Network Intrusion detection using correlation functional dependency

NITIN D. SHELOKAR[1] and S.A. LADHAKE[2]

[1]Sipna College of Engineering, Amravati, (India).
[2]Department of Computer Science & Technology,
Bengal Engineering Science University, Shibpur, Howrah - 711 103 (India).

(Received: March 29, 2010; Accepted: May 11, 2010)

ABSTRACT

We will learn the concept of intrusion detection system in real time. This seminar will give brief idea to have our data to be in secured system i.e free from hackers. We will elaborate the types of intrusion detection system and get into concept of real-time system to detect any intruder coming into the system. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. We have also discussed the real time intrusion detection system in brief with the efficiency related to instruion detection systems. Data processed by the IDS may be a sequence of commands executed by an user, a sequence of system calls launched by an application (for example a web client), network packets, and so on. Finally, the IDS can trigger some countermeasures to eliminate attack cause/effect whenever an intrusion is detected.

Keywords: Intrusion detection system.

INTRODUCTION

An Intrusion detection system (IDS) is software and/or hardware designed to detect unwanted attempts at accessing, manipulating, and/or disabling of computer systems, mainly through a network, such as the Internet. These attempts may take the form of attacks, as examples, by crackers, malware and/or disgruntled employees. An IDS cannot directly detect attacks within properly encrypted traffic.

An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. This includes network attacks against vulnerable services, data driven attacks on applications, host based attacks such as privilege, unauthorized logins and access to sensitive files, and malware (viruses, trojan horses, and worms).

Computer systems and networks have been shown to suffer from security vulnerabilities, regardless of their propose, manufacturer, or origin. It is both technically difficult and expensive to ensure that an information system will not be harmed by attacks exploiting those vulnerabilities. Therefore, intrusion detection systems (IDS) are used to monitor systems during their lifetime and use to detect possible attacks against them.The information system being protected (application, computer and/or network) is usually submitted to a usage configuration or policy that describes legitimate actions allowed to each entity (user, host or service) profile. Audit data describing entity actions or system states are generated (even systematically or trigged by the IDS) and then analyzed by the IDS, which evaluates the probability of these states or actions being related to an intrusion. Data processed by the IDS may be a sequence of commands executed by an user, a sequence of system calls launched by an application (for example a web client), network packets, and so on. Finally, the IDS can trigger some countermeasures to eliminate attack cause/effect whenever an intrusion is detected.

Concerning the analysis method, IDS are usually classified in two categories. A misuse or knowledge-based IDS aims at detecting the occurrence of state or action sequences that has been previously identified to be an intrusion. Thus, in this kind of IDS attacks must be known and described a priori and IDS are usually unable to deal with new or unknown attacks. Alternatively, an anomaly or behavior-based IDS assumes that an intrusion can be detected by observing deviations from a normal or expected behavior of a monitored entity. The valid behavior is extracted from previous reference information about the system. The IDS later compares the extracted model with the current activity and raises an alert each time that a certain degree of divergence from the original model is observed.

Types of Intrusion-Detection Systems

In a network-based intrusion-detection system (NIDS), the sensors are located at points in network to be monitored, often in the demilitarized zone (DMZ) or at network borders. The sensor captures all network traffic and analyzes the content of individual packets for malicious traffic. In systems, PIDS and APIDS are used to monitor the transport and protocols for illegal or inappropriate traffic or constructs of a language (say SQL). In a host-based system, the sensor usually consists of a software agent, which monitors all activity of the host on which it is installed. Hybrids of these two systems also exist.

- A network intrusion detection system (NIDS) is an independent platform which identifies intrusions by examining network traffic and monitors multiple hosts. Network Intrusion Detection Systems gain access to network traffic by connecting to a hub, network switch configured for port mirroring, or network tap. An example of a NIDS is Snort.
- A protocol-based intrusion detection system (PIDS) consists of a system or agent that would typically sit at the front end of a server, monitoring and analyzing the communication protocol between a connected device (a user/PC or system) and the server. For a web server this would typically monitor the HTTPS protocol stream and understand the HTTP protocol relative to the web server/system it is trying to protect. Where HTTPS is in use then this system would need to reside in the interface, between where HTTPS is un-encrypted and immediately prior to its entering the Web presentation layer.

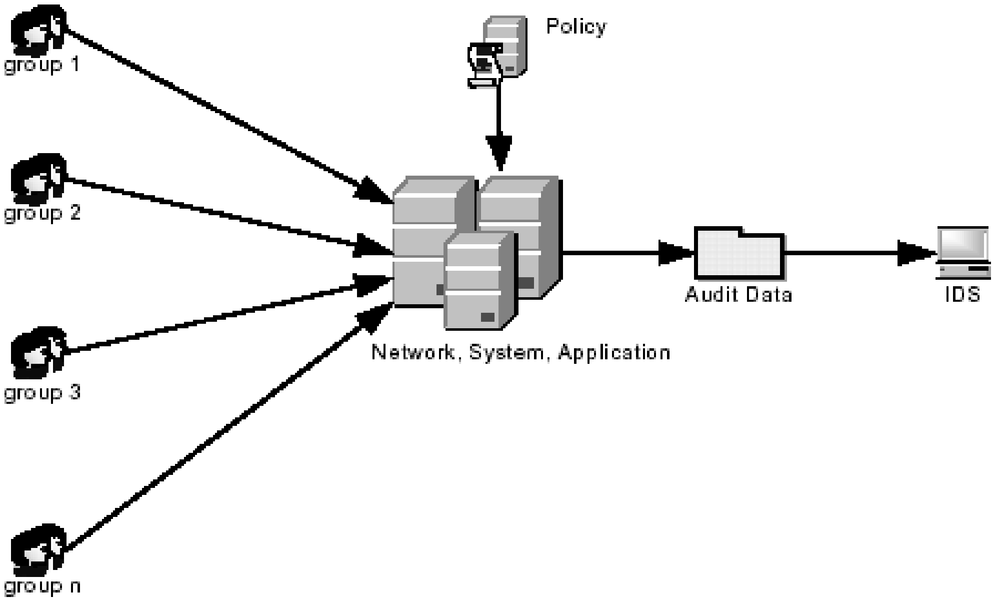

Fig. 1: Information System Entities and IDS.

- An application protocol-based intrusion detection system (APIDS) consists of a system or agent that would typically sit within a group of servers, monitoring and analyzing the communication on application specific protocols. For example, in a web server with a database this would monitor the SQL protocol specific to the middleware/business logic as it transacts with the database.
- A host-based intrusion detection system (HIDS) consists of an agent on a host which identifies intrusions by analyzing system calls, application logs, file-system modifications (binaries, password files, capability/acl databases) and other host activities and state.
- A hybrid intrusion detection system combines two or more approaches. Host agent data is combined with network information to form a comprehensive view of the network.

Generic Intrusion Detection System

The term system is used here to denote an information system being monitored by an intrusion-detection system. It can be a workstation, a network element, a server, a mainframe,a firewall, a web server, an enterprise network,etc.The term audit denotes information provided by a system concerning its inner workings and behavior. Examples of audits include but are not limited to C2 audit trail, accounting, and syslog in the UNIX world,Syslog in the MVS world, the event log in Windows NT, and incident tickets in X25 networks.

An intrusion-detection system dynamically monitors the actions taken in a given environment, and decides whether these actions are symptomatic of an attack or constitute a legitimate use of the environment. Therefore, with respect to this definition, we do not consider well-known tools such as Cops or Satan to be intrusion-detection systems; we consider them configuration analyzers, even though some of their functionalities can be used to detect intrusions.

An intrusion-detection system can be described at a very macroscopic level as a detector that processes information coming from the system. This detector uses three kinds of information: long-term information related to the technique used to detect intrusions a knowledge . base of attacks, for example, configuration information about the current state of the system, and audit information describing the events that occur on the system. The role of the detector is to eliminate unnecessary information from the audit trail and present a synthetic view of the security-related actions taken by users. A decision is then made to evaluate the probability that these actions can be considered symptoms of an intrusion.

Efficiency of intrusion-detection systems

The following measures to evaluate the efficiency of an intrusion-detection system are as follows:-

1. Accuracy. Inaccuracy occurs when an intrusion-detection system flags as anomalous or intrusive a legitimate action in the environment.
2. Performance. The performance of an intrusion-detection system is the rate at which audit events are processed. If the performance of the intrusion-detection system is poor, then real-time detection is not possible.
3. Completeness. Incompleteness occurs when the intrusion-detection system fails to detect an attack. This measure is much more difficult to evaluate than the others, because it is impossible to have a global knowledge about attacks or abuses of privileges.
4. Fault tolerance. It should itself be resistant to attacks, particularly denial of service, and should be designed with this goal in mind. This is particularly important because most intrusion-detection systems run on top of commercially available operating systems or hardware, which are known to be vulnerable to attacks.
5. Timeliness. It has to perform and propagate its analysis as quickly as possible to enable the security officer to react before much damage has been done, and also to prevent the attacker from subverting the audit source or the intrusion-detection system itself. This implies more than the measure of performance, because it not only encompasses the intrinsic processing speed of the intrusion detection system, but also the time required to propagate the information and react to it.

CONCLUSION

With this seminar we have studied the intrusion detection system in detail. An intrusion detection system is used to detect several types of malicious behaviors that can compromise the security and trust of a computer system. We have also discussed the real time intrusion detection system in brief with the efficiency related to instruion detection systems. Data processed by the IDS may be a sequence of commands executed by an user, a sequence of system calls launched by an application (for example a web client), network packets, and so on. Finally, the IDS can trigger some countermeasures to eliminate attack cause/effect whenever an intrusion is detected.

REFERENCES

1. Paper on Towards a taxonomy of intrusion-detection systems by herve Debar.
2. Real Time Systems - James Liu
3. www.securityfocus.com/ The Evolution of Intrusion detection Systems.htm
4. Paper on A Model-based Real-time Network Intrusion Detection System.