Intrusion Detection Prevention System (IDPS) using ACL and AAA

A.Hyils Sharon Magdalene
Student

K.Rajalakshmi
Assistant Professor,

Center for information Technology and Engineering,
ManonmaniamSundaranar University,
Tirunelveli, India.

***Abstract*—It is widely recognized that the threat to enterprises from insider activities is increasing and that significant costs are being incurred. The multi-faceted dimensions of insider threat and compromising actions have resulted in a diverse experience and understanding of what insider threats are and how to detect or prevent them. The purpose of this research is to investigate the potential for near real-time detection of insider threat activities within a large enterprise environment using monitoring tools centered on the information infrastructure. As inside threat activities are not confined solely to cyber-based threats, the research will explore the potential for harnessing a variety of threat indicators buried in a different enterprise operations connected or interfacing with the information infrastructure, while enabling human analysts to make informed decisions efficiently and effectively.**

Key words—Intrusion detection and prevention system (IDPS); TCP; UDP; AAA; time to leave (TTL).

I. INTRODUCTION

Our research incorporates both theoretical and applied research aimed at delivering a significantly enhanced capability in insider threat detection, as well as education and dissemination materials and strategies designed to maximize uptake of the insight generated by the research. Our approach is to combine cyber security, psychology, criminology, visual analytics, enterprise operations management and executive education expertise to:

a) Develop a model for insider threat [5] which is flexible enough to underpin detection systems based on both detecting deviations from normal behavior, and the identification of specific events of interest which might indicate the presence of an attack involving an insider. The model will support the distinguishing of attack events relating to activities in the physical space and cyber space, based on data sources accessible via the information infrastructure.

b) Understand the potential for psychological indicators of an insider becoming a threat, including how we might detect such indicators based on cyber behaviors'.

c) Identify the most effective pattern extraction algorithms for facilitating correlation and detection across heterogeneous operational contexts.

d) Understand the enterprise culture and common practices that such novel detection systems would need to work within, and design process appropriate to enabling operations [1]

e) Understand the enterprise culture and common practices that such novel detection systems would need to work within, and design processes appropriate to enabling operation.

f) Provide a visual analytical interface to assist human analysts in more complex reasoning and decision-making processes by enabling them to fuse their knowledge and experience with the information and threat indicators discovered by the system, hence empowering the analysts to play an active role within the detection system in addition to being consumers of its outputs.

g) Develop an understanding of both the various organizational roles that will be impacted by such an insider threat detection system and have responsibilities towards successful outcomes, and the various awareness raising and educational methods which are likely to have the greatest impact in enabling stakeholders to benefit from the research and to learn from the knowledge developed.

II. CISCO – IOS

A. Routers

To run a router, which is in a Hardware device, we need an OS which is IOS. IOS is the platform on which router runs. It is in Command Prompt Mode [CLI-Command Line Interface] [9].

B. *QOS: (Quality of Service)*

QOS is the ability of the network to provide better or special service to a set of users or applications. Implementing QOS involves three major steps:

- Identifying traffic types and their requirements.
- Classifying traffic based on the requirements identified.

- Defining policies for each traffic class. C. *Interfaces*

There are of two types:
Fixed: It is a fixed interface, we cannot change. EX: serial 0, serial 1, Ethernet 0

Module: It is like slots in a PC.

D. *Router boot up process:*

Once we buy a new router. A router typically goes into five steps:

Step 1: The router loads and runs post (Located in ROM), testing its hardware. Components including memory and interfaces.

Step 2: The bootstrap program is loaded and executed (used to find out, how IOS image and configuration files will be found and loaded)

Step 3: The bootstrap program finds and loaded an IOS image possible location of IOS image are flash, TFTP server, ROM.

Step 4: After the IOS is loaded, the IOS attempts to find and load a configure file, which is normally stored in NVRAM. Initially, NVRAM has no contents. If the IOS cannot find a configuration file, it goes to set up configuration and start up the system configuration dialogue.

Step5: After the configuration is loaded, you are presented with CLI interfaces.

E. *ACL: (Access Control List)*

It is used for packet filtering. ACL [9] is a list of commands or statements used in routers to filter packets.

There are three types of ACL:
Named is a combination of standard and extended. Standard and extended use numbers. Named uses word.
Standard: 1-99
*Extended***:** 100-199
Named: Any character/word

F. *EIGRP (Enhanced Interior gateway routing protocol)*

EIGRP is a balanced hybrid protocol. It is a Cisco proprietary protocol. We can configure EIGRP only in Cisco devices.

G. *EIGRP (Enhanced Interior gateway routing protocol)*

EIGRP is a balanced hybrid protocol. It is a Cisco proprietary protocol. We can configure EIGRP only in Cisco devices.

G. AAA:(Authentication, Authorization, Accounting)

The AAA [9] network-security services provide the primary framework through which you set up access control on a Cisco IOS switch. AAA is an architectural framework for configuring a set of three independent security functions in a consistent manner.

III. CONTROLS IN SECURITY SOLUTIONS

A. Administrative control:

Administrative control conducts routing security awareness training programs. It clearly defined security policies. There is a change in management system, while informing the related parties. There must be logging configuration changes. It must properly screened potential employees like people involved in criminal acts.

B. *Physical control*

Physical control is a security system to monitor for intruders. It has physical security barrier like locked doors. This contains climate protection system. It consists of security personnel to guard data.

C. *Technical controls:*

It has security appliances like firewalls, IPS, IDS. It has complete authorization and applications like RADIUS, TACACLS +, and OTP (One Time Passwords).

IV. FIREWALL

According to CISCO, a firewall is a system or group of systems that enforce an access control policy between two networks. A firewall is a system or a group of systems that established a trusted network boundary (a perimeter) and then manages traffic across that boundary.

V. CISCO SELF DEFENDING NETWORK TECHNOLOGY

This will secure network [2] platform or perimeter (both internal and external). It will secure wireless access. Also secure e-commerce and web based transactions. It will comply with government policies. It reduces the impact of viruses' attacks.

VI. METHODOLOGY

CISCO recommendations for security

It uses strong passwords and enables password expiration. It will disable unneeded service and ports on hosts. It routinely applies patches to operating systems and applications. [4]

Four methods used by hackers:

- Trojan horse attack
- Social engineering attack
- Foot print analysis attack
- Privilege escalation attack

All four are because of unauthorized access.

- *Trojan horse attack*

Hackers will install by sending Trojan horse programs that will e-mail passwords to an attackers or even capture the clear of users PC.

• *Social engineering attack*

Using social engineering by calling personal (phone calls) on your network and trying to get them to give to the attacker their password information or using those horses.

• *Foot print analysis*

It is the process of gathering information about a target. EX: using Google search.

• *Privilege escalation attack*

An attacker compromises another subsystem and then through these compromises, subsystem attacks the application.

Types of CISCO firewalls [9]:

a) Static packet-filtering firewalls (layer 3 and layer 4)

b) Application layer gateways (layer 5 and layer 7)

c) Dynamic or stateful packets-filtering firewalls (layer 4)

d) Application inspection firewalls (layer 5,6,7, (mostly 7))

e) Transparent firewalls (layer 2) [10]

A. IP routing

Routers connect multiple network using routing principles. Routing means taking a packet from one device and sending it through the network to another device on a different network. To route, a router needs to do the following: know the destination address, identity the sources it can learn from, discover possible routes, select the best route, maintain and verify routing 10.120.2.0 information. Router is a layer 3 device, routed protocols – these deals with addresses. EX: IP, IPX, APPLE TALK.

Routing protocols are used for connecting networks. EX: RIP, EIGRP, OSPF, IS- IS (Intermediate system), BGP routers mainly provide routes to the destination. There are two types of routes available:

In **Static route**, one route is fixed for transmission, it is fixed, if that link is down, it cannot connect and cannot reach the destination even if there is alternate paths.

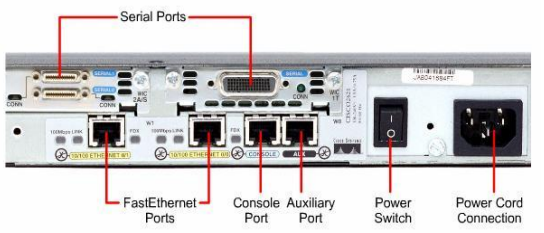

Fig.1. External Components of a 2600 Router

The dynamic route, choose the path by itself. Paths are found by the routing protocols. It chooses the best or main path. If it fails, it chooses the best alternative path. This uses a route that a network administrator enters in to the router manually. It is used for smaller network

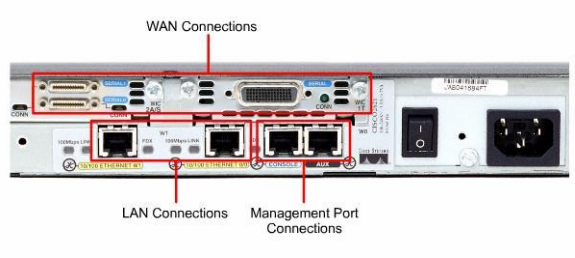

Fig.2. External Connections

The following features of Cisco IOS [10] firewalls are:

1) Application layer firewall for e-mail, web and other traffic
2) IM and P2P application filtering
3) VoIP inspection and firewalling
4) Virtual routing and forwarding (VRF) support
5) Wireless integration (if equipped)
6) Stateful failover
7) Local URL filtering: white list and black list support

VII. RESULTS AND DISCUSSION

A. Types of Events Detected:

The types of events [6] most commonly detected by Softwares: (Advanced IP Scanner, XArp, Wireshark, Nmap – Zenmap GUI, Network DLS, Tenable Network Security (Nessus), burpsuite) are,

a) Network reconnaissance attack:

With a reconnaissance attack, the attacker is trying to learn information about your network topology, the devices that you are in your network and configuration of those devices. This information is used by the attacker to implement DOS and is access attacks.

b) Hackers:

Hackers are the most obvious externally threat to network security. There are several different species of hackers according to CISCO. They can also be grouped by their motivations.

- White hat – ethical hacker
- Black hat – unethical hacker
- Gray hat – a hacker, who has a real job and sometimes plays both sides of the law, they
- Often motivated by intellectual challenge and notoriety, but usually not monetary gain.
- Blue hat – bug testers
- Cracker – hacker with criminal intent, are motivated by economic gain.
- Phreakers (or phone phreak) – hackers are in telephone systems.
- Script kiddies – hackers with little or no skill.
- Hacktivist – hackers with political agenda.

c) *Hacker specialization*

Whether a hacker wears a white, black, gray or blue hat, they can be further defined by the type of hacking, they perform.

- *Computer security hackers:* usually, secretive and specialize in computers and networks
- *Academic hackers:* not usually secretive specialize in designing elegant software and gravitate toward UNIZ and the open source movement.
- *Hobby hackers:* usually hack code related to video games and gaming hardware and other home computing.

d) IP spoofing attacks:

IP spoofing is the networking equivalent of identity theft. If you fake some other device IP addresses, you can pretend to be that other device in order to, gain root access, inject erroneous data into an existing conversation, fool other devices in order to divert packets to the hacker, overload resources on servers. (DoS), accomplish a task as part of a large attack. One of the things that make IP spoofing so effective is that the process of routing is destination based meaning that routers make their best path determination based on the destination IP address in an IP packet, often ignoring completely the source address.

Types of spoofing:

- *Man-in-the-middle attacks (MIM):* The attacker assumes the identity of a trusted host on the network and steals information. An example of this is session hijacking.

- *DOS attacks:* The information gained leads to a flooding of resources on a targeted system. An example would be excessive hard drive thrash of an unpatched web server.

- *Distributed DOS attacks:* The information learned during the reconnaissance leads to a flooding of resources on a targeted system from multiple hosts and simultaneously. An example would be an attack on a core network device that consumes all the bandwidth into and out of a network.

MIM attacks attack the networks confidentiality. They also attack the network integrity because invalid data can be replaced in to the network by a spoof system. DOS and DDOS attacks attack the networks availability.

B. Prevention capabilities[6]

1) Access control list-Standard ACL-Building concepts:

Standard ACL checks the packets of source IP only. It will not check the destination. It checks, whether source packets can be allowed or denied. This is a Permits/Deny entire TCP/IP protocol suits. It permits all TCP/IP option. It denies all TCP/IP options. ACL uses wild card mask. So, if we want to filter only one PC, we can give (Permit/Deny only one PC)

a) Inbound access lists

Data's goes from one interface to another interface. When an access list is applied to an inbound packets on an interface to another interfaces. When an access list is applied to an inbound packets on an interface by those packets are processed through the access list before routed to the outbound interface.
EX**:** Data's going from s0/0 to inside.

b) Outbound access lists

Data's coming from outbound to interfaces.
EX: binding of fa0/0

When an access list is applied to outbound packets on an interface by those packets are routed. If ACL is not there, PCs will ping easily. If ACL is there, PCs will ping only if it matches. ACL works like a IF-ELSE statement. If first deny is given and the permit, it will deny that PC and permit others. If first permit is given and then, deny one PC is given, it will do only permit option and permit's all PC's. Deny PC will not be denied and will be permitted.

2) Extended ACL: (100-199)

It is used to check: source IP, destination IP, and the service used to block, which service options like, if we want to block HTTP service alone. It permits/denies entire TCP/IP protocol suite (or) deny specified service.

3) AAA

a) Authentication

Authentication provides a method for handling the following: user identification, login and password dialog, challenge and response, messaging, encryption. Authentication identifies users prior to accessing the network and network services. AAA configures authentication [9] by defining a named list of authentication methods and then applying that list to various interfaces. The method list defines the types of authentication performed and their sequence. These methods are applicable on a per-interface basis. However, all interfaces on Cisco routers and switches adhere to a default method list named Default when no other authentication methods are defined. A defined method list always overrides the default method list.

The commands used are,

'aaa authentication login console-in local' - it SPECIFIES THE login authentication method list name console-in using the local user database on the router.

Other commands are, ***'aaa authenication enable default'***, ***'aaa authentication local default'.***

b) Accounting

Accounting provides the method for collecting and sending security server information used for billing, auditing, and reporting. This type of information includes user identities, network access start and stop

times, executed commands (such as PPP), number of packets, and number of bytes. This information is useful for auditing and improving security as each switch or router monitors each user. In many circumstances, AAA uses protocols such as RADIUS, TACACS+, or 802.1X to administer its security functions. If your switch is acting as a network access server, AAA is the means through which a switch establishes communication between your network access server and your RADIUS, TACACS+, or 802.1X security server. The command used to start and stop tacacs+ is : ***'aaa accounting exec start stop tacacs+'.***

c) Authorization

Authorization provides the method for remote access control. This remote access control includes onetime authorization or authorization for each service on a per-user account list or a user group basis. The AAA authorization process on switches or routers works by contacting a common, centralized database of a set of attributes that describe the network user's authorized services, such as access to different parts of the network. The centralized server returns a result of allowed services to the switch or router in question to execute the user's actual capabilities and restrictions. This database is generally a centrally located server, such as a RADIUS or TACACS+ security server.

4) *CISCO self defending network*

Perimeter security means secures the boundaries between zones. Communications security provides information assurance (C-I-A) [7]. Core network security ensures that only compliant traffic traverses the perimeter. It protects against malicious software and traffic anomalies. It enforces network security policies and ensures survivability. End point security enforces compliance to identity and device security policies.

Seven steps for compromising targets and applications: According to CISCO, the seven steps for compromising targets and applications are as follows: [8]

- Platform footprint analysis (reconnaissance)
- Enumerate applications and operating systems.
- Manipulate users to gain access.
- Escalate privileges.
- Gather additional passwords and secrets
- Install back doers.
- Leverage the compromised system.

VIII. CONCLUSION

This project has successfully implemented in networking techniques using routing, ethical hacking Technologies like EIGRP, RIP, INTRUSION PREVENTION SYSTEM, and INTRUSION DETECTION SYSTEM. This project can be implemented in enterprise, where network security is very vital as this project has successfully implemented in both IDS and IPS Technology.

This project helps both LAN and WAN network s to be highly secured as it helps to detect hackers and prevent unwanted packets to attack to attack our networks. It can be used both in private and government sectors especially in cyber based security systems.

REFERENCES

[1] Scarefone Karen and Mell Peter, "Computer Security, National Institute of Standard Technology", 2007

[2] Networks Security Essentials: Application and Standards by W. Stallings, Pearson Education, 2007

[3] Shukla Brahma Dutta and Gupta V.K., "Performance Interoperability between RDBs and OODBs", *Res. J. Recent Sci.*, 1, 419-421, 2012

[4] Gupta Dhiraj, Shukla Brahma Dutta, "Constraint of Secured Database in Distributed Database management System", [*advancement in computational technique & application]*, 1, 190-194, 2011.

[5] "Cisco Intrusion Prevention System Solutions", 2008 Cisco Systems available in http://www.cisco.com

[6] Mell Peter and Scarfone Karen, "Guide to Intrusion Detection and Prevention Systems", U.S. Department of Commerce, 2007.

[7] Konstantinos Xynos, Iain Sutherland and Andrew Blyth, "Effectiveness of blocking evasions in Intrusion Prevention Systems", April 2013 Copyright held by the authors and the University of South Wales, Pontypridd, Wales (White paper)

[8] IBM corporation software group, "IBM Security Network Intrusion prevention system", produced in the United States of America, Route 100, Somers, NY 10589, March 2013.

[9] "Cisco Intrusion Prevention System Sensor CLI Configuration Guide for IPS 6.0", © 2006-2012 Cisco Systems available in http://www .cisco.com, 4- 28, 6- 14, 8-18, 8- 33, 9 -8, 11-1,13-13, 13 -22, 16-16, 16-18, A-17, A-20, A-25, B-1, B-14, B-15, B-34, B-39, C-1.

[10] "Cisco IOS Intrusion Prevention System Deployment Guide", © 2010 Cisco and/or its affiliates available in http://www.cisco.com

AUTHORS PROFILE

A. HYILS SHARON MAGDALENE, doing Final Year M.Tech. (Information and communication Technology) in Center for information Technology and Engineering (CITE), M.S. University, Tirunelveli. She completed her B.Tech. Degree in the same course in M.S. University, Tirunelveli in the Year of 2012 with First Class distinction.

K. RAJALAKSHMI, received B.E.,Computer Science and Engineering and M.E., Computer Science and Engineering from Government College of Engineering ,Tirunelveli and Ph.D., degree from ManonmaniamSundaranar University in Remote Sensing Image Processing. She has a teaching experience of more than fifteen years in various reputed Engineering Institutions. She has published many papers in international journals and IEEE conferences. She is a GATE qualified Scholarship receiver in her Post graduate .She has been recommended for Common Wealth Split Site Doctoral Scholarship by UGC, New Delhi. Her current research interest includes Neurofuzzy and Softcomputing. Currently she is working as a faculty in the Centre for Information Technology and Engineering, M.S. University, Tirunelveli.