XB@ND Implementation for Intrusion Detection System

Manoj Singh
M.Tech (Comp. Science)
Kautilya Inst. of Technology & Engineering,
Jaipur(Ra.j)

Sunil Pathak
Asso. Prof.(Deptt. Of CSE)
Kautilya Inst. Of Technology & Engineering,
Jaipur(Raj)

Abstract

Security has been the concern in every aspect of our daily life. New ways and instruments have been devised to ensure privacy. In the same way, computer network is the field which has and is still facing lots of threats. Firewall has been useful for certain type of attacks but it has its own limitations and can be bypassed. Intrusion detection is the method of identifying unauthorized use, misuse, and abuse of computer systems by both system insiders and external attackers. This paper provides an overview of the motivation behind IDS and IPS, its advantages, disadvantages and limitations using implemented XB@ND software. We can effectively protect the computer systems, if we use three fundamental techniques against intrusions: prevention, detection and response. Such preventive measures include user authentication (using passwords or biometrics), fencing around the network using firewalls, very tight access control mechanisms, avoiding programming errors etc. In the end, we conclude with the provision of further future directions for handling the intrusions more effectively.

Index Terms -Firewall, Intrusion Detection System, Intrusion Prevention System, Intrusion Detection Prevention System.

1. Introduction

Computer Networks have seen a tremendous growth in the previous couple of decades. Most of the organizations have shifted to electronic storage and communication of their data through the computer networks. Just like in manual storage and communication of data, organizations need to maintain security of data. Unfortunately, it is really hard to attain ample security level, as due to scalability and variety of users, networks are always prone to attacks from outside and inside as well. With the increased use of computers and easy access to internet, the ways to attack and deceive a system has also increased. And hence it has escalated the need of adoption of some security mechanism. Currently, antivirus software, pass phrases, cryptography and firewall etc are used. But still optimizations are required due to design restrictions and the limitations of implementation. Cryptographic algorithms have a draw back as passwords can be broken easily. Firewalls can prevent the system from being attacked by the outside attacker but can be intruded and bypassed by the insiders easily. Therefore, the need of Intrusion Detection System (IDS) arose and has become the second, rather last line of defense. In this paper, we investigate different types of IDS and their corresponding approaches that are currently in use. Additionally, with the popularity and maturity of cluster computing in the last decade, especially the use of High Performance Computing (HPC) clusters and grid have become a vital part for future IDS based solutions [5].

This paper is assembled as follows. Section 2 describes the firewall, its types and drawbacks. Section 3 is about the IDS, its types, methods, characteristics and drawbacks of each method.. Section 4 presents the XB@ND an implementation of intrusion prevention system (IPS), its characteristics.

2. Firewall

Firewall is a common security defense and nowadays is treated as an integral part of every network. It was supposed to exist between any two networks [3], but with increase in popularity of internet and small networks, it has become a part and parcel of every gateway for preventing external intruders from gaining access to the local/private network. The most valuable function of firewall is filtering, i.e. diverting incoming traffic according to pre-defined policy,

which can protect the system from flooding type attacks. Hence, firewall guards the front door and is treated as the first line of defense. Basic firewall installation is shown in figure 1. Several types of firewalls, ranges from packet level to proxy firewalls, some of them are discussed below:

A. Static Packet filtering firewalls

Such firewalls sort the packets according to allow/deny rules, based on header fields information such as host/ destination address or port numbers etc. They do not perform deep analysis (malicious code detection in the packet) and treats each packet as an individual entity. The main disadvantage is that, it cannot resist well against fragment and spoofing attacks.

B. Stateful packet filtering firewalls

These firewalls have notion of states. Generally, in client server environment; client requests to server and receives responses against these requests. Since, generally client initiates communication, therefore server responses are allowed in bypassing the firewall rules. This optimizes the screening process, which increase the overall firewall performance. These firewalls require some resources, such as memory for maintaining state tables.

C. Proxy firewalls

These firewalls have ability to isolate internal network within the internet. They analyze the protocol syntax by breaking up client/server connection. Main disadvantage is that, they need lot of network resources.

The Firewalls [5] are just rules on which they allow or deny packets of an IP address. Today's Denial of Service (DoS) attacks are too complex for the firewall, because it could not distinguish good traffic from DoS attack traffic.

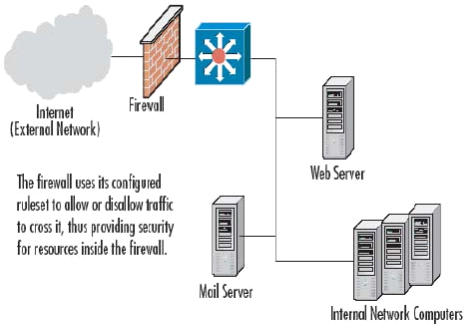

Figure 1. Basic Firewall Installation [4]

3. Intrusion Detection System (IDS)

Firewalls have been used for security in the networks since long but they can be easily deceived as a lot of techniques for deceiving the firewall have been developed [3]. Tunneling is one of the techniques used to bypass the firewall; one can envelop message for a protocol inside some other message format. Another method is to route the illegitimate traffic through some other unauthorized route. We know that firewalls sniff the packets at the border i.e. between the networks, and have nothing to do with the traffic flowing inside the network. So it is not useful for the attacks generated from inside the network. An intrusion is defined as "any set of actions that attempt to compromise the integrity, confidentiality, or availability of a computer resource" [6]. The definition disregards the success or failure of those actions, so it corresponds to attacks against the computer systems. Hence, an intrusion detection system (IDS) is a piece of software that monitors a computer system to detect any intrusions, and alerts a designated authority. Intrusion Detection systems can be classified in several ways. Depending on the source of data, the intrusion detection systems are categorized into host-based or network-based systems. The network-based intrusion detection systems process the data that originates on the network, such as TCP/IP traffic. Malformed packets, packet flooding, probes are some of the attacks which can be detected by such systems. The host-based intrusion detection systems analyzes the data that originates on computers (hosts), such as application and operating system event logs, system call traces. Such systems are effective for insider threats. Abuse of privileges by insiders, accesses of critical data is some of the attacks which can be detected by these systems. Intrusion detection systems can also be classified, depending on the detection model used, into misuse or anomaly detection models. Misuse detection systems look for well-defined patterns of known attacks. The known attacks are represented as *patterns* or *signatures.* Misuse Detection is therefore, simply a problem of matching patterns of attack in the given source of data. Such systems detect patterns of known attacks quite accurately and efficiently, and generate very few false alarms. The limitation of misuse detection is that it cannot detect novel, unknown attacks or variations of known attacks. In addition, misuse detection requires the nature of attacks to be well understood. This implies that human experts must work on the analysis and representation of attacks, which is usually time consuming and error prone. Anomaly detection is based on the normal behavior of the subject *{e.g.*, a user, program or a system). Any action that

significantly deviates from the normal behavior is considered as intrusive. Such systems build a statistical or machine learning model of normal behavior of the subject. The model is basically a list of metrics or patterns that capture the normal profile. The system flags an intrusion if any observed metrics or patterns of given behavior significantly deviate from the model. Such systems can detect previously unknown patterns of attacks but usually generate many false positives (normal behavior classified as intrusive). Another common problem is that since a subject's normal behavior is modeled on the basis of the audit data over the period of normal operation and if undiscovered intrusive activities occur during this period, they will be considered as normal activities. Intrusion detection systems can also be classified by their mode of operation: real-time or off-line. A real-time IDS monitors the system continuously and reports intrusions as soon as they are detected. Such systems can substantially reduce the damage to the system, if the system administrator can be notified as early as possible. Moreover, there is a great chance of stopping the attack currently in progress and catching the intruder as intruder would not get much time to delete his trail *{e.g.,* by erasing logs). An off-line IDS inspects system logs at periodic intervals and then discovers any suspicious activity that was recorded. Such systems are very effective in correlating attacks that span multiple hosts, slow probing attacks that span over hours and days, and for forensic analysis. An offline IDS typically reduces system overhead but gives much less timely notification of intrusions. Lastly, intrusion detection systems can be categorized based on their architecture. The most common IDS architectures are: centralized, hierarchical or distributed systems. In centralized IDS, the data may be collected from various sources (hosts or networks) but is sent to a centralized location where it is analyzed. Such systems limit the system scalability as it could become bottleneck on increasing number of sources and also represent a single point of vulnerability. In hierarchical IDS, some of the data collected from multiple hosts or a single host is passed up through the layers and is analyzed to varying degree at each level. In Distributed IDS, the data is collected and analyzed across the entire network being monitored and results are then sent to a centralized location. Such systems are scalable and not subject to a single point of failure. Figure 2 describes the standard network intrusion detection architecture.

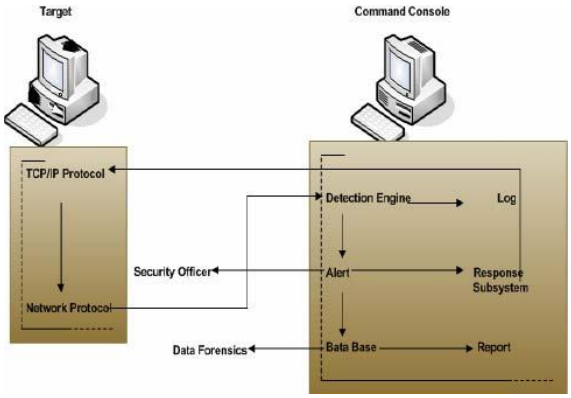

Figure 2. A Standard Network Intrusion Detection Architecture[6]

Desirable characteristics of an intrusion detection system

Crosbie and Spafford [1] define the following desirable characteristics of an intrusion detection system:

- It must run continually with minimal human supervision.
- It must be fault tolerant by being able to recover from accidental system crashes and re-initializations.
- It must resist subversion. The intrusion detection system must be able to monitor itself and detect if it has been attacked or modified by an attacker.
- It must impose a minimal overhead on the system where it is running, to avoid interfering with the system's normal operation.
- It must be scalable to monitor a large number of hosts while providing results accurately and without degradation of performance.
- It must provide graceful degradation of service. The failure of any component of the intrusion detection system should not immediately fail the entire system.
- It must allow dynamic reconfiguration, allowing the system administrator to make changes in it's configuration without restarting the whole intrusion detection system. While building a new intrusion detection system, these above characteristics of IDS should always be kept in mind. It would not be easy to include all the characteristics as there will always exist some trade-offs between these characteristics.

4. XB@ND : Implementation Of IDS

•Authentication. Authorization and Accounting Gateway

Passport provides a mechanism which allows user on a closed network to gain rights to use network services as defined in the profile created for the particular user. It will authenticate a user on the basis of

1. IP /Mac/User id
2. Type (administrator/user)

•Bandwidth Control

This module basically features on controlling the bandwidth requirements of the Network/Users. This also deals with dynamically setting up of bandwidth requirements. This will be done accordingly

1. By defining bandwidth requirements on a particular user/IP/Pool/Time/Protocol*.
2. Restrictions on bandwidth requirements for upload and download data transfer.
3. Should also give the total bandwidth status of bandwidth available/used on the passport server. Since passport is directly on the Internet backbone & the LAN is further connected a cumulative status of bandwidth on passport is desirable to see the overall status of the network.

•Network Security

Restricting the traffic on the basis of

1. Specific/Generic URLs, Source–IP, Destination-IP, Source Port, Destination Port, Expressions, Phrases.
2. Blocking the NetBIOS and NetBEUI traffic.
3. Ability to deal with Denial of Service Attacks
4. Reduction of Network Congestion
5. Restricting the traffic of a particular application at any point of time for e.g. restricting the FTP/mails during times when its critical (i.e. virus attacks etc.)
6. Scheduled access control. This will be used to configure to allow or deny access at specific periods. For example, this could be used to limit the amount of time staff can browse the web during the working day.
7. Stateful inspection: Stateful Inspection architecture intercepts, analyzes, and takes action on all communications before they enter the operating system of the gateway machine, ensuring the full security and integrity of the network and the gateway itself. Any traffic not explicitly allowed by the security rules is dropped by default and real-time security alerts and logs are generated, providing the system manager with complete network status.
8. Logging: Firewall events can be selectively logged to physical medium. This will detect and log range of denial of service attacks including SYN and FIN flooding, ping of Death, Smurf Packets and port scans.
9. Anti-virus Solution support: Server takes care of the viruses in the network servers & workstations (including mobile users) from the main machines. This would ensure a virus free environment in the complete network.

•Network Connectivity

Should be able to support connectivity through:

1. Ethernet LANs.
2. Wireless LANs.
3. Cable Modems.
4. DSL Networks.
5. Tel Lines of Data compatible EPABX through RAS.

•Interface for Users

Facilitate the user interface with following facilities

1. Change of password
2. Change of Secret Questions
3. View Profile
4. View Statistics

•Messaging and Brand Image

This includes creation, sending and management of messages for

1. For various notifications Package expiry, Renewal Details, network problems, package details and Modifications. These messages exemplify the above module

a) You have been deactivated by the Administrator
b) You have been disconnected by the administrator
c) You are not allowed to login from this machine
d) You have used up your allotted surfing time, so you have been disconnected from the Internet
e) Wrong username/password

2. For troubleshooting
3. For advertisement

•Network Trouble Shooting and Monitoring Wizard

This module is used by the administrator for:

1. Monitoring the bandwidth usage on daily/weekly/fortnightly/monthly and yearly basis.
2. The Passport administrator could control and monitor its passport customers by storing their information in a management information base (MIB) .Now using SNMP and these MIB values it can control, administer, and troubleshoot his customers remotely.
3. Checking the status of Passport Server, Gateways, DNS Servers, and Cache Server.
4. Checking the status of Users (Active, Inactive, Online, and Offline).
5. Troubleshooting a particular user.
6. Real Time Web Based Monitoring.

•User Data Backup and Restore facility

•System Services Modules

This module will manage and configure various system services which include

1. Configuration and management of Routing, DNS servers, Cache Server, DHCP Server, Passport Server.
2. Starting and Stopping of remote services.
3. Supporting Multiple Gateways.
4. Cache Management

- **Extensive reporting (Graph and Tabular)**

For each host, passport records the following information:

- **Data sent/received**: The total traffic (volume and packets) generated or received by the host classified according to network protocol (IP, IPX, AppleTalk, etc.) and, when applicable, IP protocol (FTP, HTTP, NFS, etc.).
- **TCP session's history**: The list of currently active TCP sessions established/accepted by the host and associated traffic statistics.
- **UDP traffic**: The total amount of UDP traffic (volume and packets) sorted by port. It is worth noting that it is possible to recognize simple port scan and protocol scan (e.g., an SNMP manager issued SNMP requests to a given host) when the host has received packets at a specified port but has sent no data.
- **TCP/UDP used services**: The list of IP based services (e.g., open and active ports) provided by the host with the list of the last five hosts that used them.
- **Operating system (OS) type**: The operating system of the host is identified.
- **Used bandwidth percentage**: Actual, average, and peak bandwidth usage.
- **Traffic distribution**: Local (subnet) traffic, local vs. remote (outside specified/local subnet), remote vs. local.
- **IP traffic distribution**: UDP vs. TCP traffic; relative distribution of the IP protocols according to the host name.
- **Local network usage**: Statistics about open sockets, data sent/received, and contacted peers for each process running on the host.

In addition, passport reports **global traffic statistics**, including:

- **Traffic distribution**: Local (subnet) traffic, local vs. remote (outside specified/local subnet), remote vs. local.
- **Packet distribution**: Total number of packets sorted by packet size, unicast vs. multicast vs. broadcast, and IP vs. non-IP traffic.
- **Used bandwidth**: Actual, peak, and average bandwidth usage.
- The list of **active TCP sessions** for each known host.
- **Protocol utilization and distribution**: Distribution of the observed traffic according to both protocol and source–destination (local vs. remote).
- **Local subnet traffic matrix**: 2D matrix where each cell (X, Y) contains the traffic sent by host X to host Y, where X and Y are hosts that belong to the local subnet of the host where passport is running.
- **Network Flows**: Traffic statistics for each user-defined flow.
- **Use of duplicate IP addresses**.
- **Identification of all the subnet routers** so that it is possible to find out whether a misconfigured host wrongly believes it acts as a router for the local subnet or a host is using a wrong netmask for the actual network.
- **Protocol misuse:** Identification of those computers that speak unnecessary protocols. For instance, the Windows OS installs by default protocols such as NetBEUI and IPX, while most people use just TCP/IP.
- **Excessive network bandwidth utilization**: In organizations where the Internet connection has limited bandwidth, it is important to detect the hosts/users that use most of the available bandwidth. For

instance, this can be done by either tracking traffic values for certain protocols (i.e., HTTP or FTP) or identifying hosts with connections established with remote hosts.

6. Conclusion

In this paper we surveyed the effectiveness and upcoming challenges of security needs in a network environment, especially a larger one. security, their types and detection schemes along with summarizing basic details of Firewall, IDS, IPS and IDPS. Such tools are used for securing networks form intruders, so this requires enhancement and evolution with the time. Research allows highlighting multiple ways to encounter the attacks. Over the time attackers seek new evasion techniques, so it is necessary to replace existing system with new one but it may be troublesome such as cost. There should be mechanisms to enhance the existing system rather than replacing it every time. Network security tools should be based on incremental model theory.

Intrusion detection has different types and each type has strength with its radius. Therefore, it is recommended to take account of corresponding threats while opting for IDS. It should also meet future requirements and allows enhancements with minimum cost and structural changes. It is therefore recommended to use hybrid system for the security. IDS with the rule based techniques work well, but these rules are human coded, so there is chance of error (attack may be interpreted wrong by the programmer). Hence, there must exist a tool that suggests better way to the human, to guide different ways of network traffic interpretation, however, its correct understanding is a difficult task. Intrusion detection and prevention systems analyze packets deeply. During this process it is possible that administrator reveals sensitive and confidential information about the users.IDS and IPS are security tools but attaining 100% satisfaction and security is still not possible. Therefore combination of both may provide in-depth security.

References

[1] M. Crosbie and E. Spafford. Active defense of a computer system using autonomous agents.
Technical Report 95-008, COAST Group, Department of Computer Science, Purdue
University, Feb 1995

[2] R. Heady, G. Luger, A. Maccabe, and M. Servilla. The architecture of a network level
intrusion detection system. Technical report, University of New Mexico, Department of
Computer Science, August 1990.

[3]Rebecca Bace, "An Introduction to Intrusion Detection and Assessment for System and
network security Management", ICSA, Inc
http://www.icsalabs.com/icsa/docs/html/communities/ids/whitepaper/Intrusion1.pdf

[4]Vera Marinova-Boncheva, "A Short Survey of Intrusion Detection Systems", Problems of
Engineering Cybernetics and Robotics, 58, 2007. http://www.iit.bas.bg/PECR/58/23-30.pdf

[5]Dinesh Sequeira, "Intrusion Prevention Systems-Security's Silver Bullet?", SANS Institute InfoSec Reading Room 2002. http://www.sans.org/reading_room/whitepapers/detection/intrusion_prevention_systems_securitys_silver_bullet_366? show=366.php&cat=detection

[6]Harley Kozushko, "Intrusion Detection: Host-Based and Network-Based Intrusion Detection Systems",2003http://infohost.nmt.edu/~sfs/Students/HarleyKozushko/Papers/IntrusionDetectionPaper.pdf