NETWORK TRAFFIC MONITORING USING INTRUSION DETECTION SYSTEM

Dr.Nikhil Raj [1], Dr Kavitha[2], Dr. Ganapathi sridhar[3], Naresh Manda[4], N Mahesh[5]
[1,2,3,]Professor, [4,5]Asst. professor, Dept. of ECE,MRCE, Hyderabad

Abstract— Security is a big issue for all networks in today's enterprise environment. Many methods have been developed to secure the network infrastructure and communication over the Internet, among them the use of firewalls, encryption, and virtual private networks. Intrusion detection is a relatively new addition to such techniques. IDS protect a system from attack, misuse, and compromise. It can also monitor network activity. Network traffic monitoring and measurement is increasingly regarded as an essential function for understanding and improving the performance and security of our cyber infrastructure.

Keywords- IDS, NTM, Pattern Matching, IMAP

I. INTRODUCTION

A. Statement Of Problem

Security is a big issue for all networks in today's enterprise environment. Intruder infect the file by adding some signatures and by applying IDS that file is detected. With networking technologies and services evolving rapidly, as witnessed by the explosive growth of the World-Wide Web, peer-to-peer networks, and the GRID, accurate network traffic monitoring is required to ensure the security and optimize the efficiency of our cyberspace.

B. Intrusion Detection System:

The purpose of the IDS is to detect certain wellknown intrusion attacks on the host system and display warnings to the user and also store information regarding the IP addresses and allow the traffic based on that information.

C. Network Traffic Monitoring:

Network traffic monitoring and measurement is increasingly regarded as an essential function for understanding and improving the performance and security of our cyber infrastructure. Network Traffic Monitor is network analytic tool that examines local area networkusage and provides a display of upload and download statistics. The main purpose of the application is monitoring the IP traffic between your local area network network and Internet.

II. LITERATURE SURVEY

A. Basic Terminology

1) Intrusion:

1) Host based Intrusion Detection System:

An unauthorized entry into a network or system. Frequently synonymous with an information technology security incident.

2) Signatures:

Signature is the pattern that you look for inside a data packet. A signature is used to detect one or multiple types of attacks Signatures may be present in different parts of a data packet depending upon the nature of the attack. Usually IDS depends upon signatures to find out about intruder activity. Some vendor-specific IDS need updates from the vendor to add new signatures when a new type of

3) Network Traffic:

Incoming and outgoing packets generating traffic.

B. Need

A virus, worm program that is either downloaded B. Need

A virus, worm program that is either downloaded form of an attachment to an email message that you open, or that is delivered via an embedded Active X control or JavaScript program in a Web page. To detect these viruses

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-12, 2017
DOI: 10.21276/ijcesr.2017.4.12.25

and worms we need a powerful system IDS. Traffic consist of packets which are coming from various ports like HTTP,FTP,SMTP, etc; these packets may be malicious or non-malicious. To view the integrity of packets we need network traffic monitoring tool. By using network traffic monitoring tool incoming and outgoing packets are captured and then analyze by using pattern matching IDS system.

C. Types Of Ids

HIDS involves not only looking at the network traffic in and out of a single computer, but also checking the integrity of your system files and watching for suspicious processes.

2) Network based Intrusion Detection System:

NIDS is a system which monitors network

intrusion. Intrusion may be detected by techniques like anomaly detection, signature pattern matching etc. Signature pattern matching is a method in which network data is compared with the known attack techniques that are saved in a database.

D. Pattern Matching:

Almost all IDSs are signature based, also known as knowledge based. Signature based IDSs monitor network traffic and analyzes this traffic against specific predefined attacks. This means that any traffic that doesn't specifically match a signature is considered safe. Pattern matching is based on looking for a fixed sequence of bytes in a single packet. As its name suggests, it is an approach that is fairly rigid but simple to employ. In most cases the pattern is matched against only if the suspect packet is associated with a particular service or, more precisely, destined to/from a particular port. This helps to lessen the amount of inspection done on every packet. However, it tends to make it more difficult for systems to deal with protocols that do not live on well defined ports and, in particular, Trojans, and their associated traffic, which can usually be moved at will. The structure of a signature based on the simple pattern-matching approach might be as follows: If the packet is IPv4 and TCP and the destination port is 2222 and the payload contains the string "foo," fire an alarm. This example of a pattern match, of course, is a very simple one, but the variations from this point are also simplistic. You could include a specific starting point and endpoint for inspection within the packet, for instance, or you could specify the TCP flags for packets to be considered. In the end,though, this technique remains the simplest and most primitive building block for intrusion detection.

E. Network Traffic Monitoring

Network Traffic Monitor is a network analytic tool that examines local area network usage and provides a display of upload and download statistics. The main purpose of the application is monitoring the IP traffic between your local area network and Internet. Network Monitor is a network diagnostic tool that monitors local area networks and provides a graphical display of network statistics. Network administrators can use these statistics to perform routine trouble-shooting tasks, such as locating a server that is down, or that is receiving a disproportionate number of work requests. The process by which Network Monitor collects this information is called capturing. By default, Network Monitor gathers statistics on all the frames it detects on the network into a capture buffer, which is a reserved storage area in memory. To capture statistics on only a specific subset of frames, you can single out these frames by designing a capture filter. When you have finished capturing information, you can design a display filter to specify how much of the information that you have captured will be displayed in Network Monitor's Frame Viewer window.

III. PROBLEM STATEMENT

One of the techniques used in IDS is pattern matching. Using pattern matching, pattern is matched against only if the suspect packet is associated with a particular file. Intrusion detection involves not only looking at the network traffic in and out of a single computer, but also checking the integrity of your system files and watching for suspicious processes. Network Monitor is a network diagnostic tool that monitors local area networks and provides a graphical display of network statistics. Network administrators can use these statistics to perform

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-12, 2017
DOI: 10.21276/ijcesr.2017.4.12.25

routine trouble- shooting tasks, such as locating a server that is down, or that is receiving a disproportionate number of work requests. While collecting information from the network's data stream, Network Monitor displays the following types of information:

- ☐ The source address of the computer that sent a frame onto the network.
- ☐ The destination address of the computer that received the frame.
- ☐ The protocols used to send the frame.
- ☐ The data, or a portion of the message being sent.

The process by which Network Monitor collects this information is called capturing. By default, Network Monitor gathers statistics on all the frames it detects on the network into a capture buffer, which is a reserved storage area in memory. To capture statistics on only a specific subset of frames, you can single out these frames by designing a capture filter. When you have finished capturing information, you can design a display filter to specify how much of the information that you have captured will be displayed in Network Monitor's Frame Viewer window.

A. Functional Requirement

The requirements to develop the system or software can be listed at two levels of abstraction.

- ☐ To develop an application that is capable of sniffing the traffic, to and from the host machine.
- ☐ To develop an application that is capable of analyzing the network traffic and detects several pre-defined intrusion attacks and mappings.
- ☐ To develop an application that warns the owner of the host machine, about the possible occurrence of an intrusion attack and provides information regarding that attack.
- ☐ To develop an application that is capable of blocking traffic to and from a machine that is identified to be potentially malicious and that is specified by the owner of the host machine.

B. Feasibility Study

Feasibility study consists of following things:

1. Technical feasibility
2. Operational feasibility
3. Economical feasibility
4. Reliability
5. Efficiency
6. Portability

1) Technical Feasibility:

Technical feasibility determines whether the organization has the technology and skills necessary to carryout the project and how this is obtained. The existing resources are capable and can hold all the necessary data. The system is too flexible and it can be expanded further.

2) Operational feasibility:

Operational feasibility determines if the proposed

system satisfied user objectives and can be fitted into the current system operation. The proposed system will not cause any problem under any circumstances. The proposed system will certainly satisfy the user objectives and it will also enhance their capability. The proposed system can be best fitted into current operation.

3) Economical Feasibility:

It determines whether projects goal can be with in the resource limits allocated to it. It must determines whether it is worthwhile to process with the project all or whether the benefits obtained from the new system is not worth the costs. After conducting cost benefit analysis, it reveals that the objectives of the proposed system can be achieved within the allocated resources.

4) Reliability:

It is evaluated by measuring the frequency and

severity of failure, the accuracy of output results, the mean-time-to-failure (MTTF) , the ability to recover from failure, and the predictability of the program.

5) Efficiency:

The amount of computing resources and code

required by program to perform its function. The degree to which the software makes optimal use of system resources as indicated by some attributes like time behaviour, resource behaviour.

6) Portability:

As java language is being used the program is portable i.e. platform independent .Effort required to transfer the program from one hardware and /or software system environment to another. The ease with which the software can be transposed from one environment to another as indicated by some attributes such as adaptability, installability, conformance, replaceability.

C. Use Case Digram

1) Actors:

1. User: User sends request to server and server responds by providing the requested service.
2. Network: Network carries the IP packets from source to destination.
3. IDS: IDS takes the packets from the network, analyses the packets.
4. System Administrator: System Administrator is alerted by the IDS of any suspicious activity or whenever intrusion is detected.

2) Use Case Description

IP Packets Network gives the IP Packets to IDS which does further processing of these packets.

☐ Signature recognition : IDS examines the traffic looking for well-known patterns of attack, which are saved in pattern database and triggers the alert system, if a match is found.

☐ Alert System: triggered by anomaly detection or signature recognition, it alerts the system administrator.

Use Case Diagram

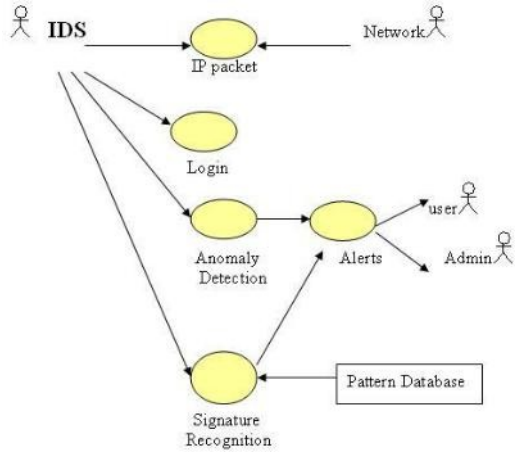


Fig. 3.1 Use Case Diagram

IV. PLATFORM USED

A. Java Version 1.6:

1) Generics :

This long-awaited enhancement to the type system allows a type or method to operate on objects of various types while providing compile-time type safety. It adds compile-time type safety to the Collections Framework and eliminates the drudgery of casting.

2) Class Data Sharing :

The class data sharing feature is aimed at reducing application startup time and footprint. The installation process loads a set of classes from the system jar file into a private, internal representation, then dumps that representation to a "shared archive" file. During subsequent JVM invocations, the shared archive is memory-mapped in, saving the cost of loading those classes and allowing much of the JVM's metadata for these classes to be shared among multiple JVM processes.

B. Base Libraries

Lang and Util Packages

For a synopsis of java.lang and java.util enhancements,

II)Networking

java.net.InetAddress.getLocalHost ()

would cache the lookup of the IP address of the local machine for the entire session of the application.

III)Security

This release of J2SE offers significant enhancements for security. It provides better support for security tokens, support for more security standards ,improvements for scalability and performance, plus many enhancements in the crypto and Java GSS areas.

C. Image I/O

The Image I/O system now has readers and writers for BMP and WBMP formats.

D. AWT

Version 1.6 features many AWT enhancements and bug fixes, including some that have often been requested by our customers. Most notably, the new MouseInfo class makes it possible to determine the mouse location on the desktop. New Window methods make it possible to specify the default location for a newly created window (or frame), appropriate to the

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-12, 2017
DOI: 10.21276/ijcesr.2017.4.12.25

platform. Another Window enhancement makes it possible to ensure that a window (or frame) is always on top. (This feature does not work for some window managers on Solaris/Linux.) In the area of data transfer, the new DropTargetDragEvent API allows the drop target to access transfer data during the drag operation.

F. Swing

Beyond look and feels, have added printing support to JTable, which makes it trivial to get a beautiful printed copy of a JTable.

G. JpCap

I) What is Jpcap

Jpcap is an open source library for capturing and sending network packets from Java applications. It provides facilities to:

- ☐ capture raw packets live from the wire.
- ☐ save captured packets to an offline file, and read captured packets from an offline file.
- ☐ automatically identify packet types and generate corresponding Java objects (for Ethernet, IPv4, IPv6, ARP/RARP, TCP, UDP, and ICMPv4 packets).
- ☐ filter the packets according to user-specified rules before dispatching them to the application.
- ☐ send raw packets to the network Jpcap is based on libpcap/winpcap, and is implemented in C and Java.

What kind of applications can be developed using Jpcap Jpcap can be used to develop many kinds of network applications, including:

- ☐ network and protocol analyzers
- ☐ network monitors
- ☐ traffic loggers
- ☐ traffic generators
- ☐ user-level bridges and routers
- ☐ network intrusion detection systems (NIDS)

- ☐ network scanners
- ☐ security tools

WinPcap

What is WinPcap

WinPcap is a free, public system for direct network access under Windows. Most networking applications access the network through widely used system primitives, like sockets. This approach allows to easily transfer data on a

network, because the OS copes with low level details (protocol handling, flow reassembly, etc.) and provides an interface similar to the one used to read and write on a file. Sometimes however the 'easy way' is not enough, since some applications need a low level view in order to directly handle the network traffic. Therefore, they need raw access to the network, without the intermediation of entities like protocol stacks. The purpose of WinPcap is to give this kind of access to Win32 applications; it provides facilities to

- ☐ capture raw packets, both the ones destined to the machine where it's running and the ones exchanged by other hosts (on shared media)
- ☐ filter the packets according to user-specified rules before dispatching them to the application
- ☐ transmit raw packets to the network
- ☐ gather statistical values on the network traffic What kinds of programs use WinPcap:

WinPcap can be used by different kind of tools for network analysis, troubleshooting, security and monitoring. In particular, classical tools that rely on WinPcap are

- ☐ network and protocol analyzers
- ☐ network monitors
- ☐ traffic loggers
- ☐ traffic generators
- ☐ user-level bridges and routers
- ☐ network intrusion detection systems (NIDS)

V. IMPLEMENTATION

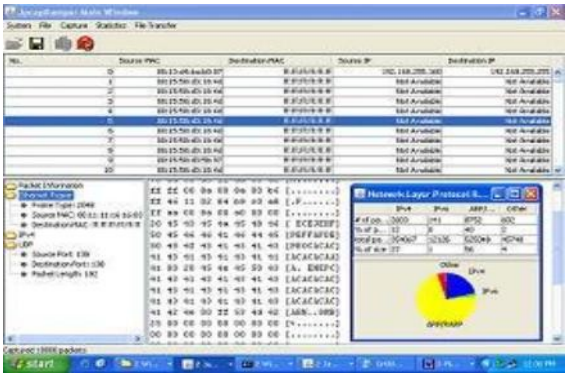
A. Login:

Administrator can login for monitoring network traffic. Login screen is as follows:

B. Main window:

ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-4, ISSUE-12, 2017
DOI: 10.21276/ijcesr.2017.4.12.25

This is the main window for packet capturing as follows:



C. File Transfer:

Now there is a option “File Transfer” for transferring the file from server to client following image shows the window.

D. Client Communication:

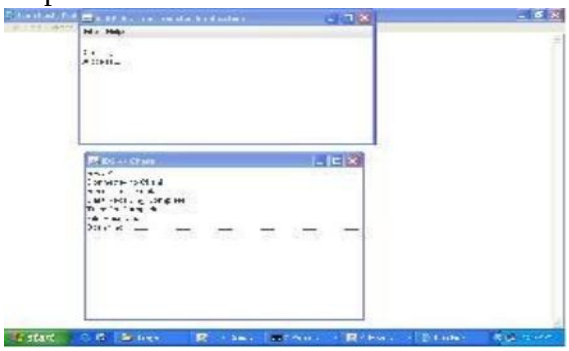
Now client is ready for receiving the file.

E. Opening and send file:

Server browse for sending file and then gives the success after receiving the file by client.

F. Pattern Matched:

If pattern is matched then client receive that corrupted file and delete it.



VI. CONCLUSION

For IDS has been to blend the use of pattern matching, stateful pattern matching. The IDS arena and will incorporate new techniques as they become efficient, practical, cost-effective, and commercially viable. Host based intrusion detection involves not only looking at the network traffic in and out of a single computer, but also checking the integrity of your system files and watching for suspicious processes. Network traffic monitoring is an analysis and reporting tool. It works in all Windows based operating systems. It captures all traffic transport over both Ethernet and WLAN networks. Network traffic monitoring decodes all major TCP/IP protocols. With Network traffic monitoring , you can easily filter the network traffic to focus on the information that you are looking for. Comprehensive reports and graphic views allow you to understand network performance and usage quickly and identify problems in simple steps. Protocol decoders for TCP/IP and many application protocols including ARP/RARP, ICMP, IP, TCP, UDP, DNS, POP3, SMTP,

IMAP, HTTP/HTTPS, TELNET, FTP. Powerful and easy to set filters allow user to focus on useful traffic and narrow down the problem. Easy to use user interface.

VII. FUTURE WORK

Network Packet Analyzer is a comprehensive and affordable solution to the following problems: Troubleshooting network problems; Debugging new applications with network communication involved; Monitoring network traffic for performance, bandwidth usage, and security reasons; Analyzing network traffic to trace specific transactions or find security breaches; Monitor employee Internet access, email communication and other transactions to enforce company policies. Generate reports on network usage and statistics for network performance review and planning, network auditing and many other purposes. Comprehensive Features Real-time packet capture and analysis over both Ethernet and WLAN; Many reports and graphic charts allow you to see various statistics, Captures and decode HTTP/HTTPS packets to allow you to analyze Internet traffic; Capture and analyze POP/Pop3, SMTP and IMAP emails, display and save in Outlook Express Message Format.

REFERENCES

1.http://www.informit.com/content/downloads/perens/0 131407333.pdf

2. www.securitydocs.com/library/3009

3.http://www.robertgraham.com/pubs/hostbased- intrusion-detection.html

4. http://www.javvin.com/packet.html

5. Book on “Java Network Programming” by Elliotte Rusty Harold

6. IEEE paper on “The Role of Intrusion Detection System” by John McHugh, Alan Christie, and Julia Allen.

7. Book on “Intrusion Detection” by Edward G. Amoroso.