Volume 2, Issue 8, August 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Network Security Using IP firewalls

Mr. Sachin Taluja[1], Mr. Pradeep Kumar Verma[2], Prof. Rajeshwar Lal Dua[3]
[1]*M.Tech Scholar, Department of Electronics & Communication Engineering, Jaipur National University, Jaipur*
[2]*M.Tech Scholar, Department of Electronics & Communication Engineering, Jaipur National University, Jaipur*
[3]*HOD, Electronics & Communication Engineering, Jaipur National University, Jaipur*

ABSTRACT:-Network Security concerns with concept of designing a secured network is the most important task in any enterprise or organization development. Securing a network mainly involves applying policies and procedures to protect different network devices from unauthorized access. Servers such as web servers, file servers, mail servers, etc., are the important devices in a network. Therefore, securing these servers is the first and foremost step followed in every security implementation mechanism. Thispaperwork demonstrates the tasks needed to enhance the network security in Linux environment. The various security modules existing in Linux makes it different from other operating systems. we analyzing network packets using the most popular open source network protocol analyzer wire shark and on thebasis of analyzing the packet work has been done on writing the script to block/allow the network traffic using ip firewall and after blocking traffic further capturing and analyzing of packets using wire shark.

Keywords- Firewall, Linux, Network Security, wire shark, ip tables

I Introduction

Network security is an important task that must be seriously considered when designing a network. Network security is defined as the policies and procedures followed by a network administrator to protect the network devices from threats and simultaneously, the unauthorized users must be prevented from accessing the network[1].Network firewalls are devices or systems that control the flow of traffic between networks employing different security postures. The network traffic flow is controlled according to a firewall policy. The filtering decision is based on a firewall policy defined by network administrator. For each type of network traffic, there are one or more different rules. Every network packet, which arrives at firewall, must be checked against defined rules until first matching rule is found. The packet will be then allowed or banned access to the network, depending on the action specified in the matching rule[2].

Packet filtering allows you to explicitly restrict or allow packets by machine, port, or machine and port. For instance, you can restrict all packets destined for port 80 (WWW) on all machines on your LAN except machine X and Y.

Ip firewalls are used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different tables may be defined. Each table contains a number of built-in chains and may also contain user- defined chains[3].

II Linux Overview

Linux is an open-source operating system, as it has the main beneficial features where users can modify the code. It is designed in such a way that it can run on different types of hardware. Linux also supports different types of servers such as Apache server and SSH server to run on it and it supports web browser like Mozilla Firefox. Linux is used in a network because, it has a kernel programming interface, can support many users, can run many tasks, provides a secure hierarchical file system, is portable and has a large collection of useful utilities for system administration. Linux operating system supports in building firewalls, ipfirewalls and squid proxy server. Linux ipfirewalls which are used between WAN and LAN, provide good security and data filter from WAN network.

Ip firewalls are used to set up, maintain, and inspect the tables of IP packet filter rules in the Linux kernel. Several different firewalls may be defined. Ip firewalls is currently the default firewall package that comes from Red Hat, Centos, UBUNTU and Fedora, right after ipchains dominated them long time ago. Ip firewalls support different types of filters. To name a few, Ip firewalls can do filters and firewall rules by usernames, by group IDs and user profiles, by source and destination ports, by source host and destination hosts, by URLs, by IP addresses, by packet ID flags, by protocols, and a lot more including filtering by MAC address[4].

III Firewall Policies at Different Security Levels

In order to determine the impact from different security controls on network performance, seven different firewall security policies are specified, so as to set up the firewall system for a project qualitative evaluation. The security levels defined

in the paper are not based on any published class of security evaluation criteria such as the orange book . However, lower security levels are theoretically and practically less secured than higher security levels. There are four basic components in building a firewall policy, advanced authentication, packet filtering, and application gateway. We specify a total of seven configurations and security levels of firewall, according to the requirementsstated in the corresponding security policies we defined theoretically. Security is considered higher for a higher level [5].

IV Firewall rules

Different firewalls usually provide different rule logic with different parameters. But some basic elements are common to all. They all allow an action to be defined allowing or banning specific network traffic. Also, all of them allow checking for most important elements in packets like IP addresses, ports and protocol. Software for firewall rule optimization (FIRO) was originally developed for ip firewalls firewall command tool. One of the most important functionalities of ip firewalls firewall is stateful inspection. Stateful inspection automatically opens only the ports necessary for internal packets to access the Internet. It only allows transfer of packets which are defined in firewall rules and which are part of established connections.

V Firewall chains

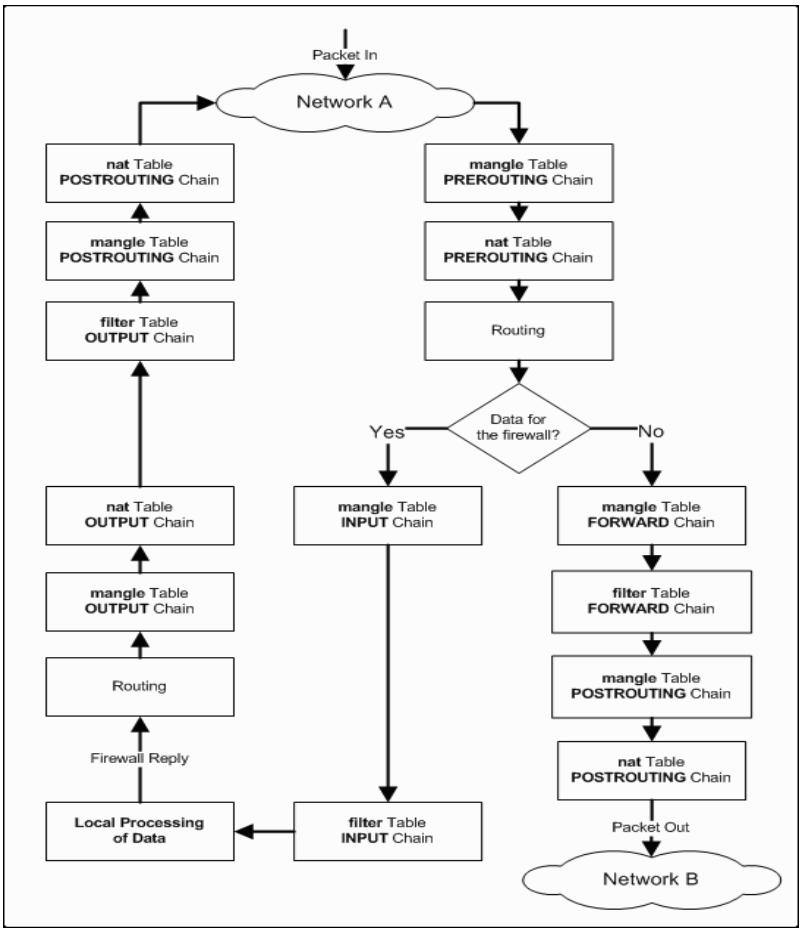
ip firewalls group rules in chains. Different network packets are processed by different chains:
•Incoming traffic – packets for firewall (INPUT chain).
•Forwarding traffic – incoming packets for anotherMachine (FORWARD chain).
•Outgoing traffic – packets generated by firewall(OUTPUT chain).

VI Firewall Rule Parameters

Each rule identifies specific type of network traffic. In order to enable this identification parameters for identification of specific network packets must be set for each rule.
FIRO provides optimizing procedure which is based on these parameters:
• IP addresses – it can be destination or
Source IP address; also, it can be written as a single IP, network IP or IP range,
• Ports - it can be destination or source
Port; also, it can be written as a single port, port range or port array,
• Protocol – it can be referred to TCP, UDP, and ICMP or all together,
• Interface – it can be incoming or outgoing interface,
• TTL (Time To Live) field residing in the IP headers,
• Tos (Type of Service) field residing in the IP headers,
• Length of packet,
• MAC source address,
• Syn flag – identification of new connection,
• ICMP type,
• Limit – maximum number of packetsin time interval.
Although FIRO allows use of all parameters, in real environment commonly used parameters are:
source and destination IP addresses, destination port which defines service or application, and protocol[6].

VII Linux Using IP Firewalls

The flow diagram of ipfirewalls is given below:
Input chain: Filters packets destined for the firewall.
Output chain: Filters packets originating from the firewall. The second table is the Nat queue which is responsible for networkaddress translation. It has two built-in chains; these are:
Pre-routing chain: NATs packets when the destination address of the packet needs to be changed.
Post-routing chain: NATs packets when the source address of the packet needs to be changed. The third is the mangle table which is responsible for the alteration of quality of service bits in the TCP header. It is necessary to specify the table and the chain for each firewall rule you create. There is an exception: Most rules are related to filtering, so Ip firewalls assumes that any chain that's defined without an associated table will be a part of the filter table. The filter table is therefore the default.



VIII Rules Targets

The target of a rule can be the name of a user-defined chain or one of the built-in targets ACCEPTS DROP, QUEUE, or RETURN. When a target is the name of a user-defined chain, the packet is diverted to that chain for processing. If the packet makes it through the user-defined chain without being acted upon by one of the rules in that chain, processing of the packet resumes where it left off in the current chain. These inter-chain calls can be nested to an arbitrary depth.

The following built-in targets exist:

(a) ACCEPT

Ip firewalls stops further processing. The packet is handed over to the end application or the operating system for processing.

(b) DROP

Ip firewalls stops further processing. The packet is blocked.

(c) LOG

The packet information is sent to the syslog daemon for logging. Ip firewalls continues processing with the next rule in the table. As you can't log and drop at the same time, it is common to have two similar rules in sequence. The first will log the packet, the second will drop it.

(d) ULOG

This target logs the packet but not like the LOG target. The LOG target sends information to the kernel log but ULOG multicasts the packets matching this rule through a net link socket so that user space programs can receive these packets by connecting to the socket

(e) REJECT

Works like the DROP target, but will also return an error message to the host sending the packet that the packet was blocked.

(f) DNAT

Used todo destination network address translation.I.e.rewriting the destination IP address of the packet.

(g) SNAT

Used to do source network address translation rewriting the source IP address of the packet.
The source IP address is user defined.

(h) MASQUE RADE

Used to do Source Network Address Translation.
By default the source IP address is the same as that used by the firewall's interface[7].

IX Experimental Setup

In this implementation part, one important thing to be considered is our implementation not only focuses on firewall configuration but also covers maximum aspects of building a secured network'. Therefore, firewall configuration using Ip firewalls, UBUNTU etc. We have also applied some of the security measures in configurations, Mainly setup includes Virtual Network Environment Using MS Virtual PC and installed UBUNTU Linux 9.04.Captured live traffic with Wire shark and offline analysis of traffic after that Writing of Shell script using Ip firewalls ,After blocking traffic using Ip firewalls again capturing and analyzing of traffic. The configurationsdone in each system are discussed in the following section.

Step1: To establish a segregate network using virtualization. Microsoft Virtual PC SP1 is used to establish a segregate network and UBUNTU 9.04 operating system is installed on it.
Step2:Configuring the Wire shark under root privileges Applications > Add/Remove applications > All open source application >wire shark.
Step3: Operating Wire shark (as root) and capturing network packets on eth0 interface.
Step4: Ip firewalls was downloaded under the root privileges from www.netfilter.org and installed by implementing. /configure, make, and make install command.
Step5: Writing of Ip firewalls script to deny/allow network traffic.
Step6: After blocking traffic using Ip firewalls again capturing and analyzing of network data packets using Wire shark.
The following are the various tasks and milestones completed along with the results. All the results are checked on machine Intel® Core™ 2 Duo CPU T8100 @ 2.10 GHz with frequency 778 MHz along with 2 GB RAM space. The Operating System used was Ubuntu-9.04 Linux operating system which was installed using virtualization software[8].

X Results

(a)For blocked HTTP traffic on TCP port no.80 on the Basis of specific URL's, Here we blocked social networking website that need to be banned in educational institution like www.facebook.com etc.

#Blocking of www.Facebook.com accessed through port no 80 ip firewalls -A OUTPUT -p tcp --dport 80 -d www.facebook.com -j DROP

(b)Blocking of Spam mails coming from specific IP address to secure the network so that unauthorized user was unable to access the resources of the system Here, we create new chain
SPAMLIST in which all the rules are appended through which we block spam mails coming from bad IP's. Blocked.ips is a file in which list of bad IP's is mentioned.

```
# Ip firewalls IP/subnet block script
IPT=/sbin/ip firewalls
SPAMLIST="spamlist"
SPAMDROPMSG="SPAM LIST DROP"
BADIPS=$(grep-Ev"^#|^$" root/blocked.ips")
# create a new ip firewalls list
$IPT -N $SPAMLIST
for ipblock in $BADIPS
do
$IPT -A $SPAMLIST -s $ipblock -j LOG --log-prefix
"$SPAMDROPMSG"
$IPT -A $SPAMLIST -s $ipblock -j DROP
done
```



```
$IPT -I INPUT -j $SPAMLIST
$IPT -I OUTPUT -j $SPAMLIST
$IPT -I FORWARD -j $SPAMLIST
Blocked.ips
192.168.1.0/24
Vsnloard.vsnl.net.in
202.54.1.2
SPAM
202.5.1.2
```

(c)Blocking of ICMP packet so that unauthorized user is unable to ping the system. Several Web sites block ICMP traffic due to DoS attacks

```
# set the default policies
ip firewalls -P FORWARD DROP
ip firewalls -P INPUT DROP
ip firewalls -P OUTPUT ACCEPT
```

In the mentioned method best thing is to drop the ICMP packets, by doing this we are not giving any clue to hacker whether the system is alive or not. Where as if we do reject definitely hacker will come to know that ICMP packets are blocked and the system is live.

```
#ip firewalls -A INPUT -p icmp --icmp-type echo-request -j
DROP
```

(d)In which we simply stop incoming/outgoing SMTP traffic to protect the system from the various types of attacks like Phishing, Hoaxes,and Trojans.

```
# stopping of reading and writing of Emails
ip firewalls -A INPUT -p tcp --dport 25 -j DROP
ip firewalls -A INPUT -p udp --dport 25 -j DROP
ip firewalls -A INPUT -p udp --dport 110 -j DROP
ip firewalls -A OUTPUT -p tcp --sport 25 -j DROP
ip firewalls -A OUTPUT -p udp --sport 25 -j DROP
ip firewalls -A OUTPUT -p udp --sport 110 -j DROP
```

(e)In this module we will work on blocking the P2P file sharing traffic. Peer-to-Peer (P2P) applications impede network traffic of businesses, governments, education, and the Internet infrastructure itself. These applications consume vast amounts of network resources, and prevent mission critical applications from accessing the network

```
# Block P2P Traffic
ip firewalls -A FORWARD -p tcp -m ipp2p --edk -j DROP
ip firewalls -A FORWARD -p udp -m ipp2p --edk -j DROP
ip firewalls -A FORWARD -p tcp -m ipp2p --dc -j DROP
ip firewalls -A FORWARD -p tcp -m ipp2p --kazaa -j DROP
ip firewalls -A FORWARD -p udp -m ipp2p --kazaa -j DROP
ip firewalls -A FORWARD -p tcp -m ipp2p --gnu -j DROP
ip firewalls -A FORWARD -p udp -m ipp2p --gnu -j DROP
ip firewalls -A FORWARD -p tcp -m ipp2p --bit -j DROP
ip firewalls -A FORWARD -p udp -m ipp2p --bit -j DROP
ip firewalls -A FORWARD -p tcp -m ipp2p --apple -j DROP
ip firewalls -A FORWARD -p tcp -m ipp2p --winmx -j DROP
ip firewalls -A FORWARD -p tcp -m ipp2p --soul -j DROP
ip firewalls -A FORWARD -p tcp -m ipp2p --ares -j DROP
```

XI Conclusions

The Firewall which works as the gateway for the network should be configured in such a way that it should not allow unauthorized users entering the network or accessing the information. Network audit informationsuch as log messages and network monitoring tool's record will also help in securing the network by providing information about the network access In this research paper, work has been done on capturing the live traffic using the network protocol analyzer Wire shark and on the basics of analyzed data packets further explored and designed the script using Ip firewalls to allow/deny the network traffic on the basics of the IP address of the computer sending the packets, the IP address of the computer receiving the packets, the type of packet (TCP, UDP, etc.), The port number, and URL's etc. This enables us to protect our system from a wide variety of hazards, including service attacks and hack attempts.

The script discussed here can be used for the purpose of network Security. From this implementation and research of enhancing network security, we found that; security is not only limited in choosing a secured operating system or secured server configurations, but also related to both physical and application security configured in the network.

Moreover, periodical enhancement of network security is to be performed in order to get rid of day to day attacks. Servers which contain important information are to be configured securely and placed in a secured environment.

References

[1] Enhancing Network Security in Linux Environment, Technical Report, IDE1202,February 2012

[2] Guidelines on Firewalls and Firewall Policy, Computer Security Division, National Institute of Standards and Technology Special Publication 800-41 Revision 1 Natl. Inst. Stand. Technol. Spec. Publ. 800-41 rev1, 48 pages (Sep. 2009) Gaithersburg, MD 20899-8930, September 2009

[3] Packet Filtering using IP Tables in Linux,"IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011"ISSN (Online): 1694-0814 [4]Linux - Wikipedia, the free encyclopediaen.wikipedia.org/wiki/Linux & Security Issues – Linux.orgwww.linux.org/article/view/security-issues & Quick HOWTO:Ch14 : Linux Firewalls Using iptables - Linux Home ...www.linuxhomenetworking.com/.../Quick_HOWTO_:_... - United States. &Packet filtering using iptables, http://netfilter.org/documentation/HOWTO/packet-filtering- HOWTO-7.html

[5] Michael R. Lyu and Lorrien K. Y. Lau,"Firewall Security: Policies, Testing and Performance Evaluation",& M. Goncalves, "Firewalls", McGraw-Hill, 1998 & Internet Firewalls and Securitywww.linuxsecurity.com/resource_files/firewalls/nsc/500619.html & Designing Scalable and Effective Decision Support for Mitigating ...web.eecs.umich.edu/.../securecomm11_vulnerability_m... - United States

[6] Tihomir Katić Predrag Pale,"Optimization of Firewall Rules "Proceedings of the ITI 2007 29 Int. Conf. on Information Technology Interfaces, June 25-28, 2007, Cavtat, Croatia &Manual: IP/Firewall/Filter - MikroTikWikiwiki.mikrotik.com/wiki/Manual: IP/Firewall/Filter & iptables - Wikipedia, the free encyclopediaen.wikipedia.org/wiki/Iptables &Net filter - Wikipedia, the free encyclopediaen.wikipedia.org/wiki/Net filter.& Firewall Policy Change-Impact Analysis ALEX X. LIU, Michigan State University & Guidelines on Firewalls and Firewall Policy, Computer Security Division, National Institute of Standards and Technology Special Publication 800-41 Revision 1 Natl. Inst. Stand. Technol. Spec. Publ. 800-41 rev1, 48 pages (Sep. 2009) Gaithersburg, MD 20899-8930, September 2009

[7] Daniel Bilar,"PacketProcessingInIptables"Computer science at UNO Spring 2011" & Linux Home ...www.linuxhomenetworking.com/.../Quick_HOWTO_:_... - United States. &Packet filtering using iptables

[8] ipfirewallsHome,http://www.netfilter.org/& iptables Scripting, http://www.linuxdoc.org/ [14]iptables command,http://www.redhat.com/docs/manuals/linux/RHL-9-Manual/ref-guide/s1-iptables-options.html

Authors:-

Sachin TalujaM.Tech Scholar at Jaipur National University, Jaipur. He received B.E. from M.D.University Rohtak, Haryana in Electronics and Communication . He has over 5 years of Industrial experience in the Field of Computers. His Area of interest includes Network Security, Artificial intelligence, Communication system, Computer architecture, Wireless Communications, Digital Communications, fiber optics, Nano Technology. He has attended various workshops on different domains of computers.

Pradeep Kumar Verma- Student of M. Tech (Communication and signal processing) final semester at Jaipur National University, Jaipur. Completed B. Tech from Northern India Engineering College, Lucknow from Uttar Pradesh Technical University in Electronics and Communications Engineering in 2009.Worked as Site Engineer for 9 months in Telecom Industry. I have keen interest in subjects like signal and systems, digital communications, information theory and coding and wireless communications.

Prof. Rajeshwar Lal Dua a Fellow Life Member of IETE and also a Life member of I.V.S & I.P.A, former"Scientist F" of the Central Electronics Engineering Research Institute (CEERI), Pilani has been one of the most well-known scientists in India in the field of Vacuum Electronic Devices for over three and half decades. His professional achievements span a wide area of vacuum microwave devices ranging from crossed-field and linear-beam devices to present-day gyrotrons. He was awarded a degree of M.Sc (Physics) and M.Sc Tech (Electronics)from BITS Pilani. He started his professional carrier in1966 at Central Electronics Engineering Research Institute (CEERI), Pilani. During this period he designed and developed a specific high power Magnetron for defence and batch produced about 100 tubes for their use. Trained the Engineers of Industries with know how transfer for further production of the same. In 1979 he visited department of Electrical andElectronics Engineering at the University of Sheffield (UK) in the capacity of independent research worker, and Engineering Department of Cambridge University Cambridge (UK) as a visiting scientist. After having an experience of about 38 years in area of research and development in Microwave field with several papers and a patent to his credit. In 2003 retired as scientist from CEERI, PILANI & shifted to Jaipur and joined the profession of teaching. From last eight years he is working as professor and head of electronics department in various engineering colleges. At

present he is working as head and Professor in the department of Electronics and communication engineering at JNU, Jaipur. He has guided several thesis of M.tech .of many Universities.

