NETWORK INTRUSION DETECTION AND PREVENTION ATTACKS

Harpreet Kaur
C.Sc. Dept.
S.R.Govt. College (W), Amritsar

Abstract

Intrusion detection is an important technology in business sector as well as an active area of research. It is an important tool for information security. A Network Intrusion Detection System is used to monitor networks for attacks or intrusions and report these intrusions to the administrator in order to take evasive action. Today computers are part of networked; distributed systems that may span multiple buildings sometimes located thousands of miles apart. The network of such a system is a pathway for communication between the computers in the distributed system. The network is also a pathway for intrusion. This system is designed to detect and combat some common attacks on network systems. It follows the signature based IDs methodology for ascertaining attacks. A signature based IDS will monitor packets on the network and compare them against a database of signatures or attributes from known malicious threats. In this system the attack log displays the list of attacks to the administrator for evasive action. This system works as an alert device in the event of attacks directed towards an entire network.

KEYWORDS: *INTRUDERS, INFORMATION SECURITY, REAL TIME IDS, ATTACKS, SIGNATURE, DISTRIBUTED SYSTEM, DETECTION.*

1. INTRODUCTION

With the development of network technologies and applications, network attacks are greatly increasing both in number and severity. As a key technique in network security domain, Intrusion Detection System (IDS) plays vital role of detecting various kinds of attacks and secures the networks. Main purpose of IDS is to find out intrusions among normal audit data and this can be considered as classification problem. Intrusion detection systems (IDS) are an effective security technology, which can detect, prevent and possibly react to the attack. It performs monitoring of target sources of activities, such as audit and network traffic data in computer or network systems, requiring security measures, and employs various techniques for providing security services. With the tremendous growth of network-based services and sensitive information on networks, network security is becoming more and more important than ever before. Symantec in a report uncovered that the number of fishing attacks targeted at stealing confidential information such as credit card numbers, passwords, and other financial information are on the rise,.One solution to this is the use of network intrusion detection attacks by observing various network activities. It is therefore crucial that such systems are accurate in identifying attacks, quick to train and generate as few false positives as possible. This paper presents the scope and status of our research in misuse detection Experimental results have demonstrated that this model is much more efficient in the detection of network intrusions, compared with network based techniques. Finally, provides the concluding remarks and future scope of the work.

2. NETWORKING ATTACKS

A Network Intrusion Detection System is used to monitor networks for attacks or intrusions and report these intrusions to the administrator in order to take evasive action. A large NIDS server can be set up on a backbone network, to monitor all traffic; or smaller systems can be set up to monitor traffic for a particular server, switch, gateway, or router. It has been shown in fig. 1.

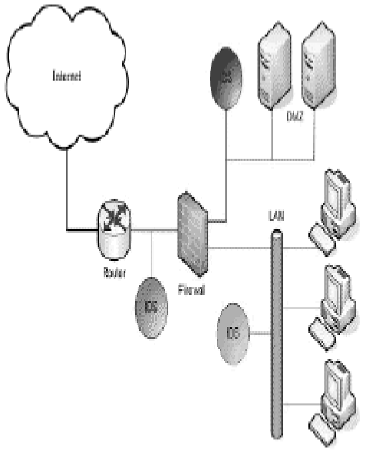

FIGURE 1: Computer network with Intrusion Detection Systems

Intrusion detection is needed in today's computing environment because it is impossible to keep pace with the current and potential threats and vulnerabilities in our computing systems. The environment is constantly evolving and changing field by new technology and the Internet. Intrusion detection products are tools to assist in managing threats and vulnerabilities in this changing environment. Threats are people or groups who have the potential to compromise your computer system. These may be a curious teenager, a disgruntled employee, or espionage from a rival company or a foreign government

Attacks on network computer system could be devastating and affect networks and corporate establishments. We need to curb these attacks and Intrusion Detection System helps to identify the intrusions. Without an NIDS, to monitor any network activity, possibly resulting in irreparable damage to an organization's network Intrusion attacks are those in which an attacker enters your network to read, damage, and/or steal your data.

These attacks can be divided into two subcategories: pre intrusion activities and intrusions.

2.1 Pre intrusion activities

Pre intrusion activities are used to prepare for intruding into a network. These include port scanning to find a way to get into the network and IP spoofing to disguise the identity of the attacker or intruder.

• **Port scans**: A program used by hackers to probe a system remotely and determine what TCP/UPD ports are open (and vulnerable to attack) is called a scanner. A scanner can find a vulnerable computer on the Internet, discover what services are running on the machine, and then find the weaknesses in those services. There are 65,535 TCP ports and an equal number of UDP ports. Stealth scanners use what is called an IP half scan, sending only initial or final packets instead of establishing a connection, to avoid detection.

• **IP spoofing**: This is a means of changing the information in the headers of a packet to forge the source IP address. Spoofing is used to impersonate a different machine from the one that actually sent the data. This can be done to avoid detection and/or to target the machine to which the spoofed address belongs. By spoofing an address that is a trusted port, the attacker can get packets through a firewall.

Various intrusions into the network are given as follows:

• **Source routing attack**: This is a protocol exploit that is used by hackers to reachprivate IP addresses on an internal network by routing traffic through another machine that can be reached from both the Internet and the local network . TCP/IP to allow those sending network data to route the packets through a specific network point for better performance supports source routing. Administrators to map their networks or to troubleshoot routing problems also use it.

• **Trojan attacks**: Trojans are programs that masquerade as something else and allow hackers to take control of your machine, browse your drives, upload or download data, etc. For example, in 1999, a Trojan program file called Picture.exe was designed to collect personal data from the hard disk of an infiltrated computer and send it to a specific e-mail address. So-called Trojan ports are popular avenues of attack for these programs.

• **Registry attack**: In this type of attack, a remote user connects to a Windows machine’s registry and changes the registry settings. To prevent such an attack, configure permissions so that the every one group does not have access.

• **Password hijacking attacks**: The easiest way to gain unauthorized access to a protected system is to find a legitimate password. This can be done via social engineering or using brute force method.

2.2 System Description

2.2.1 Packet Sniffer

This module involves capturing all traffic passing through the network. The sniffer will be installed on the end system in a network on which the traffic has to be captured. The sniffer capturesall network traffic by operating the network adapter in promiscuous mode.

2.2.2 Determination of attack signatures

Attack Signatures refers to the pattern of attack traffic. Signatures are modeled based on the packet header pattern a particular attack follows. It involves a count of packets from a particular target or a particular source or destination port or it may even be modeled with the help of other details in the packet such as header size, Time to Live (TTL), flag bits, protocol.

2.2.3 Identification of attacks

This involves extracting useful information from captured local traffic such as source and destination IP addresses, protocol type, header length, source and destination ports etc and compare these details with modeled attack signatures to determine if an attack has occurred.

2.2.4 Reporting attack details

This involves reporting the attack to the administrator so that he may take evasive action.

Reporting involves specifying attack details such as source and victim IP addresses, time stamp of attack and more importantly the type of attack.

2.3 Experimental Results

2.3.1 Signature based intrusion detection

Signature-based IDSs operate analogously to virus scanners, i.e. by searching a database of signatures for a known identity – or signature – for each specific intrusion event. In signature-based IDSs, monitored events are matched against a database of attack signatures to detect intrusions.

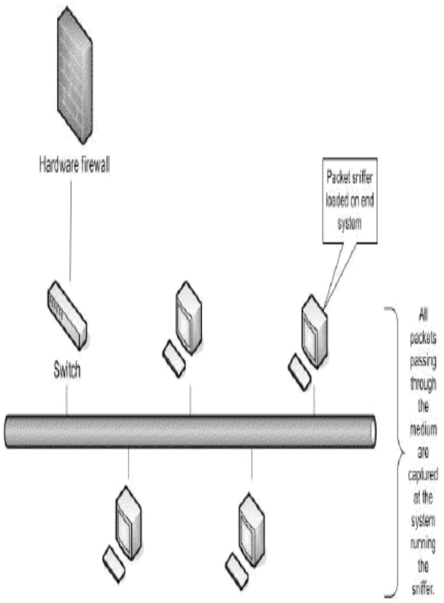
Hardware firewall
Packet sniffer loaded on end system
Switch
All packets passing through the medium are captured at the system running the sniffer.

FIGURE 2: IDS in Promiscuous mode

Signature-based IDS [15] are unable to detect unknown and emerging attacks since signature database has to be manually revised for each new type of intrusion that is discoveredThis system follows the signature based IDs methodology for ascertaining attacks. A signature based IDS will monitor packets on the network and compare them against a database of signatures [19] or attributes from known malicious threats.

Most intrusion IDS are signature based. This means that they operate in much the same way as a virus scanner, by searching for a known attack or signature for each specific intrusion event. And, while signature-based IDS is very efficient at sniffing out known attack, it does, like anti-virus software, depend on receiving regular signature updates, to keep in touch with variations in hacker technique. Because signature based IDS can only ever be as good as the extent of the signature database, wo further problems immediately arise. Firstly, it is easy to fool signature-based solutions by changing the ways in which an attack is made. This technique simply skirts around the signature database stored in the IDS, giving the hacker an ideal opportunity to gain access to the network. This can be overcome by using defense in depth technique. Secondly, the more advanced the signature database, the higher the CPU load for the system charged with analyzing each signature. Inevitably, this means that beyond the maximum bandwidth packets may be dropped. We have overcome these problems in our IDS system by using capture drivers that support network of up to 1GBPS (Giga bits per second). Network Traffic

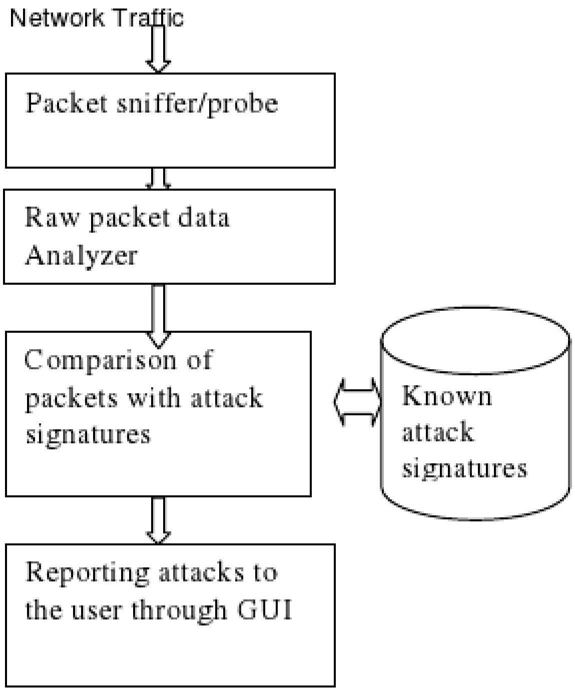
Network Traffic
Packet sniffer/probe
Raw packet data Analyzer
Comparison of packets with attack signatures
Known attack signatures
Reporting attacks to the user through GUI

Fig3. Implementation Architecture

2.3.2 Packet sniffing and promiscuous mode

Packet sniffers generally require that a network interface is in promiscuous mode. The packetsniffer normally requires administrative privileges on the machine being used as a packet sniffer,

2.4 Testing tool

We have used Karalon traffic IQ professional [11, 24] for testing our software with intrusionattacks. Traffic IQ Professional provides a unique industry approved software solution for auditingand testing the recognition and response capabilities of Intrusion detection systems.

Features include

- Traffic Replay
- Traffic scan list
- Reporting
- Traffic file editor
- Command prompt
- Traffic library

3. CONCLUSION

We have successfully created a network based intrusion detection system with signature IDSmethodology. It successfully captures packets transmitted over the entire network by

promiscuous mode of operation and compares the traffic with crafted attack signatures. The attack log displays the list of attacks to the administrator for evasive action. It may be incorporated with further signatures for attacks. The types of attacks share the characteristic that upon their initiation and while they are in progress, Global attack and of distributed intrusion detection processes produce sufficient network traffic (e.g. port scanning) so that local detectors can find sufficient evidence of the attack and report the attacks.

REFRENCES:

[1].http://www.networkcomputing.com/1116/1116ws3side1.html

[2.]Mirkovic, L., Dietrich, S., Dittrich, D. and Reiher, P. (2005). *Internet Denial of Service – Attack and Defense Mechanisms*.

[3].Northcutt, S. (1999). *Network Intrusion Detection – An Analyst's Handbook.*

Northcutt, S., Zeltser, L., Winters, S. Frederick, K. K. and Ritchey, R. H. (2003) *Inside*

Network Perimeter Security. Scarfone, K. and Mell, P. Guide to intrusion detection and prevention systems (IDPS). http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

[4].Detection and Prevention.

http://cse.seas.wustl.edu/Research/FileDownload.asp?176

[5.]Zhou, C. V., Karunasekera, S. and Leckie, C. A Peer-to-Peer Collaborative Intrusion Detection System. http://www.cs.mu.oz.au/~cvzhou/pub/icon05.pdf

[6.]Dubin, J. Intrusion detection and prevention: More than a firewall.

http://searchsmb.techtarget.com/tip/0,289483,sid44_gci1267542,00.html

[7.]Endorf, C, Schultz, E and Mellander, J. (2004) Intrusion Detection and Prevention. Huang, N-F. Intrusion detection and prevention system (IPS) –Technology, applications, and trend. http://www.apan.net/meetings/taipei2005/presentation/APAN_IPS_NFHUANG_0826-2005.pdf

[8].Intrusion Detection Systems using Snort. [Y. Liang and A. Kelemen.(2009) "Time lagged recurrent neural network for temporal gene expression classification," International Journal of Computational Intelligence in Bioinformatics and Systems Biology.

[9.]Rebecca C. Leng, (May 4, 2009). Review of web applications security and intrusion detection in air traffffic.