RESEARCH ARTICLE OPEN ACCESS

Intrusion Detection System: Security Monitoring System

ShabnamNoorani, Sharmila Gaikwad Rathod

Abstract
An intrusion detection system (IDS) is an ad hoc security solution to protect flawed computer systems. It works like a burglar alarm that goes off if someone tampers with or manages to get past other security mechanisms such as authentication mechanisms and firewalls. An Intrusion Detection System (IDS) is a device or a software application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station.Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from this malicious or abnormal activity..In this paper we are comparing host based and network based IDS and various types of attacks possible on IDS.

Keywords: IDS, SYN/ACK, DOS, TCP, UDP.

I. INTRODUCTION

An intrusion detection system (IDS) is an ad hoc security solution to protectflawed computer systems. It works like a burglar alarm that goes off if someone tampers with or manages to get past other security mechanisms such as authenticationmechanisms and firewalls.The major tasks of an IDS are to collect data from a computer system, analyse these data to find security relevant events, and present the results to the administrator.More or less automatic response mechanisms may also be built into the system. An Intrusion Detection System (IDS) is a device or asoftware application that monitors network or system activities for malicious activities or policy violations and produces reports to a management station. Intrusiondetection systems constantly monitor a given computer network for invasion or abnormal activity. Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from this malicious or abnormal activity. 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 With the ability to analyze network traffic and recognize incoming and ongoing network attack, majority of network administrator has turn to IDS to help them in detecting anomalies in network traffic.

II. ARCHITECTURE

The proposed approach has the following three phases:

1) Data pre-processing: Convert raw data to machine readable form.
2) Training: In this phase the network will be trained on normal and attack data
3) Testing: Activity will be predict i.e. either intrusive or not.

Figure.1. depicts the architecture of the proposed approach.

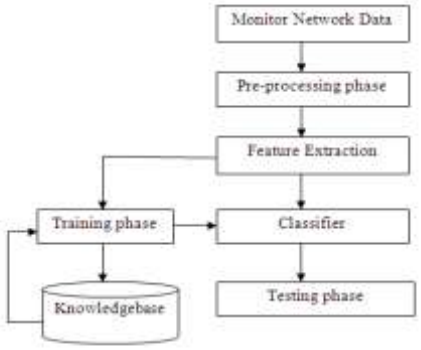

Figure1:Architecture of IDS

The architecture has following modules.

Network Data Monitoring: This module will monitor network stream and capture packets to serve for the data source of the NIDS

Pre-processing:

In pre-processing phase, network traffic will be collected and processed for use as input to the system.

Feature Extraction:

This module will extract feature vector from the network packets (connection records) and will submit the feature vector to the classifier module. The feature extraction process consists of feature construction and feature selection. The quality of feature construction and feature selection algorithms is one of the most important factors that influence the effectiveness of IDS. Achieving reduction of the number of relevant traffic features without negative impact on classification accuracy is a goal that largely improves the overall effectiveness of the IDS

Classifier:

This module will analyse the network stream and will draw a conclusion whether intrusion happens or not. BPN and ELM techniques can be used as a classifier. The most successful application of neural network is classification or categorization and pattern recognition.

Training:

The learning process is the process of optimization in which the parameters of the best set of connection coefficients (weighs) for solving a problem are found

Testing:

When detecting that intrusion happens, this module will send a warning message to the user.

Knowledgebase:

This module will serve for the training samples of the classifier phase. The Artificial Neural Networks can work effectively only when it has been trained correctly and sufficiently.

III. HOST BASED AND NETWORK BASED IDS

There are two types of intrusion detection systems: host-based and network-based.

Network based IDS: These types of IDS are strategically positioned in a network to detect any attack on the hosts of that network. To capture all the data passing through the network, you need to position your IDS at the entry and exit point of data from your network to the outside world. You can also position some IDS near the strategic positions of your internal network, depending on the level of security needed in your network. Since a network based IDS need to monitor all the data passing through the network, it needs to be very fast to analyze the traffic and should drop as little traffic as possible.

Depending on how they function, network based IDS can be divided into two types:

a)Statistical anomaly IDS
b)Pattern matching IDS

In statistical based IDS model, the IDS try to find out users' or system's behavior that seem abnormal. Actually, IDS make a profile of every user and system during the normal operation time. When the deviation of this normal behavior is detected the IDS trigger its alarm for intrusion. One of the main advantages of this type of IDS is that they can detect the type of intrusion that has no records of its previous occurrence. In that sense, statistical anomaly can detect new type of attack patterns. A large number of false alarms are the main problem with this system.

In pattern based system, the IDS maintain a database of known exploits and their attack pattern. During the analysis of network packets if it finds any pattern match to one of those known attack patterns then it triggers alarm. For operation of this type of IDS need to analyze every packet in the network to look for known attack patterns. Since this type of IDS mainly looks for patterns they have a very quick deploy and implementation time, unlike statistical based IDS. Another advantage is that they produce less number of false positives.

The main problem with pattern based IDS is that they cannot detect anything that is unknown to them or that of which they have no data in their pattern matching database. Since there are many network based exploits coming on each month, the need to be updated frequently.

Table1 shows the camparison of ststistical IDS and Pattern IDS.

Table1: Comparison of Statistical IDS and Pattern IDS

Statistical IDS	**Pattern IDS**
In statistical based IDS model, the IDS try to find out users' or system's behavior that seem abnormal	In pattern based system, the IDS maintain a database of known exploits and their attack pattern.
When the deviation of this normal behavior is detected the IDS trigger its alarm for intrusion	During the analysis of network packets if it finds any pattern match to one of those known attack patterns then it triggers alarm.
A large number of false alarms are the main problem with this system.	The main problem with pattern based IDS is that they cannot detect anything that is unknown to them or that of which they have no data in their pattern matching database.
The main advantages of this type of IDS are that they can detect the type of intrusion that has no records of its previous occurrence.	The main advantage is that they produce less number of false positives.

Host based IDS: Host based IDS are installed in a host and they can monitor traffics that are originating and coming to that particular hosts only. If there are attacks in any other part of the network, they will not be detected by the host based IDS .Apart from monitoring incoming and outgoing traffic, a host based IDS can also analysis the file system of a host, users' logon activities, running processes , data integrity etc.

Some of the advantages of this type of IDS are:

1) They are capable of verifying if an attack was successful or not, whereas a network based IDS only give an alert of the attack.
2) They can monitor all users' activities which is not possible in a network based system

They are capable of identifying attacks that originate from inside the host.

3) A host based system can analyze the decrypted traffic to find attack signature-thus giving them the ability to monitor encrypted traffic.
4) They do not require any extra hardware since they can be installed in the existing host servers.
5) They are cost effective for a small scale network having a few hosts.

The main disadvantages of this system are they can be compromised as soon as the host server is compromised by an attack. In addition, they eat up extra computing power from the host where it resides. They can be ineffective during the denial of service attacks.

However, there are many differences betweenthe two. While their roots are similar, their operational use is different. Intrusiondetection is based on analyzing a set of discrete, time-sequenced events for patterns ofmisuse. Intrusion detection sources both network-based and host-based, are sequentialrecords that reflect specific actions and indirectly reflect behavior. Host-basedtechnology examines events like what files were accessed and what applications wereexecuted. Network-based technology examines events as packets of informationexchange between computers (network traffic).Intrusion detection is network-based when the system is used to analyze networkpackets. This is in contrast to host-based intrusion detection, which relates to processingdata that originates on computers themselves, such as event and kernel logs. Networkpackets are usually "sniffed" off the network, although they can derive from the output ofswitches and routers. The most common protocol targeted is TCP/IP. Network sourcesare unique because of their proximity to unauthenticated, or outside, users. They arepositioned to detect access attempts and denial of service attempts originating outside thenetwork.There are many attack scenarios that would not be detected by host-basedtechnology, thereby highlighting the differences between the two. Unauthorized accessoccurs when an outsider comes in over the network and logs into the system uninvited.This can be detected by host-based systems once the attacker is inside, but the ultimategoal is to detect them before they get access, or during the process of getting access.Another scenario is password downloads. Unauthorized password file downloads givesattackers the ability to attack other systems. The Network Security Monitor, one of thefirst network intrusion detection systems looked for the pattern "/etc/passwd" in FTPtraffic outbound from the network.

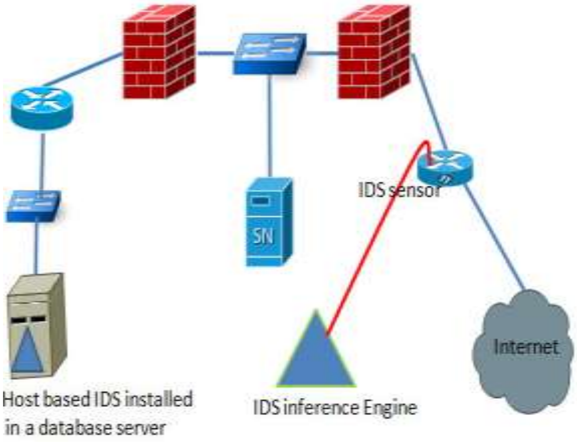

Figure 2:Network based IDS

Table 2.Comparision between Host Based and N/w Based IDS

Host based IDS	Network based IDS
Host-basedtechnology examines events like what files were accessed and what applications wereexecuted.	Network-based technology examines events as packets of informationexchange between computers (network traffic).
A host-based system analyzes logs and consists of information regarding the status of your system	A network-based system analyzes a network traffic directly, thus checking every network event.
while you are off your LAN, only a host-based system will offer protection.	While off your LAN,noprotection.
A host-based system does not requires specific training like NIDS	A network based system requires training.
HIDS does not utilize LAN bandwidth	NIDS utilize the LAN bandwidth.
For a host-based system enabling of port spanning is not required for scanning LAN traffic	For a network-based system enabling of port spanning is required for scanning LAN traffic
For cross platforms HIDS offers weak adaptability.	For cross platforms NIDS offers better adaptability as compared to a host-based system.
Personal area networks are scanned by a host-based system only	Personal area networks cannot be scanned by a network-based system.

In case of packet rejection host-based system will not perform	In case of packet rejection only network-based system will perform
Strong deterrence for insiders	Strong deterrence for outsiders
Strong insider detection and weak outsider detection	Strong outsider detection and weak insider detection.
Good at detecting suspicious behaviour.	Weak at detecting suspicious behaviour

IV. 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.

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 avictim. 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 attackswhich give the unauthorized attacker the ability to gainaccess to system resources, privileges, or data. Onecommon way for this to happen is by exploiting a software flaw. This attack would be considered 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.

V. DIFFERENT PROTOCOL ATTACKS

ICMP: 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 hosts. 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 forcertain connections through the attacker's host.

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'treassemble 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 ping sover whelms 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 AR Pattack 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 anover flow 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 agate way 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 inter rupting. 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 with outimplicit handshaking dialogues for providing reliabilityordering, or data integrity. Thus, UDP provides anunreliable service and datagram may arrive out of order,appear duplicated, or go missing without notice. UDPassumes that error checking and correction is either notnecessary or performed in the application, avoiding theoverhead of such processing at the network interfacelevel.Some UDP attacks are describe below :

UDP flood attack: Similar to ICMP flood attack, UDPflood attack sends a large number of UDP messages to thetarget 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.

VI. CONCLUSION

In this paper study the different types attacks comparing host based and network based IDS and various types of attacks possible on IDS. Also study the different type protocol attack like ARP, UDP, Teardrop, fraggle.

REFERENCES

[1] Danny Rozenlum,” Understanding Intrusion Detection System” SANS Institute Reading Room site

[2] K. Rajasekhar, B. Sekhar Babu, P. Lakshmi Prasanna, D. R Lavanya, T.Vasmi Krishna,” An Overview of Intrusion Detection System”

[3] Roshani Gaidhane, C.Vaidya, M. Raghuwanshi” Survey: Learning Techniques for Intrusion Detection System”.

[4] Mahak Chowdhary, Shrutika Suri, Mansi Bhutani” Camparative Study of Intrusion Detection System”.