR, Patel A, Rajarajan M. Integrating signature apriori based Network Intrusion Detection System (NIDS) in cloud computing. Procedia Technology. 2012; 6:905–12.
2. Wang SS, Yan K-Q, Wang S-C, Liu C-W. An integrated intrusion detection system for cluster-based wireless sensor networks. Expert Systems with Applications. 2011; 38(12):15234–43.
3. Chung CJ, Khatkar P, Xing T, Lee J. NICE network intrusion detection and countermeasure selection in virtual network system. IEEE Transactions on Dependable and Secure Computing. 2013; 10(4):198–11.

4. Feng W, Zhang Q, Hu G, Huang JX. Mining network data for intrusion detection through combining SVMs with ant colony networks. Future Generation Computer Systems. 2014; 37:127–40.
5. Amudhavel J, et al. An robust recursive ant colony optimization strategy in VANET for accident avoidance (RACO-VANET). International Conference on Circuit, Power and Computing Technologies (ICCPCT); Nagercoil. 2015. p. 1–6.
6. Amudhavel J, et al. A krill herd optimization based fault tolerance strategy in MANETs for dynamic mobility. International Conference on Circuit, Power and Computing Technologies (ICCPCT); Nagercoil. 2015. p. 1–7.
7. Amudhavel J, Prabu U, Dhavachelvan P, Moganarangan N, Ravishankar V, Baskaran R. Non-homogeneous hidden Markov model approach for load balancing in web server farms (NH2M2-WSF). Global Conference on Communication Technologies; Thuckalay. 2015. p. 843–5.
8. Elhag S, Fernández A, Bawakid A, Alshomrani S, Herrera F. On the combination of genetic fuzzy systems and pairwise learning for improving detection rates on Intrusion Detection Systems. Expert Systems with Applications. 2014; 42(1):193–202.
9. Mamalakis G, Diou C, Symeonidis AL,Georgiadis L. Of daemons and men: A file system approach towards intrusion detection. Applied Soft Computing. 2014; 25:1–14.
10. Moraes F, Abdelouahab Z, Lopes D, Oliveira E, Teixeira C, Labidi S, Teles A. Advances in self-security of agent-based intrusion detection systems. Emerging Trends in ICT Security; 2014. p. 153–71.
11. Shen X J, Liu L, Zha Z-J, Gu P-Y, Jiang Z-Q, Chen J-M, Panneerselvam J. Achieving dynamic load balancing through mobile agents in small world P2P networks. Computer Networks. 2014; 75(Part A):134–48.
12. Xia J, Luo B. A novel intrusion detection system based on feature generation with visualization strategy. Expert Systems with Applications. 2014; 41(9):4139–47.

© 2016 JCT. All Rights Reserved