Case Study on JAVA based IDS

Dr. Sameer Shrivastava

Abstract - Hacking and intrusion incidents are growing terrifyingly every year with the roll out of new technology. Nothing can hide in today's digitally connected world. One can be traced on DNS, NSlookup, Newsgroups, web site trawling, e-mail properties etc. In our project, we tried our hand on designing of an Intrusion Detection System (IDS) that shall implement pre-defined algorithms for identification of attacks over a network. Java programming language has been used for the development, JPCap shall be used to provide access to the winpcap. Online capture of packets shall be done on the network i.e., the one coming on the interface of the network. The systems that are directly or indirectly connected on the Internet can be secured by using the IDS designed.

Index Terms – CaseStudy, IDS, JAVA, Security.

1. INTRODUCTION

Almost all companies and institutions are worried about the security of their network. All the intruders are searching new ways to break the privacy of everyone. Even though there is development in the field of filtration of intrusion to the infrastructure of the network via the Internet but the network is not yet safe.

But IDS is a comparatively new technology for intrusion detection methods that came forward in recent years. To prepare and deal with the network attacks is the main role of Intrusion detection system.

Anyone if tries to break into or misuse the system then it is called an intrusion. Stealing confidential data or misusing your email system for spam both comes under the category of "misuse". The concept of Global village has taken its origin with the coming out of Internet and the World Wide Web. Any kind of information is virtually easy to achieve any on the internet. Networking computers and associated devices are an advantage for this, and are in rapid progress. The intruders and people who provide security to the systems in networks are in race with each other. Our project can be hosted on the client to assist the administrator in detection of several intrusion attacks and inform the owner of the system and also provide security by blocking the malicious users based on their IP addresses.

2. NETWORK INTRUSION

Network Intrusion is a planned attempt to enter a network breaking the security and confidentiality of the information present in the systems of the network, and the person carrying out this is called as an Intruder. The network administrator is believed to defend his network from such persons and this software can help his in his efforts.

Dr. Sameer Shrivastava is an Associate professor in the Department of Computer Science and Engineering, in Global Nature Care Sangathan group of institutions, Jabalpur, M.P. India. He received his Ph.D. (Computer Science and Engineering) from Bhagwant University, Ajmer, Rajasthan in 2011. He has 14+ years of experience in teaching and research. His areas of specialization include Network Security. He is a Cisco Certified Network Associate, SUN certified and Microsoft Certified Professional. He has published papers in many International and national level Journals on Network Security and Computer Networks

2.1 Intrusion detection systems (IDS)

A system responsible for detecting abnormal, inappropriate, or other data that may be considered illegal occurring on a network is an IDS. An IDS is subject to capture and inspect the traffic, despite of whether it's permitted or not. An alert is generated, based on the contents, at either the IP or application level.

2.2 Categories of Intrusion Detection System

IDS can be classified into three categories: signature based detection systems, anomaly based detection systems and specification based detection systems.

2.2.1 Signature Based Detection Systems

Signature based detection system are effective against known attacks, and get updated from new patterns or else will be ineffective in case of unknown previous threats or new releases.

2.2.2 Anomaly based Detection System

For the implementation of this system we must be aware of the normal behavior of the network, since it is based on rules or heuristics rather than patterns or signatures. Anomaly based detection system is able to detect previous unknown threats, but the false positive ration is quite high.

2.2.3 Specification based Detection System

It monitors the processes and matches the actual data with the program and in case of any abnormal behavior shall issue an alert. They must be maintained and updated whenever a change is there on the surveillance programs, in order to detect the previous attacks. The number of false positive ratio is comparatively less to anomaly detection system approach.

2.3 Classification of Intrusion Detection System

Intrusion detection system are classified into three types

2.3.1 Host based IDS

This is placed on either the server or workstation, where the data is analyzed locally and information is collected for this data from different sources. Anomaly and signature

based detection system can be used here.

2.3.2 Network based IDS

These are deployed on strategic point in network infrastructure. It is able to capture and analyze data to detect known attacks by either comparing patterns or signatures of the database, or by detecting illegal activities by scanning traffic for anomalous activity. We can also call them "packet-sniffers", since they capture the packets passing through the communication mediums.

2.3.3 Hybrid based IDS

This is a mix and match of both the techniques and provides logical complement to NID and HID.

3. NEED FOR AN IDS:

Intrusion detection devices form a vital part of any network. With a constant evolution of the Internet new vulnerabilities and exploits are found regularly, which provide an additional level of protection to notice the existence of an intruder, and help to provide liability for the attacker's action.

The need for IDS is critical due to identification of four different types of attacks.

3.1 Denial of service

Network-based such type of an attack is one of the easiest types. It requires very less effort to fully consume resources on the target computer, to starve the target computer of resources, or to cause critical services to fail or malfunction. Internal corporate networks usually do not have internal filtering barricades against common denial-of-service attacks, such as flooding.

3.2 Threat to Confidentiality

Some viruses are capable enough to get attached to existing files on the system they infect and then send out the infected files to others. This results in distribution of the confidential information without the author's permission.

3.3 Modification of contents

News sites modification, production of bogus press releases, and many other activities are done by Intruders, all of which could have economic impact.

3.4 Masquerade

When one entity pretends to be a different entity it's known as masquerade. After a valid authentication series has taken place it can be captured and replayed, thus enabling an authorized entity to obtain extra privileges which previously had less, by impersonating an entity that has those privileges.

A system with internet connection and provision of TCP-based network services (such as a Web server, FTP server, or mail server) is potentially subject to this attack. In addition to the attacks launched at explicit host, they could also be initiated against your routers or other network server systems if these hosts enable (or turn on) other TCP services (e.g., echo).

The consequences of the attack may vary system to system; however, the attack itself is original to the TCP protocol used by all systems.

4. REQUIREMENTS FOR IDS

There are two levels of abstraction to list the requirement of IDS.

High Level Requirements:

- To develop a capable application that can sniff the traffic, to and from the host machine.
- Development of an application that is competent of analyzing the network traffic and detects numerous pre-defined intrusion attacks and mappings.
- Development of such an application that warns the owner of the host machine, about the likely occurrence of an intrusion attack and information is provided regarding that attack.
- Such an application to be developed that should block traffic to and from a machine that is identified to be potentially malicious and is defined by the owner of the host machine.

Low Level Requirements:

- To develop an application capable enough to display the incoming and outgoing traffic from the host machine in the form of packets to the owner of the host.
- An application that detects occurrence of Denial of Service attacks such as Smurf Attack and Syn-Flood Attack is required.
- Development of an application that detects attempts to map the network of the host, using techniques such as Efficient Mapping and Cerebral Mapping.
- Such an application is required that detects actions attempting to gain unauthorized access to the services provided by the host machine using techniques such as Port Scanning.
- To develop an application that maintains a "Log Record" of identified intrusion attacks done on the host in the present session and also displays it upon request.
- Activation or de-activation of each of the Attack Detection methods should be possible.
- To provide a selection procedure for the user of the host for framing Rules which explicitly specify the set of IP addresses to be blocked or allowed. These Rules shall determine the flow of traffic at the host.

5. USE AND SCOPE

Use of the system: The system must detect certain familiar

intrusion attacks on the host system and warnings to be displayed to the user and also store data regarding the IP addresses that allows the traffic based on the data.

Scope of the system: Based on the input provided by the user, the system frames certain rules. The traffic then flows to and fro based upon the rules. Some well-known attacks are also detected and warnings are given.

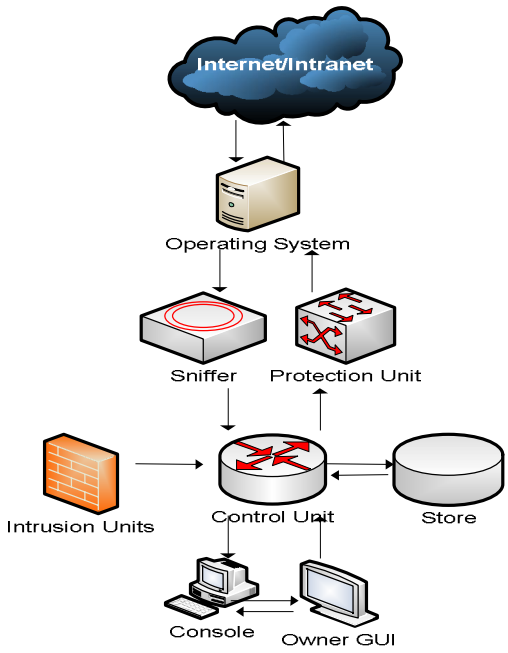
5.1 System overview

On the arrival of the packets, they are sniffed by the sniffer and then various processing techniques are applied to detect the attacks, and the users are warned against it. These are predefined and well known attacks. The following attacks detection are implemented in the system.

- Port Scanner,
- Smurf Attack,
- SYN Flood Attack,
- Efficient Mapping, and
- Cerebral Mapping.

The system has the provision of blocking traffic from a specific IP address which has been recognized to be malevolent or troublesome. Provision has been done to allow traffic from specific IP addresses for some trusted systems, whose traffic is not monitored. Unknown hosts traffic is monitored and any possible attacks are informed to the user.

6. SYSTEM STRUCTURING



Detailed Class Descriptions:

The system contains 31 classes of which 7 are inner classes. The following are the important classes identified, DataProcessor, PacketCapture, ControlUnit, IntrusionAttacks, Console, IntrusionUnit, Attack, SimpleDES, Rule, ProtectionUnit, XmlData, Owner, and IDSMain.

Design with Reuse as goal

Almost all the components in the system are sequence independent from other components, which are designed in such a way that they can be reused by other systems. The components that can be used as Reusable components are as follows:

PacketCapture, XmlData, SimpleDES, IntrusionUnit, and Console.

The usage of JAVA in the development makes it Platform independent making the code portable on any Operating system.

7. CONCLUSION AND FUTURE WORK

All the systems present in the network and connected directly or indirectly to the Internet can be secured by basic detection techniques provided in IDS. Performing such a task goes hand in hand with success as well as failure in fulfillment of the objective. At least the job is done. But at last the Network Administrator has to make sure that his network is not in danger. This software does not completely defend network from Intruders, but the very purpose of IDS is to help the Network Administrator to track the bad guys on the Internet who are suppose to bring your network to a breach point and thus making it vulnerable to attacks. The following is an attempt to show what should be the source of action while using the software and after an attack has been detected by IDS. Like other conventional IDS this also provides facilities for Intrusion Protection. The blocking or allowing particular IP, range of IPs or a subnet IPs by applying relevant rule on the Operating system depends on this. This is a reusable system. Due to the high end flexibility and extensibility provided in the design of the system it becomes easy to add more number of attacks to the system in future.

Java has been the core for the development, thus making it platform independent, yet it has been tested only on WindowsXP. Though it will work fine on other operating systems also and thus satisfy the requirements and pre-requisites for the IDS system. A log is maintained that is valid only for the current session and contains no information about the past sessions, which can be enhanced in future. Enhancements in the system are possible on the works listed below:

The present system can display the log information but none of the techniques to analyze the data present in the log records and extract knowledge is present. Extension is possible by incorporating Data Mining techniques for analysis of the log records which may help in efficient decision making. The present system only detects the known attacks, which can be extended by incorporating Intelligence into it to gain knowledge by itself by analyzing the growing traffic and learning new Intrusion patterns. Presently system runs on an individual host machine and is not a distributed

application; while in future it can be extended to as a distributed application where different modules of the same system running on different machines may interact with each other thus providing distributed detection and protection the machines on which the system is running.

REFERENCES

[1]. M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti-Jamming Techniques in Sensor Networks", in IEEE Transactions on Mobile Computing, January 2007

[2]. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis, Y. Yesha, Threshold-based intrusion detection in ad hoc networks and secure AODV, Ad Hoc Networks 6 (2008) 578–599.

[3]. [42] S.A. Razak, S.M. Furnell, N.L. Clarke, P.J. Brooke, Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks, Ad Hoc Networks 6 (2008) 1151–1167

[4]. N. Komninos, C. Douligeris, LIDF: layered intrusion detection framework for ad hoc networks, Ad Hoc Networks 7 (2009) 171–182.

[5]. Idika, N. & Mathur P. A., "A Survey of Malware Detection Technique", In Proceeding of Software Engineering Research Center Conference, SERC-TR286, 2007.