ORIENTAL JOURNAL OF
COMPUTER SCIENCE & TECHNOLOGY
An International Open Free Access, Peer Reviewed Research Journal
Published By: **Oriental Scientific Publishing Co., India.**
www.computerscijournal.org

ISSN: 0974-6471
April 2014,
Vol. 7, No. (1):
Pgs. 185-192

Intrusion Detection and Prevention System using ACL

A. HYILS SHARON MAGDALENE

Center for information Technology and Engineering M.S.University, Tirunelveli, India.

(Received: March 22, 2014; Accepted: April 03, 2014)

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 centred 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, ICMP, time to leave (TTL).

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:

Develop a model for insider threat 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.

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

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

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

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.

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.

CISCO – IOS

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].

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.

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.

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.

ACL: (Access Control List)

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

There are three types of ACL

1. Standard
2. Extended
3. Named

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

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.

OSPF (Open Shortest path first)

It is an open standard routing protocol that has been implemented by a wide variety of network vendor including CISCO. It supports multivendor like CISCO, Alcatel, juniper, 3com

routers. OSPF works by using Dijkstra algorithm. First A shortest path tree is constructed. Secondly, routing table is populated with the resulting best paths. OSPF is used:

To decrease routing overhead
To speed up convergence
To confine network instability in to single area of a network

Controls in security solutions

- Administrative controls: These are primarily policy centric.
- Physical control: These help to protect data environment.
- Technical control: These uses a variety of hardware's and software's to protect data.

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.

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.

Technical controls

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

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.

CISCO self defending network techmology

This will secure network 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.

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.
Four methods used by hackers:

A. Trojan horse attack
B. Social engineering attack
C. Foot print analysis attack
D. 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

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)

Static packet-filtering firewalls

It works at layer3 and layer 4. It analysis network traffic at the network and transport layers. Static packet-filtering routers are relatively unintelligent. By using ACLs, they can either permit or deny traffic up to the layer 4 of the OSI model, but they do not see the PDUs (Protocol Data Units) that carry the data as part of a dynamic conversation. For example, they can permit traffic, if it matches, the well known TCP port number for HTTP port 80, but they can only filter the packets one by one and have no appreciation for how a TCP connection is built, carries and retransmits data as required, and is torn down, and filter packets one at time.

Application layer gateways

An Application layer gateways or proxy server is a firewall that proxies a clients connection to a server at layer 5 and layer 7 (session and application) of the OSI model. At the application layer, the client first connects to the application layer gateway. The user is authenticated to the proxy at the application layer (optional). The application layer gateway proxies (acts on behalf of) the clients connection to the application servers. The application layer gateway forwards the replies to the client.

Dynamic (stateful) packet – filtering firewalls

A game starts with an opening serve from the player, who has service (requester send SYN). The in-bounds serve is supported to be returned by the opponent (responder sends RST) because the opponent is not ready. If the initial player receives the ball back from the opponent (SYN, ACK) they will return the ball (thank you very much!) with an (ACK) the volley continues. The initial 3-way handshake (SYN; SYN, ACK; ACK) is complete. Either the initial serves or the opponent can tear down the volley (the TCP session) at any time by sending a (fin) to their opponent, beginning a z-way handshake that culminates in the session (the volleys) termination.

Application inspection firewalls

It will perform deep packet inspection at the application layer in order to determine that protocols that are proceeding across the firewall are compliant with the organizations security policy. At the same time, the AIF can ensure that the protocol is standards-compliant and also look signs of unauthorized protocols tunneled inside the application session. For EX: the edockey protocol that is used by the popular p2p application kazaa, could be blocked, when it appears inside an HTTP session.

Transparent firewalls

The final category of firewalls is transparent firewalls. Transparent firewalls, as its name implies, starts making forwarding and filtering decisions at the data link layer (layer 2) of the OSI model. It works in a secure bridging mode at layer 2, while offering rich layer 2 through 7 security services. Stateful firewall stores the following information.

a) Source IP
b) Destination IP
c) Port numbers
d) TCP sequence numbers
e) TCP/UDP flags for that session
f) Stateful firewalls are needed to open UDP ports used in RTP streams.

The following features of Cisco IOS firewalls are:

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

RESULTS AND DISCUSSION

Types of Events Detected

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

Network reconnaissance attack

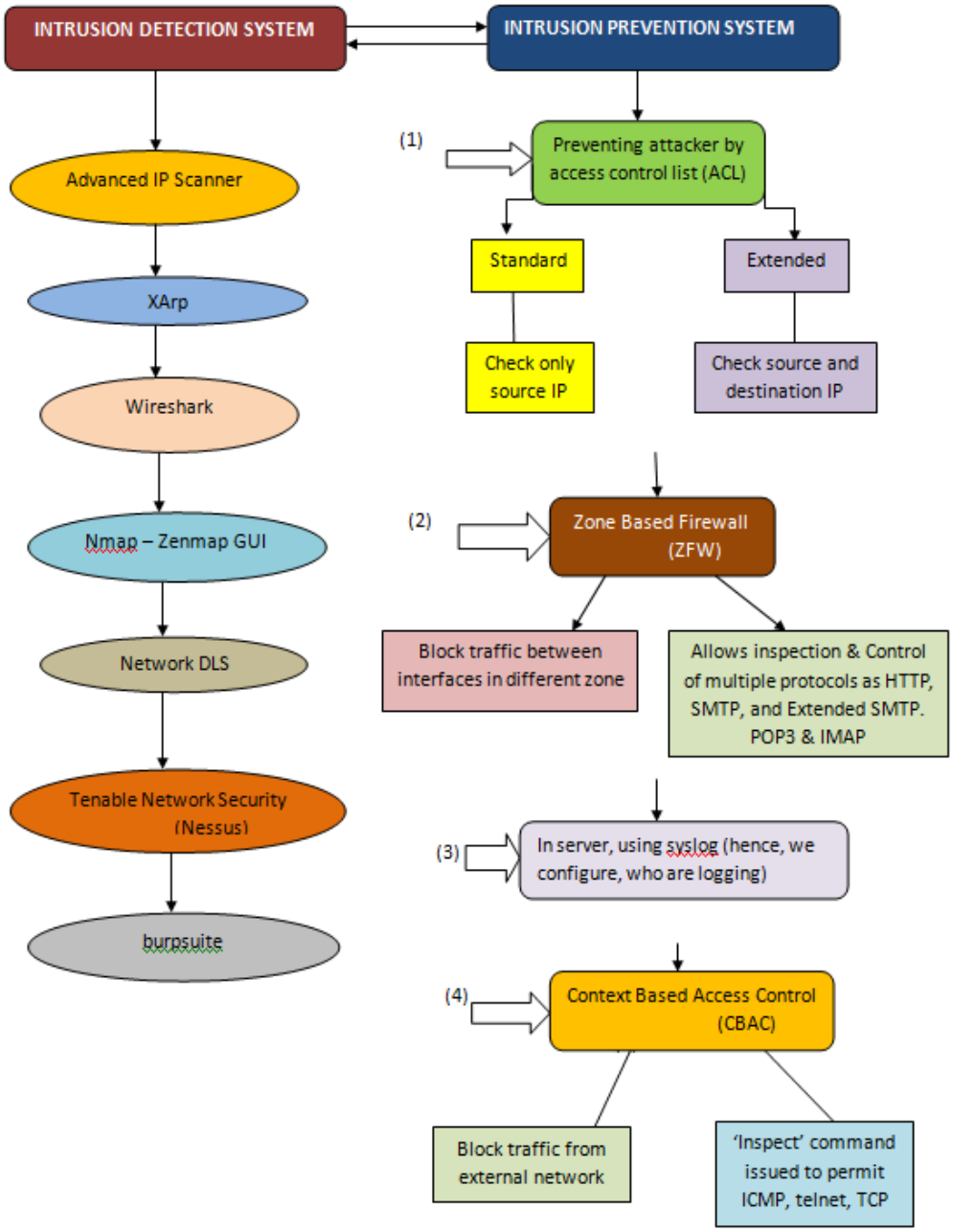
With a reconnaissance attack, the attacker is trying to learn information about your network topology, the devices that you are in your network and configuration of those devices. This

information is used by the attacker to implement DOS and is access attacks.

Hackers

Hackers are the most obvious externally threat to network security. There are several different species of hackers according to CISCO. Hacker is a computer enthusiast. 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.

The motivation of hackers are Intelligence gathering, theft of intellectual property, DOS (denial of service), Embarrassment of the target, Intellectual challenge

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.

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

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

A. 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.
B. 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.
C. 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.
D. 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.

Prevention capabilities

Firewall implementation best practices

Place firewalls at key network security boundaries. Set connection limits to prevent from worms and attacks. Although the firewalls are the primary security devices, it is unrealistic to assume that the firewall is all that is needed for security. Adopt a 'deny all' strategy by default. Deny all traffic except that which is expressly needed. Do not forget physical controls on firewall access. Regularly monitor firewall logs for signs of intrusion. Make sure that changes to the firewalls configuration occur within an overall change management policy. Firewalls are primarily technical controls against outside attack. Do not let internal security lapse as a result. Adopt strong administrative controls and physical controls to complement the firewalls technical controls.

- Service policy – use deep packet inspection engine.
- URL filter – use URL filtering engine.

CISCO-IOS zone based firewalls: (ZFW)

ZFW available in IOS release 12.4(6)T or later, changes that, the concept behind zone based firewalls is similar to that used by appliance firewalls. Router interfaces are placed in to security zones. Traffic can travel freely between interfaces in the same zone, but is blocked by default from travelling between interfaces that has been assigned to a security zone and those that have

not you must explicitly apply a policy, to allow traffic between zones. ZFW allows the inspection and control of multiple protocols, including the following:

- HTTP and HTTPs
- SMTP, extended SMTP (ESMTP), POP3 and IMAP.

Peer-peer applications with the ability to use heuristics to track port hopping. Instant messaging applications (AOL, yahoo, and MSM as of this writing). Remote procedure calls (RPC). By default ZBF permits.

- Traffic flowing to and from the routers self interface.
- Traffic flowing among the interfaces that are not assigned to any zone

Traffic flowing among the interfaces that are members of the same zone. ZFW policy maps can take the following action under each class:

- Drop – drop the packet
- Inspect – use context based access control engine
- Pass – pass the packet (the pass action works in only one direction)
- Police – police the traffic
- Service policy – use deep packet inspection engine. URL filter – use URL filtering engine.
- Threat mitigation with ACLs:
- Inbound IP address spoofing
- Outbound IP address spoofing
- DOS and DDOS, TCP, SYN attacks
- DOS smurf attacks
- Inbound and outbound ICMP messages (used for DOS attacks and reconnaissance)
- Trace route (used for reconnaissance)

CISCO self defending network

Perimeter security means secures the boundaries between zones. Communications security provides information assurance (C-I-A). 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:

- 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.

CONCLUSION

This project has successfully implemented in networking techniques using routing, ethical hacking Technologies like EIGRP, RIP, INTRUSION PREVENTION SYSTEM, 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 Securiy, 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. Sheetlani Jitendra and Gupta V.K.,

"Concurrency Issues of Distributed Advance Transaction Process", *Res. J. Recent Sci.,* **1**: 426-429 (2012).

6. Gligor V.D. and Shattuck S.H., "Deadlock detection in distributed systems", *IEEE Trans. Softw. Eng.* SE-6, 5, 435- 440 (1980).
7. Gupta Dhiraj and Gupta V.K., "Approaches for Deadlock Detection and Deadlock Prevention for Distributed systems", *Res. J. Recent Sci.,* **1**: 422-425 (2012).
8. Mell Peter and Scarfone Karen, "Guide to Intrusion Detection and Prevention Systems", U.S. Department of Commerce, (2007).