Implementation of Network Security Analysis in Open Source Software Linux

Voore Subba Rao
Research Scholar,
Dayalbagh Educational Institute,
Department of Computer Science
DEI, Deemed University
Agra City., India

Vookanti Ramu
Asst.Professor
Chaitanya Institute of Tech. & Science,
Computer Science & Engineering Dept
Affiliated to Kakatiya University
Warangal Dist., India

Abstract- Network Security is most important concerns with concept of designing and managing a secured network and information security in any enterprise or organization management efficiently. Secure a network mainly involves applying policies and procedures to protect from unauthorized access. This paperwork demonstrates the tasks needed to enhance the network security using in Linux environment. And also this paperwork describes the importance open source software linux policies for secure the information. The Linux is open source software can get software upgrades directly from internet. This research project explores the key role of Linux configurations that the server an easy target to hackers over the internet. By following industry best practices by some security configurations, a Linux Server can be well secured. This research project explores and suggests best practices for the general hardening for common Linux security services such as Proxy server, Apache Web Server, and firewall (IPTABLES) to block connections to unwanted ports and blocking bad traffic and minimize unauthorized access and maximize security, privacy and access protection of organization network.

Index Terms - **Firewall, IP Tables, Proxy Server, Apache Web Server, Open Source Software, Linux**

I. INTRODUCTION

Network security is an important task to manage information security. 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. This research paper focusing the importance of Open Source Software Linux for implementing the network policies for well maintaining the organizational network. 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. 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 selected computers. 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[1,5].

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 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 multiple tasks, provides a secure hierarchical file system, is portable and has a large collection of useful utilities for users with network-related responsibilities. Linux operating system supports in building firewalls, IP firewalls and squid proxy server. Linux IP firewalls 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 Linux. IP firewalls can do filters and firewall rules by usernames, by source and destination ports, by source host and destination hosts, by URLs, by IP addresses and filtering by MAC address[5,10]

III. LINUX NETWORKS

Linux is used to drive networks in mission-critical environments and system/network administrators working in those environments must have far deeper expertise than ever before. Advanced Linux Networking picks up where conventional Linux networks, helping experienced Linux system and network administrators accomplish more and more solve more problems. The Linux networks structured into four sections, each essential to the working Linux administrator: Low-Level Configuration, Local Network Servers, Internet Servers, and Network Security and Router Functions. In-depth coverage includes: kernel and TCP/IP configuration, alternative network stacks, server start up scripting, DHCP configuration, Kerberos authentication, printer sharing, mail protocols, remote login servers, GUI access, remote system administration, network backups, iptables firewalls, and VPNs. The extensive section on Internet services shows how to handle virtual domains and secure sites; analyze Apache log files; and run FTP servers; and contains detailed coverage of SMTP-based email systems [13].

3.1. Linux Networks Hardware and Software issues

The security issues need to be considered and potentially deal with number of different tools and process available security exposures they represent. These issues are described in the following some representative software and hardware security issues in linux networks. Many of these software products can be downloaded from one or more of the Web sites listed in. Some of the security measures described is obvious and in common usage such as passwords it is used in the Linux networks.

The Internet has become a hazardous place, in the last few years. As the traffic increases and more important transactions are taking place your risk grows as bad guys try to damage, intercept, steal or alter your data. If there is something worth stealing then someone will try and steal it. Linux-based systems have no special exclusion from this universal rule. A primary reason that Linux systems are so popular is because they are robust and have many sophisticated security measures.

3.2. Firewalls Security in Linux

A firewall is one of the most widely used solutions for the Internet world. All traffic inside to outside and vice versa, must pass through the firewall.

A firewall is one of the most widely used solutions for the Internet world. All traffic inside to outside and vice versa, must pass through the firewall. Different types of firewalls have different types of rules and security policies. The authorized traffic will be sent based only on local policies. The firewall itself is protected, i.e.; it uses a trusted hardware and operating system[17].

IV. EXPERIMENTAL SETUP

The open source operating system software RedHat Linux is the provide security for network using network policies Proxy server, Web server and Firewall. The live experimental setup as follows.

4.1.Proxy Server filtering web content

Squid is a proxy server for caching and filtering web content. Squid proxy is used by various organisation and internet providers to reduce bandwidth and to increase response time. Squid proxy service will cache the requested web-content and re-using it for the further request of the same content.

Squid is the most popular proxy server for linux systems. It also used for the web filtering. Its widely use for increasing web server speed by caching repeated data.

In the below diagram, squid proxy will cache the web content of cse.cits.com.com from the ISP during the first request and it will deliver the cached content for the further requests of cse.cits.com without requesting from ISP. This will reduce bandwidth and will increase response time as the content is delivered from the local network[10].

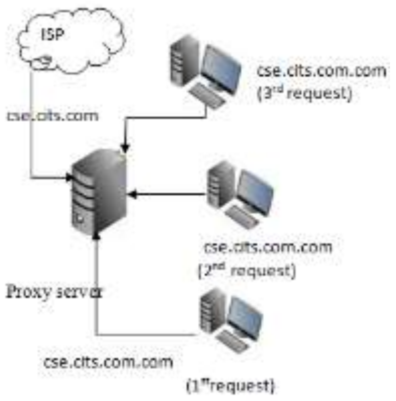


Fig.1 Proxy Server in Linux

Implementation of Proxy Server in Linux

Configuration and install of squid server

```
#yum install squid
```

1. Share specific website with squid

```
#acl shareip dstdomain 192.168.10.10
#http_access allow 192.168.10.10
```

Block specific website with squid

```
#acl blocksite1 dstdomain yahoo.com
#acl blocksite2 dstdomain www.rediff.com
#http_access deny blocksite1
#http_access deny blocksite2
```

2. create a file /etc/squid/blockwebsites.lst and put domain names one per per line and add below rule in squid configuration file.

```
#cat /etc/squid/blockwebsites.lst
yahoo.com
facebook.com
rediff.com
```

```
#acl blocksitelist dstdomain "/etc/squid/blockwebsites.lst"
#http_access deny blocksiteslist
```

4.2.Apache Server Web Page Authentication and Security

Web Page Authentication Security in Linux using Apache server. Only authorized users can login the web page content. The following method used to implementation method for creating Web Page authentication in Linux as follows.

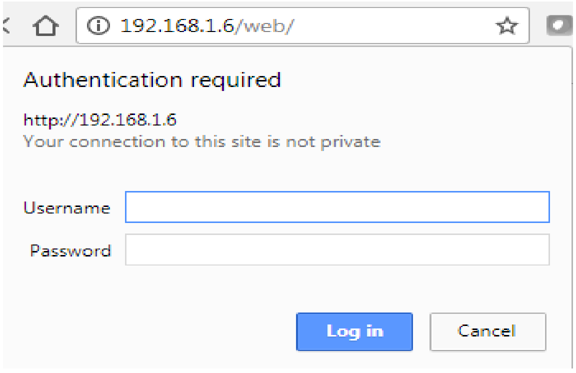
```
#htpasswd
#htpasswd -c /etc/httpd/.htpasswd deepak
New password:
Re-type new password:
Adding password for user Deepak
```

Next create a .htaccess file with below content at /var/www/html/secret/.htaccess

```
AuthType Basic
AuthName "Secret Files"
AuthUserFile /etc/httpd/.htpasswd
Require user Deepak
```

We are all set up to start out httpd server

```
# systemctl restart httpd
# systemctl is-active httpd
```



192.168.1.6/web/

Authentication required

http://192.168.1.6
Your connection to this site is not private

Username

Password

Fig.2 Password authentication for web page access

4.3. Firewalls (IP Tables) Network based security

Managing network traffic is one of the toughest jobs a system administrators in Organization.. The Administrator must configure the firewall in such a way that it will meet the system and users requirements for both incoming and outgoing connections, without leaving the system vulnerable to attacks. IP Tables is a Linux command line firewall that allows system administrators to manage incoming and outgoing traffic via a set of configurable table rules. IP Tables uses a set of tables which have chains that contain set of built-in or user defined rules[10].

Configuration and Implementation of IP Tables in Linux

To Start/Stop/Restart Iptables Firewall

```
#/etc/init.d/iptables start
# /etc/init.d/iptables stop
# /etc/init.d/iptables restart
```

Specific IP Address in IPtables Firewall

If you find an unusual or abusive activity from an IP address you can block that IP address with the following rule:

```
# iptables -A INPUT -s 192.168.10.10  -j DROP
```

Unblock IP Address in IPtables Firewall

If you have decided that you no longer want to block requests from specific IP address, you can delete the blocking rule with the following command:

```
# iptables -D INPUT -s 192.168.10.10 -j DROP
```

Block Facebook on IPtables Firewall

Some employers like to block access to Facebook to their employees. Below is an example how to block traffic to Facebook.

First find the IP addresses used by Facebook:

```
# host facebook.com
facebook.com has address 66.220.156.68
# whois 66.220.156.68 | grep CIDR
CIDR: 66.220.144.0/20
```

You can then block that Facebook network with:

```
# iptables -A OUTPUT -p tcp -d 66.220.144.0/20 -j DROP
```

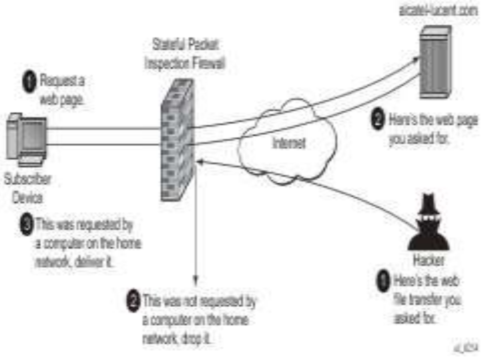

alcatel-lucent.com
Stateful Packet Inspection Firewall
1 Request a web page.
Subscriber Device
Internet
2 Here's the web page you asked for.
3 This was requested by a computer on the home network, deliver it.
2 This was not requested by a computer on the home network, drop it.
Hacker
1 Here's the web file transfer you asked for.

Fig.3 Fire wall Network protection policy

V.COMPARATIVE STUDY & REULTS

The comparative study is enhance the live implementation and security levels of using Proxy server, Firewall and Web page security. These Performance levels and utilization report of these Security levels in Linux is as follows.

5.1. Analysis of Proxy Server filtering web content

Table1: Proxy server for filtering network traffic of web pages.

Security (in %)	Fast Accessing of Web Pages (in %)	Access IP Address (in %)	Blocking IP address (in %)	Blocking web content (in %)
Proxy Server	80	90	90	90

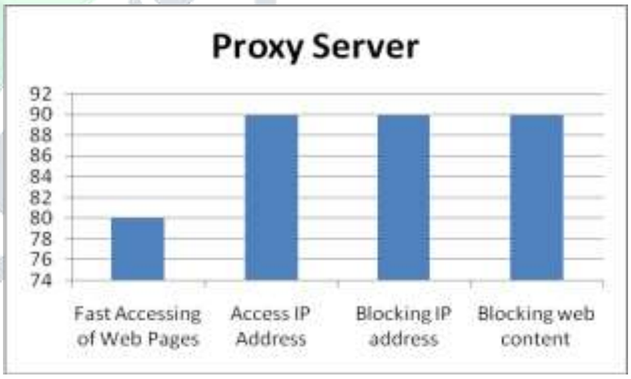


Fig.4 Proxy server for filtering network traffic of web pages.

5.2. Analysis of Apache Server Web Page Authentication and Security

Table2: Web Page authentication of users logins and passwords

Security (in %)	Web Page access (in %)	Web page secure access (in %)	Web Page Access login & password (in %)
Web Page Access	90	95	85

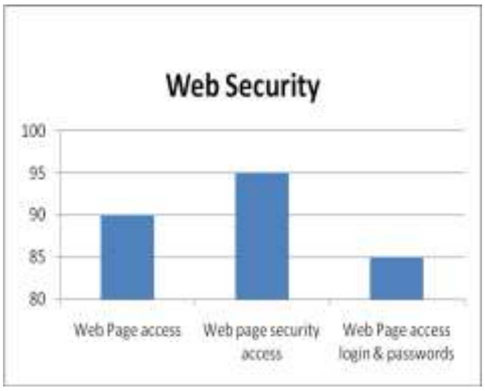


Fig.5 Graph Showing the authentication in web page

5.3. Analysis Firewalls (IP Tables) Network based security

The security and filtering capability of Firewall IP Tables implemented in Linux in a tabular form.

Table3: Firewalls for filtering traffic method.

Security (in %)	Drop IP address (in %)	Block Social websites access (in%)	Block Social websites access (in %)	Accept IP Address access (in %)
Firewalls (IP Tables)	90	85	90	85

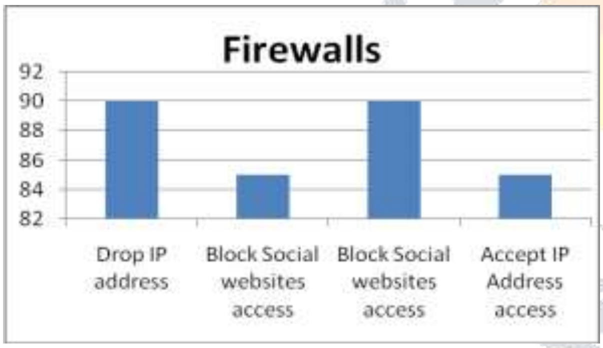


Fig.6 Graph of suing firewall for filtering traffic Proxy Server

CONCLUSION & FUTURE SCOPE

In this topic security in Linux Environment implementation and research of enhancing network security is done. The Security is not only limited in choosing a secured operating system or secured server configurations, but it is also related the both physical and application security configured in the network. The above implementation security methods by using Open source software Linux secure polices are important for Administrator to put secure of organization. Moreover, periodical enhancement of network security is to be performed in order to get rid of day to day attacks. The Secure environment information are to be configured securely and placed in a security system. In this scenario use the Firewall -which not usage the unauthorized users entering the network or accessing the information Network audit information such as log messages and network monitoring tool's record will also helps in securing the network by providing information about area of research in which policies and procedures used for security implementation are updated frequently, based on types of new attacks discovered. In future work, we enhance more secure methods using Linux for implementing network policies for useful way.

ACKNOWLEDGMENT

Thanks to the God for His showers of blessings throughout my research paper work to complete the research successfully. I would like to express my deep and sincere gratitude to management and principal of Dayalbagh Educational Institute, Agra providing computer systems and infrastructure in time to complete my research paper.

REFERENCES

[1] Peter G.smith,"Linux Network Security", Charles River Media, Edition 1, March 2005.

[2] Ken Denniston, "Building a Simple Network", Intel Press, Edition 2, Chapter -1.

[3] Wenzheng Zhu; Changhoon Lee; Coll. of Comput., Konkuk Univ., Seoul", Design for Security Operating System", IEEE Computer Conference on Third Asia International, pp. 667-670, 2009.

[4] LI Hongjuan, LAN Yuqing, "A Design of Trusted Operating System Based on Linux", IEEE Computer

[5] Bokhari, S.N.,"The Linux operating system", IEEE Computer,vol. 28,no. 8,pp 74-79.1995.

[6] W. A. Arbaugh, D. J. Farber, and J. M. Smith, "A Secure and Reliable Bootstrap Architecture," in IEEE Computer Society Conference on Security and Privacy. IEEE, 1997, pp. 65–71.

[7]Mark G. Sobell, "A Practical Guide to Ubuntu Linux", Third Edition, Pearson.

[8] Haral Tsitsivas, "UNIX System Management and Security: Differences between Linux, Solaris, AIX and HP-UX", white paper, SANS institute, 2007.

[9] Machtelt Garrel, "Introduction to Linux", Edition 1.27, 2008.

[10] Jichiang Tsai; Chung-Hsin Feng; Chuyuan Tsai," A Network Safety-Defense Mechanism with the Linux Security Module", 2006 IEEE Region 10 Conference, pp. 1-4, 2006.

[11] Si-Jung Kim; Choul-Woong Son; Cheon-Woo Lee," Linux based Unauthorized Process Control"IEEE Computer Conference on ICISA,pp. 1-5,2011.

[12] Chris Wright, Crispin Cowan, Stephen Smalley, James Morris, Greg Kroah-Hartman,"Linux Security Module: General Security Support for the Linux Kernel", Emmanuel Fleury, 2006-2007.

[13]James Morris,"SELinux", source: http://selinuxproject.org/page/Main_Page(Last accessed: February 06, 2012)

[14]Alan Bartlett,"SELinux", Source: http://wiki.centos.org/HowTos/SELinux (Last accessed February 06, 2012)

[15] Werner Puschitz," Securing and Hardening Red Hat Linux Production Systems", PUSCHITZ.COM, 2007.

[16] J. Marceline, S. Smith, O. Wild, and R. MacDonald, "Experimenting with TCPA/TCG Hardware, Or: How I Learned to Stop Worrying and Love the Bear," in Technical Report TR2003-476, Dartmouth PKI Lab Dartmouth College, Hanover, New Hampshire, USA, December 2003.

[17] Deng Yiquan," Linux Network Security Technology", IEEE Computer Conference on CASE,pp. 1-3,2011.

[18] William Stallings, "Cryptography and Network Security Principles and Practices", Edition:4, Prentice Hall,2005.

[19] Eric A. Young, Tim J. Hudson,"Open SSL", Source: http://www.openssl.org/(Last accessed: February 06, 2012).

[20] Anthony J.Stieber, "OpenSSL Hacks", Linux Journal Issue #147/July 2006.

[21]Ubuntu documentation team,"Open SSH Server" Source:https://help.ubuntu.com/8.04/serverguide/C/openssh-server .html (Last accessed: February 06, 2012).

[22] R .Arends, R. Austein, M.Larson, D.Massey, S.Rose," DNS Security Introduction and Requirements", rfc: 4033, The Internet Society, 2005.

the network access. In the network security system is a wide

[23] Duane De Capite, “Self-Defending Networks: The Next Generation of Network

[24] Security”, Cisco Systems, Inc., September 2006.

[25] William H. Allen, Gerald A. Martin and Luis A. Rivera. “Automated detection of malicious reconnaissance to enhance network security” in IEEE conference on South east, Publication 2005, pages: 450-454.

[26] David Kotfila, Joshua Moorhouse, Ross Wolfson, "CCNP Implementing Secured Converged Wide-Area Networks (ISCW 642-825) Lab Portfolio. (Last accessed: November 24, 2011)

[27] IBM Corporation” Understanding DNS Queries”, iSeries Information Center, Version 5 Release 3,2002, 2005.

[28] Rick Hofstede, Tiago Fioreze, Surf Map: A network Monitoring Tools Based on the Google Maps in IEEE conference on Integrated Network Management, Publication 2009, Pages: 676-690.

[29] Paul Ferrill”Linux Network Monitoring Tools -Ping and Etherape”, Tutorial, Quintet Inc, 2012.

[30] Gordon Lyon,”Nmap.org”, Source: http://nmap.org/ (Last accessed: February 06, 2012).

[31] Richard Sharpe, Ed Warnicke “Wireshark”, Source:http://www.wireshark.org/docs/wsug_html/#ChapterIntroduction (Last accessed: February 06, 2012).