Integrating Intrusion Detection System with Network monitoring

Prof. Naveen Kumar [*], Sheetal Angral[**], Rohan Sharma[**]

[*] Computer Science & Engineering, B.V.P.C.O.E.P
[**] Computer Science & Engineering, B.V.P.C.O.E.P

Abstract- In today's enterprise environment, Security is a big issue for everybody. Methods such as cryptography, VPN, etc have been developed to secure the network channel and have a complete privacy over the Internet, among them the use of, encryption, firewalls, and virtual private networks is also very common. To this era of technology Intrusion detection has come up with new expectations. Intrusion detection system also commonly called as IDS provides a complete protection to the system from attack, compromise, and misuse. It is also most commonly used for monitoring network activities. For understanding and improving the performance and security of our cyber infrastructure, Network traffic monitoring is considered as an essential function.

I. INTRODUCTION

A. Problem statement

Security is considered a major issue in today's enterprise environment. An Intruder can infect the package by adding some signatures This intrusion can be detected by applying IDS. As networking technologies and services have evolved rapidly due to massive expansion of WWW, GRID, peer-to-peer networks, accurate network traffic monitoring is essential to optimize the efficiency of our cyberspace and ensure the security.

B. Network traffic monitoring

- What is it??

Network Traffic Monitoring (NTM) is a network analytic tool that observes local area network usage and provides a statistical display of the uploads and the downloads in an network. The main purpose of NTM is monitoring the I/P traffic between the LAN and the Internet.

NTM is a essential function for improving and understanding the security and performance of our cyber infrastructure.

C. Intrusion Detection System (IDS)

Intrusion Detection System is a packet filtering device used to monitor traffic based on predefined set of rules or pattern. It inspects traffic and looks for any suspicious behavior pattern. If any suspicious activity is detected it stores the I/P address and alarms the user with a warning.

II. LITERATURE SURVEY

A. Basic Terminology

- Signatures

A signature is a pattern or a form of predefined code that one looks for inside a data packet. By using signatures various kinds of attacks can be detected. A signature can be present in any part of the packet, which may depend upon the type of attack.

The Intrusion Detection system completely depends on signatures to identify an intrusion.

Some of the IDS which are vendor specific need timely updates of the signatures from the server in order to detect a new attack.

- Intrusion

Intrusion is an unauthorized access to an network or a system, in which the attacker usually intent to access the privacy of the user.

- Network Traffic

It is the traffic generated by incoming and outgoing packets in a network.

B. Types of Intrusion Detection system

- IDS based on network

Network intrusion detection system is the system that monitors intrusions on the network. Various techniques such as pattern matching, anomaly detection etc are used to detect the intrusion. The most popular among many is the signature pattern matching in which the network data is compared with the stored data. The stored data is nothing but a pre-known attack technique.

- IDS based on host system

Host based intrusion detection system is the system in which both (the network & the host system) is monitored for any suspicious activity. It not only check the data packets that may be going in and out of the system, but it also keeps any eye on the internal file system and keeps a log of the suspicious processes. Techniques such as SANDBOX etc are used by these systems.

C. Pattern matching technique

As the name suggests pattern matching technique works on intrusion detection based on pattern matching. A signature of a known attack is first stored in the database of the system. Once a packet is received, it monitors the signature based on the information stored in the system database. If the signature matches the information of the database, the packet is considered as suspicious and is immediately dropped by the system.

All most all intrusion detection systems works on signature matching technique. Any packet that doesn't match the signature is marked as Safe by the system.

Pattern matching technique is less flexible but easy to deploy. In most of the IDS, the packet is only examined if the particular packet is linked with a particular service or more precisely destined for a particular Port of the system. For instance, the system will fire an alarm for those packets that are destined for the PORT NO – 1234 and the payloads of which have the string "hacker". This lets the system to vulnerable to the packets that can move (for instance Trojan Horse).

The above example of patter matching is of course very simple one but extension to this is also simplistic. One can also include start and end point in the packet for which the system will apply pattern matching technique.

D. Traffic Monitoring Tool

Traffic Monitoring tool is the networking tool that is used to examine usage of local area network and provide a statistical data of uploads and downloads in a network. Monitoring tool is usually used to monitor I/P traffic between the LAN and the internet. It is a network diagnostic system that is used to monitor local area network and provide a statistical display of the same. The data can be further used to improve the network efficiency. Other problems such as locating the down server, receiving incorrect work request etc can also be removed.

E. Why do we need it??

When a packet is received by the system, it may contain malicious data. A powerful IDS is needed to identify these packets drop them immediately. Network monitoring tool can also be used to check the integrity of the packet.

III. PROBLEM STATEMENT

The most common technique used in IDS is pattern matching. Pattern matching works on the technique that signature of a known attack is first stored in the database of the system. Once a packet is received, it monitors the signature based on the information stored in the system database. If the signature matches the information of the database, the packet is considered as suspicious and is immediately dropped by the system. The IDS not only check the data packets that may be going in and out of the system, but it also keeps any eye on the internal file system and keeps a log of the suspicious processes.

Network Traffic Monitoring (NTM) is a network analytic tool that observes local area network usage and provides a statistical display of uploads and downloads in a network. The network display monitor displays following information:

- Source address of the system that sends frame to the network.
- The protocol that was used to send the frame.
- Destination address of the system where the frame will be received.
- Data of the message that is sent.

Capturing is the process by which a network monitor collects the information. All the information is stored by default in capture buffer. Also, one can apply restrictions on the information to be captured by the system and the data to be displayed on the monitor.

A. Functional requirement

The software to be developed should perform following functions:

- Sniffing of all the incoming and outgoing packets of the host machine.
- Detect intrusion attacks on the host with the use of pattern matching.
- After detection the application should alert the user about the unusual behavior or attack.
- The application should be able to block the traffic to and from the system which is found malicious.

B. Feasibility study

Feasibility comprises of following:

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

1. Technical feasibility

Technical feasibility determines whether the application or system can be developed with existing resources and skills. The application should be flexible to adapt to any change so that it can be expanded further.

2. Economical feasibility

Economical feasibility determines whether the application can be implemented with given limited resources and if it is worth spending. Cost benefit analyses is done to find the economical feasibility of the project.

3. Efficiency

Efficiency is evaluated by measuring the degree to which system makes optimal use of resources to perform desired function.

4. Operational feasibility

Operational feasibility determines whether the application operates according to the requirements specified by the user. It also determines whether it will work under any circumstances.

5. Reliability

Reliability determines the ability of the application to avoid failures and if they occur then how to recover from them. It is basically a measure of frequency and severity of failures.

C. System design: UML Use case diagram

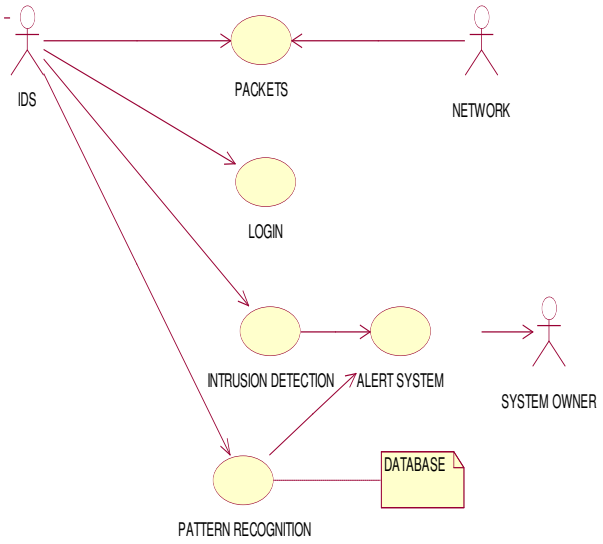
1) Actors:

- Network: It represent a collection of machines connected to the host machine and passes the packets from one machine to another.
- IDS: it takes packets from the network, analyzes them and finds intrusion.

- System owner: System owner is the client accessing services from the server.

2) Use Cases:

- Packets: All the I/P packets in the network come to IDS for analyses.
- Alert system: Alerts the system owner if intrusion is detected.
- Pattern recognition: It carries out the task of pattern matching from the known pattern of attacks saved in database.
- Log In: It authenticates the user and activates the IDS.



IV. PLATFORM USED

A. Visual C++

Visual C++ is a powerful front end GUI tool which is used to develop application programs. The interface consists of integrated set of menus, tools, windows, directories, etc that allow the user to create, refine and test the application from one place.

The added advantage of visual C++ is its inbuilt Microsoft foundation class libraries. By using these classes one can create windows, sockets, forms etc. These libraries are included to reduce the overhead of developer in creating windows and interfaces and so that he can concentrate on application development. Moreover visual C++ also supports network programming with given access to the network interface card (NIC).

Visual C++ being an object oriented language also supports features such as polymorphism, encapsulation etc.

B. WinPcap

It is a freeware which is used for direct network access under windows. WinPcap provides architecture for network analyses and packet capturing for win32 platform. It includes following features:

- Kernel level packet filter
- Low level dynamic link library(packet.dll)
- System independent and a high level library(wpcap.dll)

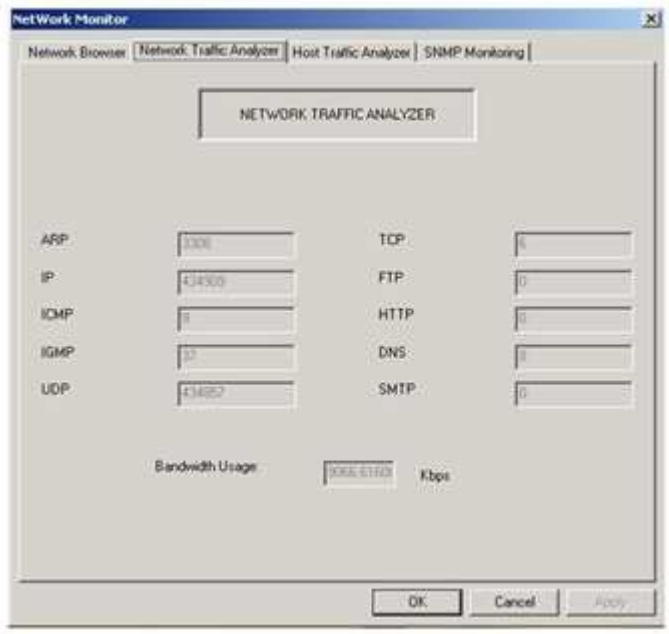
In order to directly handle the network traffic WinPcap have a low level view. WinPcap can facilitate:

- Raw packet capturing
- Filtering the packets according to the set of rules defined by the user.
- To gather statistical data related to network traffic.

V. IMPLEMENTATION

A. Network traffic analyzer

The window for network traffic analyzer is as follow:



B. Communicating with client

Client will be ready to receive the file.

C. Sending file

The file is sent and acknowledgement is received.

D. Pattern Match

If the pattern is matched, then the file is dropped by the user system.

VI. CONCLUSION

Host based intrusion detection system not only check the data packets that may be going in and out of the system, but it also keeps any eye on the internal file system and keeps a log of the suspicious processes. Traffic monitoring tool is the networking tool that is used to examine usage of local area network and provide a statistical data of uploads and downloads in a network. It is supported by all windows based operating system. With network traffic monitoring one can easily filter the content and focus on the required data.

A well composed statistical data is very helpful in understanding the network performance and also can be used to fix bugs that may be present in a network.

REFERENCES

[1] IEEE paper on " Role of intrusion detection system" John Mchugh, Alan.
[2] Book on " Intrusion Detection" , Edward g
[3] http://www.robertgraham.com/pubs/hostbased-intrusion-detection.html
[4] www.securitydocs.com/library/3009
[5] Book on "C : The complete reference', Hilbert Schild
[6] Book on "SNMP Management", Mani Subramaniam.

AUTHORS

First Author – Prof. Naveen Kumar, Computer Science & Engineering, B.V.P.C.O.E.P
Second Author – Sheetal Angral, Computer Science & Engineering, B.V.P.C.O.E.P
Third Author – Rohan Sharma, Computer Science & Engineering, B.V.P.C.O.E.P