Research article Available online www.ijsrr.org ISSN: 2279–0543

International Journal of Scientific Research and Reviews

Architecture of Host Based Intrusion Detection System for Detecting Malicious Attacks

Barve Sayali N., Deshpande Ashlesha V.*, Oka Rutuja S.*, Bankapure Niharika N., Barde Saudagar S.

Computer Department, Smt. Kashibai Navale College of Engineering, Vadgaon Bk. Pune, INDIA

ABSTRACT

With the ever increasing computing and communication resources there is also a striking increase in the number of attacks on these resources. It has become a rudimentary necessity to ensure the security in the field of network computation. Intrusion detection system (IDS) deals with these attacks by identifying, analysing and sending the data to hampered system. In this paper, we have designed the architecture and implemented a Host-Based Intrusion detection system. Our architecture builds a signature based intrusion detection system which is able to scan the incoming packets and sends a message to the host system if malicious packets are discovered. The architecture can be upgraded and re-defined as per convenience is a advantageous factor.

KEYWORDS:

MITM(Man in the middle), IDS(Intrusion detection system), DOS(Denial of service).

GENERAL TERMS

HIDS, Intrusion detection system, network security, network packets, database, DoS.

*Corresponding Author 1 -

Ashlesha Deshpande

27-B Anandvan Residency, Anandnagar,

Sinhgad Road, Pune – 411051

E Mail - official.ashlesha@gmail.com

Mob. No. - 8007775082

*Corresponding Author 2 -

Rutuja Oka

'OM' Bungalow, Swati society, Plot no. 23, Dhankwadi, Pune - 411043

E Mail - rutujaoka@gmail.com

Mob. No. – 8793490405

1. INTRODUCTION

Computers have become a integral part of daily lives and consequently our personal data is at great risk. The risk is higher when a network is under attack. Any type of attack, passive or active, equally hampers the machine. The attacker can modify the data, steal the crucial data for financial and personal reasons. Various measures have been taken so as to control these types of attacks. But to control such attacks the machine must be able to detect the attacks.

Intrusion detection system plays exactly this role of detecting if the machine is sacrificed or not.

Intrusion detection what truly does is that it scans the incoming network packets. Then it matches them with fixed patterns of well-known attacks. Then the machine is alerted if the attack has taken place. The system is able to find the IP Address of the attacker machine if it is present in the network. Different companies have architectures and setups and might have specific attacks they have to deal with. So these companies might want to develop their own intrusion detection systems. Taking this thought forward we, the authors of this paper are going to develop a architecture, an open source project which might be further developed by anyone however way they wish for and whatever purpose.

This paper focuses on a host based intrusion detection system which is specific to a machine in a network. The main advantage of Host based IDS is that it can particularly monitor file system integrity, network packets interacting with host, system log files, system registry and host access.

2. MOTIVATION

Firewalls are hardware or software systems placed in between two or more computer networks to stop the committed attacks, by isolating these networks using the rules and policies determined for them. We know that firewalls alone are not enough to secure a network completely because the attacks happening from the outer world of the network are stopped easily but internal hosts are still not secure. This is the situation where intrusions detection systems are in charge. IDSs are used in order to stop attacks, recover from them with the minimum loss or analyze the security problems so that they are not repeated.

On the other hand with the recent advances in technology, people are sharing more and more information among each other. Some organizations like medicine, military etc. are sharing data which is highly sensitive and important. For safe communication, people are using secret key, so that only authenticated receiver can decrypt the message and authenticity of message remains intact. But intruders are not interested to decrypt message. They can use various tools to attack the system on the network and get access to the confidential data. Here, IDS comes as a savior.

IDS provide three important security functions of monitoring, detecting and responding to unauthorized activities.

3. MATERIALS AND METHODS

a. Types Of Attacks

i. Man In The Middle

It's an eavesdropping cyberattack, in which a conversation is going on between two parties and a malicious attacker comes in between these parties as a proxy, impersonates both parties and gains control over the information that the two parties were trying to communicate between themselves. A MITM attack allows a fradulent attacker to trap, send and receive data meant for someone else, or not meant to be sent at all. Both the parties are not aware of this trap set by the intruder. A MITM attack exploits the real-time processing of sharing of data, communication, conversations or transfer of other data. Man-in-the-middle attacks allow attackers to intercept, send and receive data never meant to be for them without either outside party knowing until it is too late.

ii. DOS

In cyber computing, a denial-of-service attack (DoS attack) is a cyber-attack where the services of a host are disrupted temporarily or indefinitely by a perpetrator, who tries to make a machine or network resource unavailable to its supposed users. The target machine or network resource is flooded with superfluous requests. This is done in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.This is the typical methodology in which this Denial of Service works.

iii. Ping Of Death

In this type of attack, by sending malformed or oversized packets using a simple ping command, an attacker attempts to crash, destabilise, or freeze the targeted computer or service. This simple attack is Ping of Death. The size of a correctly-formed IPv4 packet including the IP header is 65,535 bytes. By sending a ping packet larger than 65,535 bytes, the Internet Protocol is violated. When the target system tries to reassemble the fragments, oversized packets are acquired also memory overflow could occur. Hence, it leads to various system problems.

iv. Port Scanning

Ports are entry points for a system. Most packets leaving thesystem come out of a port. They are actually destined for another port on another system.Various services listen on certain well-known ports. An attacker launches a port scan tosee which ports are free to scan. This is done be listening services on the port. A port scan attack occurswhen an attacker sends packets to the system, changing the destination port. The attacker canuse this to find out what all is going on in the system and to get a clear idea of the operatingsystem on the machine. Most Internet sites get a dozen or more port scans per day. This attack can be very harmful and cause confidential data leak very easily.

b. Requirements

Hardware Requirements - CPU Speed 2 GHz, RAM 3 GB.

Software Requirements - Wireshark(tshark/Pyshark interface), Django/Flask(HTML, CSS, JS), tkinter.

Operating System - Linux.

Programming Language - Shell scripting and python.

Database - File based data dump, SQL.

Editor - vim/Pycharm/Sublime

c. System Architecture

As it can be seen from diagram below, the main components are -

Sniffer

Packets Database

Analyser

Reactor

The sniffer used here is ”tshark”, command line version of wireshark, which sniffs the whole network traffic and logs it in files. Then a SQL database is used to store all the packets column wise, this makes overall analysis easy and ecient. The analyser module consist of IDS and a central SQL database.IDS is core part of this system, as it contains all detection modules which constantly monitors the trafficfor abnormal activities and alerts the admin if such activity is detected. Otherwise it simply let the packets pass. The reactor

module consist of alarming and tracking systems. Whenever any suspicious activity is detected an alarm will be generated and tracking system will track the attackers location.

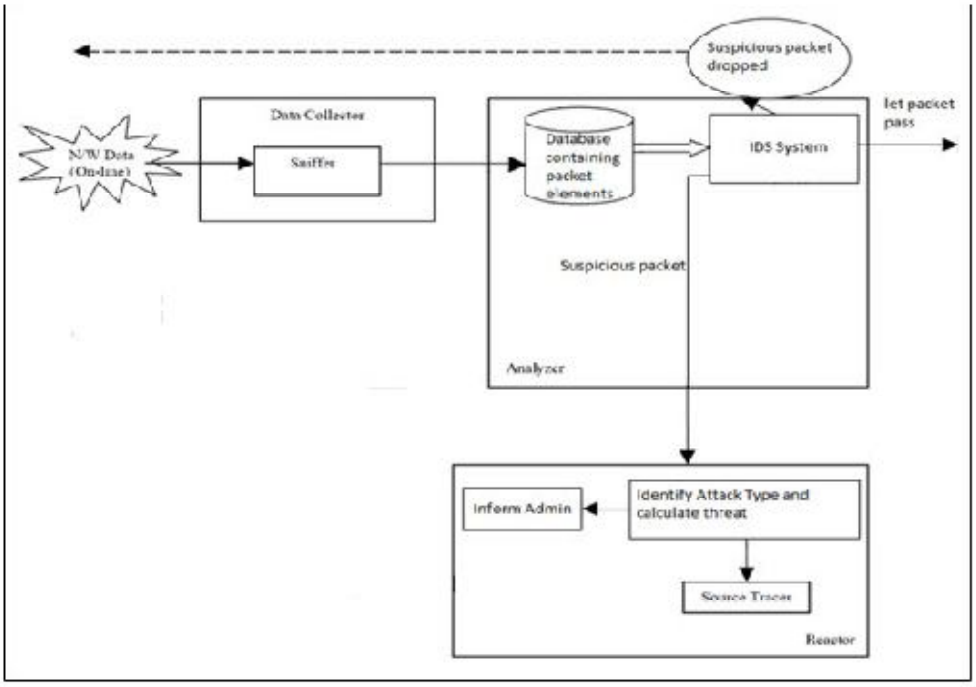

Figure No.1 : "Architecture Diagram"

d. Working

Tkinter will provide a pop up module to run the executable for detecting attacks. If any suspicious activities occur or the host is under attack an immediate email will be sent to the network administrator. This provides almost real time detection of attacks. This attcked will be automatically killed by the HIDS. For further details and analysis of the system the administrator can visit the statistics dashboard for details summary of attacks. This UI will provide Graph based and text based summaries for easy an better understanding. This is possible due to the up to date database maintained by the system. Real time traffic analysis can be done from the UI which provodes line monitoring. This data is obtained from wire shark, which is a reliable and stable source. Hence, the system provides monitoring of a system, detection of attacks, reporting of any problems, dashboard for analysis of traffic from and into the system.

4. BENEFITS

It can detect attacks that are not detected by a NIDS. It has the functionality to provide information about a host during an attack to the admin. Since a HIDS uses system log events that have actually occurred, they can determine whether an attack occurred or not.It detects attacks that a network based IDS fail to detect: Host based systems can detect attacks that network based IDS fail at. Almost real time detection- Although host based IDS does not offer true real-time response, it can comes very close if implemented properly. It has lower entry cost Statistics UI board for analysis of real time traffic on the host.

5. LIMITATIONS

Security of Intrusion Detection System needs to be taken into consideration.Complex systems are another area where anomaly detection is trending more and more applicability. When an OS is brought down by an attack, the HIDS goes down with the system.

6. FUTURE SCOPE

Self learning machine/system to automatically add new patterns to the existing database. Combining this HIDS with any NIDS to extent the scope and develop a complete IDS this will provide overall security to the network as well as individually to systems in that network.

7. RESULTS

We have discussed several different ways in which the problem of anomaly detection has been formulated and have attempted to provide an overview of various techniques. The system looks for the attack signatures and matches it with the known attack signatures from the database and alerts the admin if match is found otherwise simply let the packet pass. Live network monitoring can be done using the (statistics webpage) UI provided. The admin is provided with complete visibility of the network which keeps the admin aware of all the activities going on in the network. In this way a successful intrusion detection can be achieved and all the intellectual information of a user can be kept safe in a network.

8. CONCLUSION

We have discussed severaldifferent ways in which the problem of anomaly detection has been formulated and have attempted to provide an overview of various techniques.The system

looks for the attack signatures and matches it with the known attack signatures from the database and alerts the admin if match is found otherwise simply let the packet pass. Also the admin is provided with complete visibility of the network which keeps the admin aware of all the activities going on in the network. In this way a successful intrusion detection can be achieved and all the intellectual information of a user can be kept safe in a network. This system not only allows a reader to understand the motivation behind using a particular anomaly detection technique, but also ensures a qualified analysis of various techniques.

9. ACKNOWLEDGEMENT

We are grateful to Prof.S.S BARDE for his expert guidance and continuous motivation throughout to see that this project fulfills its target from its start to its completion.

10.REFERENCES

1. Reeder, Paul "Intrusion Detection, The Next Generation: Making it Practical" IETF-IDWG , 2001;
2. Ranum, Marcus J. "Coverage in Intrusion Detection Systems" 6 June 2001;
3. Yocom, Betsy and Brown, Kevin "Intrusion Battleground Evolves" 8 Oct.2001;
4. Northcutt, Stephen and Novak, Judy Network Intrusion Detection An Analyst's Handbook Second Edition New Riders 2001;203-213.
5. Brenda McAnderson & Paul Ramstedt "IDS: Today & Tomorrow" 18 Nov. 1999;
6. Tanase, Matthew "The Future of IDS" 4 Dec. 2001;
7. ITL Bulletin "Acquiring and Deploying Intrusion Detection Systems" Nov. 1999;
8. Messmer, Ellen "Intrusion Alert" 3 Dec. 2001;
9. Langkawi, Development of host based Intrusion detection system for Log _les. IEEE Symposium on Business, Engineering and Industrial Applications (IS-BEIA), Malaysia,2011;
10. Bro: A System for Detecting Network Intruders in Real-Time. 7th USENIX Security Symposium San Antonio, Texas,1998;
11. HSNORT: A Hybrid Intrusion Detection System using Arti_cial Intelligence with Snort. IJCTA| May-June 2013;
12. Darmstadt, Framework for Real-Time Worm Attack Detection and Backbone Monitoring. IWCIP 2005, Germany, 2005;