ISSN No. 0976-5697

Volume 4, No. 6, May 2013 (Special Issue)

International Journal of Advanced Research in Computer Science

REVIEW ARTICAL

Available Online at www.ijarcs.info

Network Traffic Monitoring with IDS

Ms. P. A. Patil
M.E.H. V. P. M.COET, Amravati
pallavi27patil@gmail.com

Prof. R. R Keole
Asst. Prof. H.V.P.M.COET, Amravati
ranjitkeole@gmail.com

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. IDSes 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

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.

A. Intrusion Detection System:

The purpose of the IDS is to detect certain well-known 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.

B. 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 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 (and counting) the IP traffic between your local area network (LAN) and Internet

II. LITERATURE SURVEY

A. Basic Terminology:

a. Intrusion:

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

b. 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 attack is discovered.

c. Network Traffic:

Incoming and outgoing packets generating traffic.

B. Types Of Ids:

a. Host based Intrusion Detection System:

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.

b. 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.

C. Intrusion Detection System

a. Pattern Matching:

Almost all IDSs are signature based, also known as knowledge based. Signature based IDSs monitor network traffic and analyze 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.

D. 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 (and counting) the IP traffic between your local area network (LAN) 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. ANALYSIS

A. Detailed Statement Of The Problem:

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 files. 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 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:

a. The source address of the computer that sent a frame onto the network.
b. The destination address of the computer that received the frame.
c. The protocols used to send the frame.
d. 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.

B. Requirement Analysis:

a. Functional Requirement:

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

a) To develop an application that is capable of sniffing the traffic, to and from the host machine.
b) To develop an application that is capable of analyzing the network traffic and detects several pre-defined intrusion attacks and mappings.
c) 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.
d) 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.

C. Feasibility Study:

Feasibility study consists of following things:

a) Technical feasibility
b) Operational feasibility
c) Economical feasibility
d) Reliability
e) Efficiency
f) Portability

a. Technical Feasibility:

Technical feasibility determines whether the organization has the technology and skills necessary to carry out 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.

b. 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.

c. *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.

d. *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.

e. *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.

f. *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

D. *Use Case Digram:*

a. *Use Cases:*

Actors:

a) User: User sends request to server and server responds by providing the requested service.

b) Network: Network carries the IP packets from source to destination.

c) IDS: IDS takes the packets from the network, analyses the packets.

d) System Administrator: System Administrator is alerted by the IDS of any suspicious activity or whenever intrusion is detected.

b. *Use Case Description:*

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

a) 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.

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

c. *Use Case Diagram*

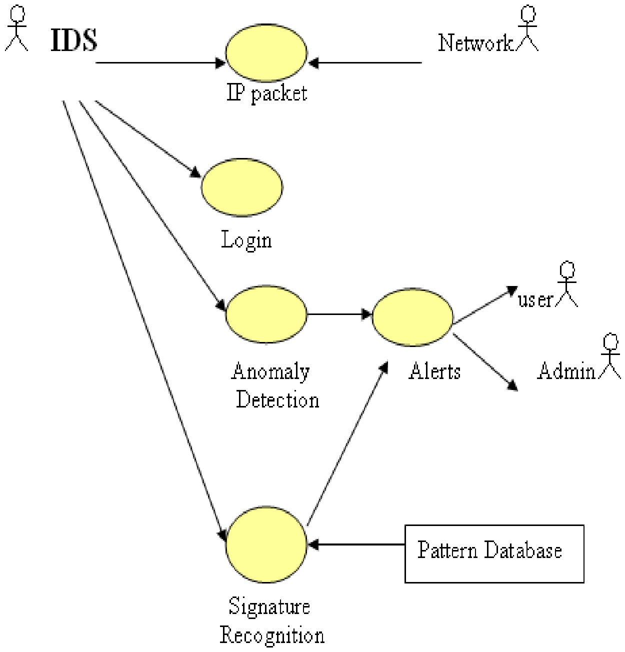


Figure. 1 Use Case Diagram

IV. DESIGN

A. *Module Diagram:*

a. *Designing of the Server and Client screen:*

Create client and server screen using JFrame( ) JMenu( ) class.

b. *Creating Server modules*:

Create server socket to connect the client through Server Socket ( ) class and start listening the clients.

c. *Create Client Modules.:*

Create client socket and connect the server through Server Socket( ) class.

d. *Transferring files:*

After connection of client to the server, files are sent by the server ,requested by the client.

e. *Scanning*:

Reading of file from the buffer line by line by using String Tokenizer ( ) class. If matched found with the pattern then do not receive file by the client side.

f. *Packet Capturing* :

Packets from the network are captured by using JpCaptor( ) class.After capturing display the whole information about the packet such as source address, destination address, ethernet address, port address, packet length, time when packet is received .

B)Flow chart for CLIENT & SERVER

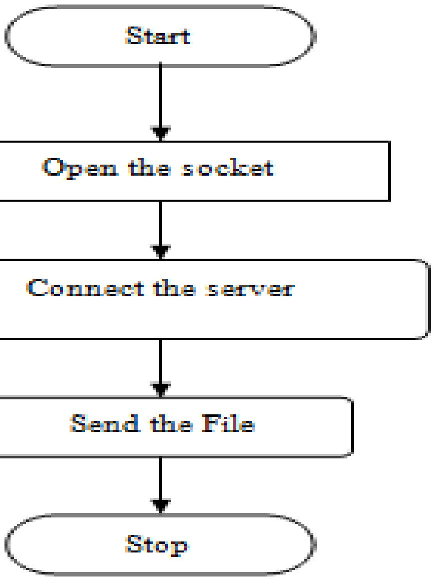


Figure: 2

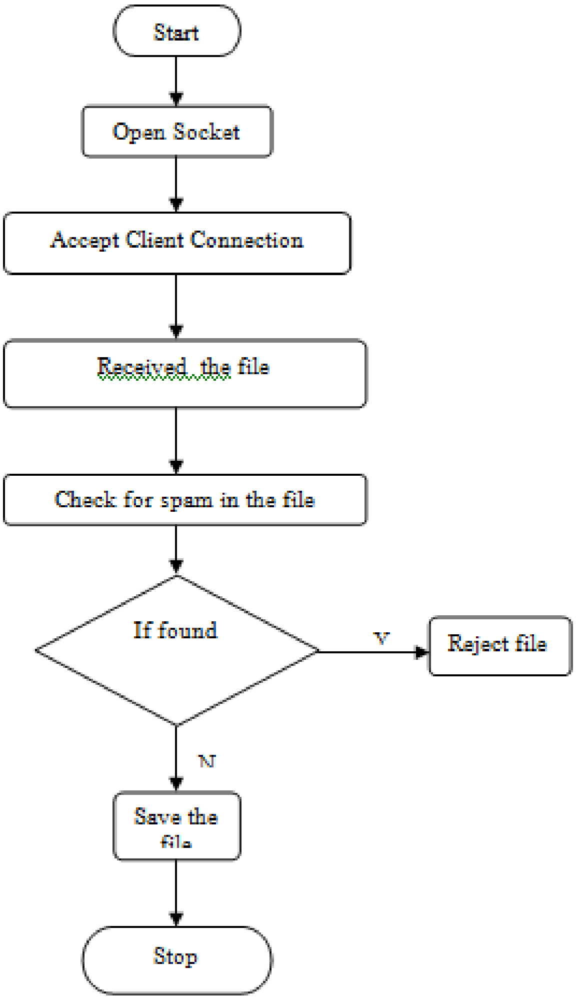


Figure: 3

V. PLATFORM USED

A. Hardware platform used:

Personal Computer configuration: Operating System: Window XP Processor: Pentium IV RAM : 512 MB.

B. Software platform used:

a. Java 1.6:

Version 1.6 features many AWT enhancements and bug fixes, including some that have often been requested by our customers. Most notably, the new Mouse Info 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 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.

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

b. JpCap :

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

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

c. 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:

a) capture raw packets, both the ones destined to the machine where it's running and the ones exchanged by other hosts (on shared media)

b) filter the packets according to user-specified rules before dispatching them to the application
c) transmit raw packets to the network
d) gather statistical values on the network traffic .

VI. IMPLEMENTATION

A. *Login*:

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

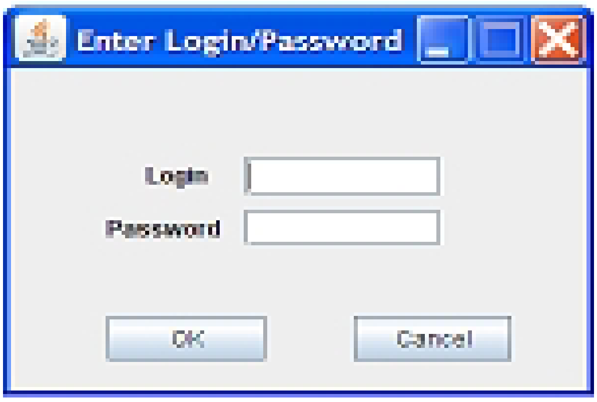
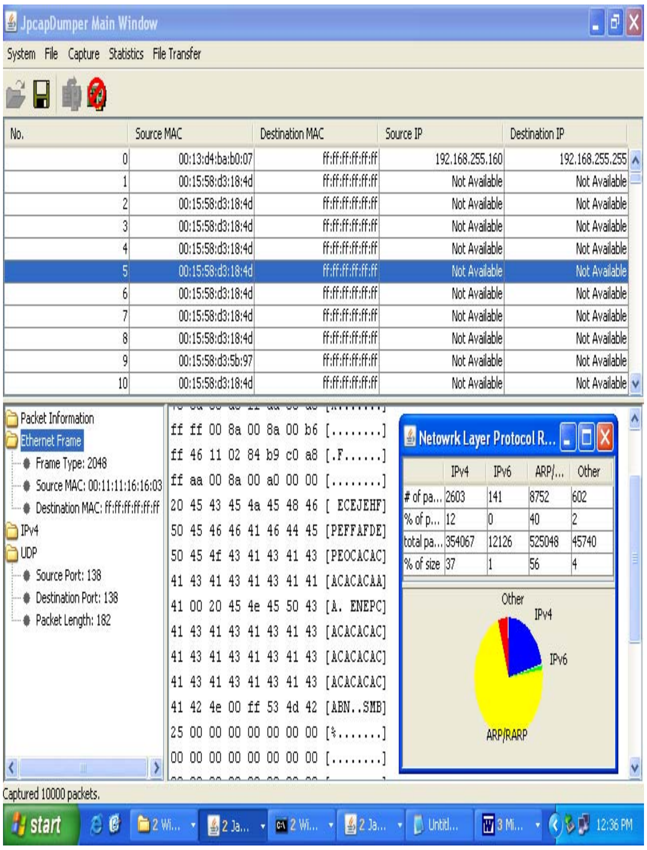


Figure:4

B. *Main window*:

This is the main window for packet capturing as follows..



No.	Source MAC	Destination MAC	Source IP	Destination IP
0	00:13:d4:ba:b0:07	ff:ff:ff:ff:ff:ff	192.168.255.160	192.168.255.255
1	00:15:58:d3:18:4d	ff:ff:ff:ff:ff:ff	Not Available	Not Available
2	00:15:58:d3:18:4d	ff:ff:ff:ff:ff:ff	Not Available	Not Available
3	00:15:58:d3:18:4d	ff:ff:ff:ff:ff:ff	Not Available	Not Available
4	00:15:58:d3:18:4d	ff:ff:ff:ff:ff:ff	Not Available	Not Available
5	00:15:58:d3:18:4d	ff:ff:ff:ff:ff:ff	Not Available	Not Available
6	00:15:58:d3:18:4d	ff:ff:ff:ff:ff:ff	Not Available	Not Available
7	00:15:58:d3:18:4d	ff:ff:ff:ff:ff:ff	Not Available	Not Available
8	00:15:58:d3:18:4d	ff:ff:ff:ff:ff:ff	Not Available	Not Available
9	00:15:58:d3:5b:97	ff:ff:ff:ff:ff:ff	Not Available	Not Available
10	00:15:58:d3:18:4d	ff:ff:ff:ff:ff:ff	Not Available	Not Available

Packet Information
Ethernet Frame
- Frame Type: 2048
- Source MAC: 00:11:11:16:16:03
- Destination MAC: ff:ff:ff:ff:ff:ff

IPv4
UDP
- Source Port: 138
- Destination Port: 138
- Packet Length: 182

```
ff ff 00 8a 00 8a 00 b6 [........]
ff 46 11 02 84 b9 c0 a8 [.F......]
ff aa 00 8a 00 a0 00 00 [........]
20 45 43 45 4a 45 48 46 [ ECEJEHF]
50 45 46 46 41 46 44 45 [PEFFAFDE]
50 45 4f 43 41 43 41 43 [PEOCACAC]
41 43 41 43 41 43 41 41 [ACACACAA]
41 00 20 45 4e 45 50 43 [A. ENEPC]
41 43 41 43 41 43 41 43 [ACACACAC]
41 43 41 43 41 43 41 43 [ACACACAC]
41 43 41 43 41 43 41 43 [ACACACAC]
41 42 4e 00 ff 53 4d 42 [ABN..SMB]
25 00 00 00 00 00 00 00 [%.......]
00 00 00 00 00 00 00 00 [........]
```

	IPv4	IPv6	ARP/...	Other
# of pa...	2603	141	8752	602
% of p...	12	0	40	2
total pa...	354067	12126	525048	45740
% of size	37	1	56	4

Captured 10000 packets.

Figure:5

VII. 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.publication should be cited as “in press” [5]. Capitalize only the first word in a paper title, except for proper nouns and element symbols.

For papers published in translation journals, please give the English citation first, followed by the original foreign-language citation.

VIII. 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 FeaturesReal-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.

IX. REFERENCES

[1]. http://www.informit.com/content/downloads/perens/0131407333.pdf

[2]. www.securitydocs.com/library

[3]. 3009http://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.