Intrusion Detection

Contents

List of Table

1 Introduction

Intrusion detection has been define as ”The problem of identifying individuals who are using a computer system without authorization and those who have legitimate access to the system but are abusing their privileges (i.e., the insider threat)”[1]. In fact intrusion detection help to examine all inbound and outbound network movement and recognize doubtful patterns that may point out a network or system attack. It is a alarm (instruction alarm) of the computer, So that computer can secure. This alarm help to inform security officer to take action against unauthorized user. Intrusion can be different type like user can may be still password by prove fake identity to the computer mean it make to realize the computer that actual user accessing the system. This user called as *masquerader*. Other significant classes of intruders are people who are lawful users of the system but who exploitation their privileges, and people who use pre-packed exploit scripts, often found on the Internet, to attack the system through a network.

An intrusion detection scheme consists of an audit data collection mediator that gather information about the system being observed. In intrusion data accumulate or processed directly by the detector from the output of this security office take more action. Normally this alarm help to investigate thoroughly

2.Intrusion detection & prevention principles

The intrusion detection system (IDS) is a kind of software which automatically help to the intrusion detection process. An intrusion prevention system (IPS) is also software but that has all the ability of an intrusion detection system and can also try to prevent unexpected occurrence.

Last couple of years intrusion detection system(IDS) and intrusion prevention system (IPS) are developed extremely. In some case they are integrated each other(intrusion detection system(IDS) and intrusion prevention system (IPS)) and both are work simultaneously. This technology merge with network device or as it is commonly referred to, one "appliance."[ ]

Technical Overview

In Table 1.a shows classification of detection principal Basically intrusion detection can be describe in two categories

- Network-based intrusion detection systems (NIDS)
- Host-based intrusion detection systems (HIDS)

anomaly	self-learning	non time series	rule modelling	W&S A.4[a]
			descriptive statistics	IDES A.3, NIDES A.14, EMERALD A.19, Ji-Nao A.18, Haystack A.1
		time series	ANN	Hyperview(1)[a] A.8
	programmed	descriptive stat	simple stat	MIDAS(1) A.2, NADIR(1) A.7, Haystack(1)
			simple rule-based	NSM A.6
			threshold	ComputerWatch A.5
		default deny	state series modelling	DPEM A.12, JANUS A.17, Bro A.20
signature	programmed	state-modelling	state-transition	USTAT A.11
			petri-net	IDIOT A.13
		expert-system	NIDES A.14, EMERALD A.19, MIDAS-direct A.2, DIDS A.9, MIDAS(2) A.2	
		string-matching	NSM A.6	
		simple rule-based	NADIR A.7, NADIR(2) A.7, ASAX A.10, Bro A.20, JiNao A.18, Haystack(2) A.1	
signature inspired	self-learning	automatic feature sel	Ripper A.21	

Table 1: classification of detection principal

Network Intrusion Detection Systems (NIDS)

A network intrusion detection system is a kind of detection system which is detect or identify malicious activity like unexpected user attack ,port scan by monitoring network traffic. NIDS are located in to internet protocol so when they are transmitted packet across LAN or WAN it read or monitoring all packet and trying to find suspicious pattern. As an example , when large number of TCP connection needs to a very large number of different ports are monitored , it can be guess that there is someone try to port scan at some of the computer in the network . It also attempt to detect incoming machine code in the same manner that an ordinary intrusion detection do. This intrusion detection mechanism not only inspect incoming traffic only but it can judge outgoing traffic also and it can attack by monitoring network or network segment, and are consequently not observed as incoming traffic at all. This system can work along with other system like firewall which is blacklist the ip address of computer used by the unauthorized user.

Host Intrusion Detection Systems (HIDS)

As we described that a network intrusion detection system monitor external interface where as a host-based intrusion detection system (HIDS) check and examine the internals of a computing system which is main difference than HID. The HID is a one kind of program just like other software that is installed on a host computer and run in the background with other application. Examples of this technology are Enterasys Dragon HID, key logger ,Symantec Host Intrusion Prevention, and Tripwire.

The HIDS can be arranged to inspect all behavior on a computer, from unsuccessful log-in try to the recording of single keystrokes, to build a complete real-time picture of an individual's activities. A host-based system examine the algorithm to decide if a particular packet or movement is uncertain. All network and host-based intrusion detection systems employ one of two methods to determine whether something is uncertain or doubtful. The

action or packet which are coming to words the system will be match up to either against a database of signatures or of anomalies.

Signatures vs Anomalies

Signature-based system :

In signature-based intrusion detection examine the information it gather and compare it of his database of attack signature. Basically the IDS looks for a exact attack that has previously been documented . In simple manner it can be define that it compare against a database of known malicious threat. Its perform same as antivirus, the way it detect is the same as most antivirus detect malicious code. In Signature-based intrusion detection the only disadvantage is there is always a time gap between the detection of a new threat and the progress of a signature for detecting the threat, so that during this interval the IDS would be unable to detect the new threat.

Anomaly-based system

In anomaly detection system, network traffic load, break down, typical packet size and protocol breakdown are classify by the system administrator. This is build up over period of time, this varies with manufacture and indentifies what is suitable for the network or host. Basically An anomaly-based intrusion system monitors packets and activities and evaluate them against a baseline of record that are unique to a network .It also inspect

- Dates and times of access
- MAC and/or IP addresses of devices that connect to each other
- Ports commonly used on the network or host system
- Bandwidth utilization, also characterized as “interface use”
- Protocols used on the network or host

The main disadvantage of this system is when baseline is under developed that time system doesn't know what is going on and it can be at risk. Partially this risk can be manageable by pre configuring expected behavior. but the good strategy allow the IDS to build base line itself and it will aware the administrator or user when something unexpected will detect in the traffic.

3.Intrusion Prevention

Instruction prevention is essential for every computer, because it protect computer from real damage. Between Instruction prevention and Instruction detection have little different from each other, Instruction prevention first examine the system or network traffic if find something wrong and determine that malicious attack is moving ahead then it inform or notify someone or security officer to take action against this attack. Due to for advanced technology Now a day's usual detection systems have included the capability not only to alert and recommend but also take practical steps to prevent a compromise . But proper intrusion prevention systems most often take the form of host-based or software firewalls like Zone Alarm or Black ICE[3]. These actions might consist of :-

- Shutdown affected ports at the host, switch, firewall or router
- Jamming exact IP addresses on the host, switch, firewall or router
- Turn on specific access lists on switches, firewalls or routers
- Causing routers to cooperate with the wide area network or telecommunication carrier connection to choke or reduce bandwidth in firm attacks.

Conclusion

In this documents we discussed about IPS and IDS. All of these have their own set of advantages and disadvantages, but to keep our system safe and secure IPS and IDS are very important it not only prevent or block malicious attack but also prevent from system crash. This intrusion detection system and Instruction prevention system applications are either signature-based or anomaly-based. But the data base (signature database) should upgrade in period of time so that doubtful or irregular activities are detect properly to keep system safe and secure.

References

[1]

[2] L. R. Rogers, Home Computer Security - CERT® Coordination Center.
http://www.cert.org/homeusers/HomeComputerSecurity/#intro

[3]Home Network Security - CERT® Coordination Center.
http://www.cert.org/tech_tips/home_networks.html

[4]Wikipedia
http://en.wikipedia.org/wiki/Intrusion_detection_system

Mustafa Ali **811107-T117** musali06@student.hh.se, mustafaalispk@yahoo.com
Partha Roy **790318 -N175**
Asif Shakoor **790810-2259** **asifshakoor143@yahoo.com**