Implementation Of Intrusion Detection System

Siva Kumar Kotamraju, Ashok Kumar Nanduri,
Dr.V.Sujatha

Abstract— The paper deals with the security issues concerned to the intrusion in a network and focuses on setup of an Intrusion Detection System (IDS) in a VLAN and detecting various types of attacks on VLAN. It describes various approaches of detecting the attacks and preventing the attacks with different techniques such as pattern matching, protocol decoding, defining rules and signatures etc. We proposed a secured architecture for a LAN with placement of Intrusion Detection System. We have used Snort as an Intrusion Detection System, which is an open source toolkit on Linux platform. It includes detailed study of Intrusion Detection System and practical implementation. Finally, architecture is being proposed to secure VLAN by placing Intrusion Detection

1. INTRODUCTION

1.1. Intrusion Detection System (IDS)

Computer systems and networks are protected from abuse by using a defensive measures component known as Intrusion Detection System. Intrusion is defined as the process of performing an action by an information system user in an illegal form. The intruder can come from either inside or outside, who go beyond his authority limits to perform an action. Even though the action causes damage or not, it is to be worried as it may cause damage for the service supplied by system or for the system's health. The detection of intrusion includes describing the worse or gain strived by an intruder for few entity, which seeks an unauthorized access for system. To recognize in prior that an intruder starts an interaction with system neither of the automated detection methodologies which are known to us is used. Meanwhile, to avoid intrusion regular actions are performed by the system administrators. These can be like requesting for the password to be provided ahead by the user to acquire any system access, blocking entire or few access of the network and physical access, affixing of the familiar vulnerabilities that may be used by the intruder to acquire unauthorized access. Systems with Intrusion detection are utilized in extra for avoiding such measures.

1.2 Requirements of IDS

An Intrusion Detection system is much required in enterprise networks, as there are more possibilities of getting threats. The threats may be any kind of attack such as DoS, backdoor entries, spoofing etc. These attacks try to use the vulnerabilities of the system and exploit them to make the network to crash and down. Once the intruders are successful in such attacks they exploit the resources for their miss-activities and put the system in trouble. To track such attacks and prevent the network from such attacks there is a need of some system which can take actions on detection of such attacks. Intrusion Detection system or Prevention System makes such attacks to minimize and make the whole system to get secured by viruses, attacks all the threats.

2. REQUIREMENTS

2.1. Snort

Network Intrusion Detection System provides cost free an open source system known as Snort. The flow of data on network is scanned by the use of NIDS which is a variety of IDS (Intrusion Detection System). To find the attacks aimed to particular host, host-based IDS (Intrusion Detection System) are installed on that specific host. Snort is classified among the peak quality systems presented today, even though all methodologies of intrusion detection are yet new.

2.2 MySQL

MySQL [5], a database which is being used along with snort to store all the data related to the traffic captured through Snort. The database has been tuned so as to use with snort and database has been created. MySQL inputs the data to Snort and BASE for analyzing the traffic and alerting the threats in a network.

2.3 Basic Analysis and Security Engine (BASE)

The analysis and presentation of data available in Snort by web interface is done by a tool which is known as BASE. Using PHP it was written. MYSQL databases and Snort are worked on this, it provides the data presented in database by a web server for user. This tool can also utilized for other products related to security such as networking monitoring and firewalls. BASE includes numerous configuration files and PHP (Pretty Home Page) that work simultaneously to gather and examine the data from database and web interfaces are used for the presentation. The interaction of a user and BASE is done by a web browser. For making it work on your system, you need to have database server, PHP, web server and few other tools to be installed in the system.

BASE offers many features [2] related to IDS

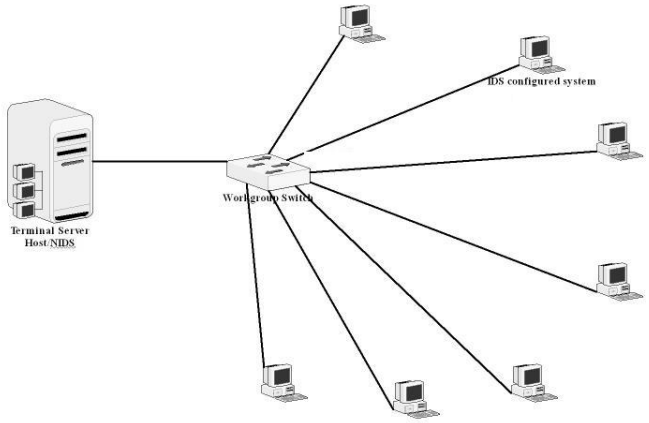
1. Searching is made based on many criteria such as destination and source addresses, ports, time and others.
2. For displaying different elements of packet, the utilization of Packet viewing is done. You can display different payload and header elements too.
3. The handling of alerts can be done by the creation of alert classes, removing, exporting and forwarding these for an email-address.
4. Graphical characterization involves charts build using protocol, time, port numbers, classifications and IP addresses.
5. Alerts database snapshots are also captured. For example, you are able display the previous 24 hours alerts, frequent alerts, unique alerts and others too.
6. The owner of a specific IP address which is causing attack to your network can also be identified by using on Internet by the use of distinct databases. Based on this we can communicate with that specific person to halt it. The data about IP addresses and domain names of the owner are included in the databases.

2.2. Apache web-server and PHP

Apache web server [4] has to be configured with PHP so as to provide the web and graphical user interface. PHP works along with BASE which runs many of the PHP scripts for various activities and plots the graphs and other measurements of Intrusion found in a network. Apache with PHP provides flexibility in use of an Intrusion Detection System with Snort.

3. IDS TEST BED SETUP

Intrusion Detection Test Bed has been setup using all the above described toolkits. The actual test bed setup looks as follows.



- The test bed has been setup in the lab VLAN starts with address 192.168.1.0. The IDS has been configured on a system with IP address 192.168.1.100 which monitoring an interface of the VLAN.
- The other machines are connected to the VLAN having the IP from 192.168.1.1 through 192.168.1.255. All these machines are connected to a workgroup Switch whose interface is being monitored by IDS. This VLAN is considered as Home Network.
- Any request coming from External Network (other than Home Network) to any of the system at Home Network, will be first filtered by IDS and raises alert and takes required action on detection of any attack or any kind of virus in the request.
- On detection of attack or illegal activity, the rules defined for particular activity generates an alert and the alert it activates the particular rules to take action.

2. Proposed Methodology

The test bed of Intrusion Detection System that has been setup for conducting experimentations and analysis of traffic over a VLAN, a secured network design is being proposed for VLAN. A survey has been carried out to study the existing network design for a VLAN. As per the analysis done over the test bed setup at lab, the IDS is currently monitoring the Lab VLAN starts from the subnet 192.168.1.0 Many security issues – different types of attacks, virus & Trojan horse, worms, backdoor entries etc on existing network design motivates for new secured design for a VLAN. The existing network design for a VLAN is shown below.

4. RULES AND SIGNATURES FOR IDS

The detection system of Snort is made up of rules, which are further depends on the signatures of intruder. The several elements of data packet can be checked using Snort rules. Snort version 2.x supports application layer header. Rules are applied in an orderly fashion to all packets depending on their types. For creating a log message, an alert message, or significant of Snort, transfer the packet of data that is drop it in mute. The sense of pass word which is used here is different for the basic meaning of pass which is utilized in router and firewalls. The drop and pass are different from each other in routers and firewalls. For understanding syntax, the rules of Snort are written in simple.

4.1. Structure of a Rule

The structure of a snort rule has been divided in to two parts – Rule Header and Rule Options as follows,

Rule Header Rule Options

Rule Header	Rule Options

Fig4.1: *Snort Rule format*

The rule header contains information about what action a rule takes. It also contains criteria for matching a rule against data packets. The options part usually contains an alert message and information about which part of the packet should be used to generate the alert message. The options part contains additional criteria for matching a rule against data packets. A rule may detect one type or multiple types of intrusion activity. Intelligent rules should be able to apply to multiple intrusion signatures [10]

Action	Protocol	Src Addr	Src Prt	Dir	Dest Addr	Dest Prt

Fig 4.2*: Expansion of Rule Header*

- Action: Specifies the kind of task to be done in the case of criteria is matched, a rule is completely met with the packet of data. A critical action creates a log message or alert or acquire other rule.
- Protocol: part can be used to provide the control on packet to a specific protocol itself, which is the primary criterion specified in rule. Few examples regarding protocols utilized are UDP, IP and ICMP etc.
- Address: parts specifies destination and source addresses. These addresses might be a multiple or single host source, or network addresses. The complex network addresses can also obtained by the use of this part.
- Direction: The field direction (→) shows the flow of traffic, which indicates the flow from source address to destination address. This field also defines which address and which port from a particular address has been used for traffic flow.

Sample example of a Rule is

alert icmp any any -> any any (msg: "Ping with TTL=100"; \ ttl: 100;)

The element of rule prior to the initial parenthesis is known as rule header. The element of rule which is enclosed by using parenthesis is known as options part.

- A rule action. According to this rule the task is “alert”, that is an alert is will created when these conditions are matched. Note that these packets are logged in default in

the case of an alert generation. Based on the field of action, the parts of rule options might include additional rules criteria.

- Protocol. ICMP is the protocol regarding this rule,that is the rule is applicable particularly on the packets having ICMP-type. According to Snort detection engine, when a packet protocol is different than ICMP, then the remaining rule will not be reviewed for saving the time of CPU. The protocol field plays a major role in the case of applying the rules of Snort for only packets regarding a specific type.
- Source port and source address. Based on this example both got mapped to “any”, which specifies on all packets obtaining by any source rule will be applicable. Certainly, port numbers and ICMP packets will not have any relevance. Port numbers are similar to protocol itself it may be UDP or TCP.
- Direction. For this scenario the direction is mapped from left to right using the → symbol.

This displays that the port number and address are present on right hand side of symbol are destination and contains left hand side are source, which also specifies that rule would be applicable on packets moving from destination to source. You can make use of ← for performing the reverse action stating to destination from source. Remember, that <> symbol can be also used for applying rules for packets traveling in any both direction.

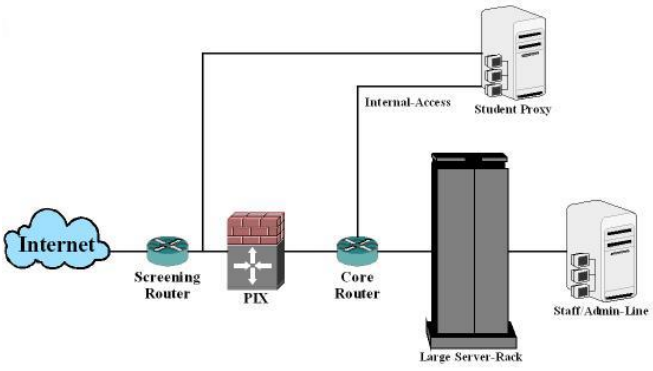
- Port address and destination address. Based on this example both got mapped to “any”, which specifies irrespective of destination address the rules will performed on entire packets. As this rule is applicable to whole packets of ICMP moving in any direction, the rule of direction will not perform any role; because of the utilization of “any” keyword among destination and source address parts.

The enclosed parts of options in parenthesis views the generation of alert message which contains text string as “Ping with TTL=100” for every TTL=100 condition get matched. Remember that Time To Live or TTL is one of the field in the header of IP packet.

5. PROPOSED WORK

5.1. Present System

The existing network design for VLAN faces some of the problems with regards to the attacks. Following figure expresses the design

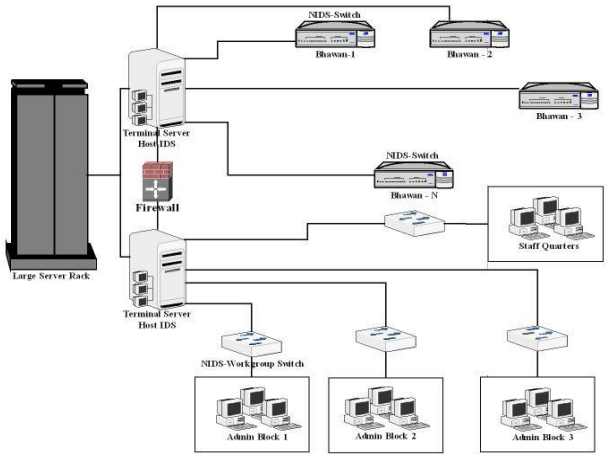


A High Level Design

5.1.1. Flaws of the Design

The major flaw of the design is in connection with student proxy.

- The student proxy is directly connected to the screening router with out any major security measures.
- Due to direct connection with screening router, there may be chances of attacks on the student proxies.
- The student proxy will be direct victim on an attack
- Once the Student proxy becomes victim of an attack, it may become source of attack to whole network
- Once the proxy gets attacked by the attacker, it will be tuned for all types of backdoor entries and starts miss activity.
- There may be chances of
  - Spreading Viruses: Attacker can spread viruses making the victim machine as source.
  - Violates integrity: Attacker gets access to the machine and there are chances of modification of confidentials and credentials of legitimate users hence violating integrity issue.
  - Access control violation: Attacker gets unauthorized access to the machine to perform various illegal activities as a root user.
  - DoS Attack: The victim may become the source of DoS attack on the other servers of the network which have direct access without any firewall or IDS.
- Once a victim is found in a network, then that can be used as source of attack to spread viruses and other kinds of worms which can affect entire network.
- Proxy can be tuned and configured as firewall but won’t be efficient as compared to firewall.
- Due to non secure mode of design in intranet of campus, a victim can become a cause to crash down the

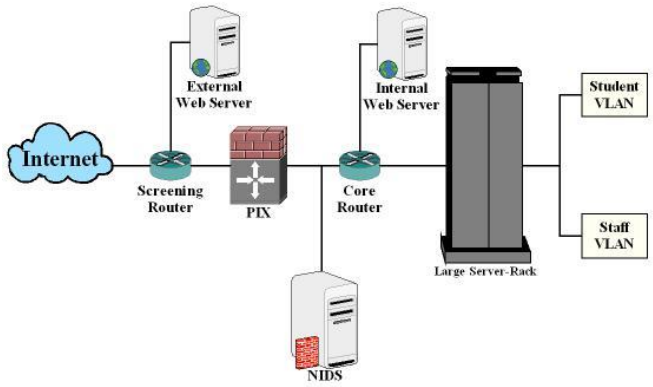


network.

5.2. Proposed Architecture

With considerations of all the flaws described in previous section, a new network design and specifically a design for VLAN is being proposed. The analysis of the existing network motivated to propose a new design for VLAN. The proposed architecture for secured network looks as follows.

Network Diagram: A High Level Design



The new network design shows

- The student proxy which was previously connected to the screening router, now moved to the large server rack where the other servers are secured by Firewall and IDS wnership data, which it in turn uses to check for MESI or other cache-coherency protocol violations
- The student proxy must be firewall enabled reduces the possibility of huge traffic on it minimizing DoS attack from external as well as internal network.
- We have configured and placed a NIDS [12] (Network Intrusion Detection System) which is most required system having capability of detecting the leakage in firewall [13].
- Intrusion Detection System, having a capabilities such as anomaly detection, protocol decoding [7], pattern matching [7], it can detect any kind of virus or worms being spread over the network.
- By this proposed design we can make our servers as well as proxies hidden from external network through firewall and IDS, hence minimizing the possibility of making victim for attack.
- According to the advantages of IDS over a firewall, IDS maintains the network much secured than the firewall but firewall is one of the major concern of ant network
- Our campus is a VLAN structured and divided in several VLANs, but the VLAN connected to Student Proxy are directly connected to outer screening routers. So the proposed design may be advantageous in connection with the flaws explained

5.2.1. Operations at Student Proxies

• The design explains that both the servers (Student Proxy and Server of Admin Blocks) are connected through a server rack. Both the servers are separated by the firewall configured, hence having restricted communication.

• All the VLANs are configured by Layer 3 Switches, and the Intrusion Detection System is configured and the interface is being monitored continuously.

• On detection of any kind of misbehavior of any of the system of VLAN, generates and takes required action. If the action is not defined in IDS configured then an alert will be generated to the IDS configured at terminal server which has capability of both Host and Network IDS [8] and takes the necessary action to the generated alert.

• Since all the VLANs configured with IDS, the security has been provided and chances of internal attacks over a particular VLAN is almost an impossible case.

5.2.2. Operations at Administration Blocks

• The administration block terminal server is separated by firewall and has restricted communication with student terminal server.

• The administration blocks are being separated by workgroup layer 3 switches [13] and all the VLANs are IDS configured and works similarly as student VLAN works.

• The terminal server of administration blocks has been configured with both kinds of IDS – host as well as network based IDS to provide additional features as anomaly detection, pattern matching [9] etc

5.3. Advantages of secured VLANs Design

There are many advantages of the proposed design over the present design. Here are some comparable advantages,

• The present system doesn't have Intranet security, hence any system can be hacked or any kind of attacks are possible in intranet. The proposed system configured with IDS at each VLAN keeps track of all the traffic of each system in VLAN and generates alert signal to administrator as and when misbehavior is found.

• The security is strong due to the IDS configured at each VLAN and having support of base IDS at the terminal server for additional actions on detection of attacks. This kind of security is missing in present system.

• The present system provides direct connection between external world and student proxy, increasing the possibility of victim machines in the internal network. This is minimized completely by placing the student proxy at a level where the intruder can't reach directly but needs to pass through firewall as well as network IDS configured.

• The external web server will be having the capability of redirecting requests to the internal web servers which reduces the direct attacks on internal web server.

• The proposed system is free from any possibility of backdoor entry or any other kind of attacks by the intruders external as well as internal.

With all these advantages which can be provided and security can be provided at maximum level with all existing resources with least cost. More secured the network, least possibilities of attacks. Hence the proposed system proves that it is advantageous over the present system and is implementation agnostic. This can be achieved with all the existing resources, but one time work of tuning the network according to our security requirements. With all the advantages of proposed system over present system proves that the proposed network design is more secured and reduces the attacks from both external as well as internal.

6. CONCLUSION AND FUTURE ENHANCEMENT

The present system and the flaws of the design motivates to work towards the security of the network. Intrusion Detection System / Prevention System with Snort makes a particular VLAN or a list of VLANs can be made secured from the external as well as internal network. This provides restricted access between the VLANs according to the defined rules of IDS, and hence minimizes the inter-VLAN attacks. The proposed network design provides a way of making the network as well as a VLAN secured. The main advantage of proposed design over the present is minimizing the possibility of victim machines attacked by external network. The design of VLAN provides security for attacks within the network. Totally the design of the network with support of Intrusion Detection System either internal or external provides security from all viewpoints.

7. REFERENCES

[1] Anita K. Jones and Robert S. Sielken, Computer System Intrusion Detection: A Survey, 2nd September 2000

[2] Rafeeq Ur Rehman, Intrusion Detection System with Snort, MySQL, PHP, ACID and Apache, Prentice Hall India, 2003

[3] www.snort.org

[4] www.apache.org

[5] Basic Analysis and Security Engine, http://easynews.dl.sourceforge.net/sourceforge/secureideas

[6] www.mysql.org

[7] Enterasys Networks, Intrusion Detection Methodologies Demystified, White Paper, Feb'2003

[8] Markus Peuhkuri, Firewalls and Intrusion Detection System, Mar'2005

[9] S. Antonatos, M. Polychronakis, P. Akritidis, K.G. Anagnostakis and E.P. Markatos, Piranha:

[10] Fast and memory-efficient Pattern Matching for Intrusion Detection, 2004

[11] Samuel Patton* William Yurcik David Doss, An Achilles' Heel in Signature-Based IDS: Squealing False Positives in SNORT, Illinois State University, 2001

[12] Case study of network security design on a hypothetical ISP network

[13] Stephen Northcut Network Intrusion Detection System, New Riders publishing, ISBN 0-7357-1008-2, September 2000,

[14] Scott C. Zimmerman, Secured Infrastructure Design, CERT Coordination Center, 2002

[15] Mark Luker and Rodney Peterson, Computer and Network Security Architecture, Jossey-Bass Inc. 2003

[16] Chris Herringshaw, Detecting attacks on Networks, December'1997

[17] Lih-Chyau Wuu, Sout-Fong Chen, Building Intrusion Pattern Miner for Snort Network Intrusion Detection System, IEEE , 0-7803-7882-2, 2003

[18] Matthew V. Mahoney and Philip K. Chan, Learning Rules for Anomaly Detection of Hostile Network Traffic, 2003

[19] Michel Attig and John Lockwood, SIFT: Snort Intrusion Filters for TCP, Computer Society, IEEE, 1550-4794, 2005