Security Analysis in Open Source Linux Network

*** Mukesh Kumar Mishra, * Dinesh Goyal**

Suresh Gyan Vihar University, Jaipur

Abstract: Simple way Linux is an operating system. It is the usage of software on a computer that enables applications and the computer operator to access the devices on the computer to perform desired function. Linux operating system is very similar to other operating systems such as windows and OS X. The security system in Linux operating system it has password authentication, file system discretions access control and security auditing. The Linux system considered to be free from viruses and malware. The different Linux tools or utilities used in implementing security are explored. Secondly, a network topology is designed using Linux systems, which contain different server and firewall configurations. One of the systems is used as the attacker system for testing the network security. Results are obtained when the attacker system tries to access the internal network, along with attack analysis information are then documented. These results are considered in one scenario. In this scenario, the results of testing the network before configuring the firewall and applying security measures in server configurations are explained, and are compared with the results after configuring.

Keywords: Linux, Security, Ping,nmap

I. INTRODUCTION

Open source software is software for which the source code is available to anyone. It can be thought of as a kind of blueprint for the software, a form that is ideal for gaining understanding of how a program works or modifying its design. A program’s source code is in many cases processed by another program called a ‘compiler’, which creates the actual file that runs on an end-user’s computer. This file is called the object code, and it is this that an end-user receives when buying traditional proprietary, closed-source software like Microsoft Word. In comparison to its source code, the object code of a program is very difficult for a human being to comprehend or modify. Thus, open source software can be said to invite and facilitate modification, while closed source software tends not to. These technical characteristics are also generally carried through into the accompanying licenses open source licences permit modification and redistribution by the user, while closed source end-user licence agreements tend to contractually bind the user to refrain from modifying or redistributing the software that they cover

.

1.1 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 than they can with any other book. Its breadth and depth make it an exceptional single-volume reference for every Linux professional [9].

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 startup scripting, DHCP configuration, Kerberos authentication, printer sharing, mail protocols, remote login servers, GUI access, remote system administration, network backups, iptables firewalls, and VPNs[13]. 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. Among the topics covered in exceptional depth: configuring Kerberos; running time servers, font servers, and chroot jails; and using Samba's scripting capabilities to burn CDs and create PDFs. For every experienced Linux system or network administrator, and for Linux power users with network-related responsibilities.

Some of the Linux functionalities are as follows:

a. **Flexibility:** Linux is flexible, as it supports high-performance server applications, desktop applications and embedded systems.

b. **Stability:** In the Linux system, if a new program or software is installed, it does not require to be rebooted periodically. Hence, it maintains the performance level of the system.

c. **Performance:** It does not degrade the performance level of the system even though it handles a large number of users simultaneously.

d. **Network friendliness:** Linux is a user-friendly operating system in terms of networking functionality such as; it can be easily configured as the server system or the client system depending on the requirement in the network.

e. Security: The Linux operating system is built with security features, as it provides the file access permission mechanism, which prevents the unauthorized users in gaining access to the files.

1.2 Security Issue in Linux Networks

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 [3].

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 [6].

As the manager of a Linux system for your department or small business, you might feel a bit daunted by all of these threats. You've heard Linux is supposed to be secure. It is a truism, of course, that if you don't use the Linux security tools provided, then you should be ready for the inevitable break-in.

Problems can also be caused by badly implemented security measures. Securing a Linux machine can get pretty complicated and entire shelves of books have been dedicated to the subject [8]

- Managing user authentication and accounts.
- Access control on file and directory.
- Process management.
- Network access control.
- Hacking prevention functions.
- Functioning of self-protection.
- Installation and performance [11]

II. SECURITY MEASURES

2.1 Firewalls

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. Generally, firewalls are of three types.

• Circuit level firewalls
• Application level firewalls

2.2 Network Servers overview

The servers which are commonly found in a network are discussed in the following sections.

- **Apache web server**

Apache web server is one of the widely used web servers in the world, as it possesses multi-threading concepts. In Apache server, both HTTP and HTTPS services are available. HTTP protocol is designed to deliver the communication between the clients and servers. By default, it runs on the port number 80. HTTP is used to establish normal connections.

HTTPS runs by default on port number 443 and it establishes secured connection. When establishing the HTTPS connection, the server responds to the client with a list of encryption techniques. In return, the client prefers the better connection mechanism. Therefore, the authentication of servers and clients is verified by exchanging the certificates and encrypted information in order to ensure that both use the same keys. HTTPS is most widely used in login pages of banks and corporate companies.

- **OpenSSL (Open Secured Socket Layer)**

SSL is an open-source tool kit which is implemented by the two layered protocols. They are: SSL v2/v3 and transport layer protocol. It uses the strong cryptography library. The current version of openSSL is 1.0.0e, that includes bugs and security fixes. OpenSSL supports many numbers of cryptographic algorithms and protocols.

SSL provides better security for web services. OpenSSL records the confidentiality and integrity for the SSL connections and also provide better security features to the higher layered protocols. For HTTP, it provides the transfer service for web client/server interaction that can operate on top of SSL [19].

There are also other three higher level protocols, which have a key role in the management of SSL exchange, they are:

- Handshake protocols.
- Change cipher protocol.
- Alert protocols [20].

- **Mail server**

Send mail server is one of the best mail servers used in the majority of real environments. By default, Send mail server can only send mails; it can't receive any mail. It is very important that receiving mail should be properly scanned and checked. Send mail supports a number of mail transfers and delivery methods such as SMTP, which is used for email transport over the Internet.

- **OpenSSH**

OpenSSH is a free version of SSH, and it provides the encrypted communication over the Internet. The tools such as telnet and rsh are insecure because they transmit passwords in clear text format. OpenSSH provides a better security service during the transfer of files.

For client connections, the SSHD (a component of SSH server) listens continuously from any client tools. OpenSSH uses different types of authentication methods, such as regular passwords and public keys [21]. Generally, telnet, rsh, and rlog are not safe remote applications because these are prone to eavesdropping. For this reason, most companies will prefer SSH for remote logins.

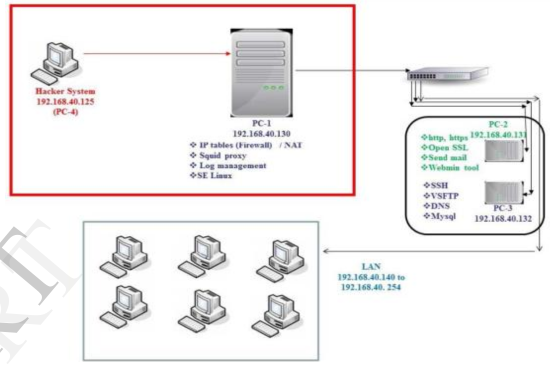
- **DNS Server**

DNS stands for Domain Name System and it is a hierarchical distributed database. It translates domain names into IP addresses and vice-versa. As the domain names are alphabetic, they are easier to remember than IP addresses, which contain numbers. However, any public or private networks are based on IP addresses but not domain names. Each time when we use a domain name, it is the DNS server which translates the name into the corresponding IP address. For example, the domain name www.example.com might be translated to 192.168.40.132. Every network contains one or more DNS server. If one server fails to translate a particular domain name, it is handled by another server and so on. In brief, DNS serves as the phone book for the Internet by mapping the directory of domain names with IP addresses and vice-versa. Therefore, securing DNS server is an important part of securing a network.

III. EXPERIMENT SETUP

Most important thing is to be considered that in our implementation it not only focuses on firewall configuration but also covers maximum aspect of building a secured network. It covers secured server installation and configurations. Firewall configuration uses IP tables, SE-Linux etc. It is applied some of the security measures in server configuration and experimental setup.

Figure below is the block diagram for implementation in a real environment, which clearly describes the function and position of each device in the network.



In the above diagram it represents our implementation in VMware consisting of two systems, which are PC-1 and PC-4. All the configurations of PC-2 and PC-3 are added to PC-1 as it is considered only two systems in VMware instead of four systems.

The configurations done in each system are discussed in the following section.

PC-1:

PC-1 consists of

- Firewall configurations:
  - o IPtables
  - o SE Linux
- Network Monitoring tools:
  - o Wire shark
  - o IPtraf
- Server configurations
  - o HTTP
  - o HTTPS
  - o OpenSSL
  - o Send mail
  - o SSH
  - o VSFTP
  - o DNS
  - o MySQL
- Web interface tool: Webmin

PC-4: PC-4 is used from outside network to test security of designed Linux network. This system contains few hacking tools to test the connectivity.

PC-4 consist of following tools

- Nmap
- Wireshark
- IPtraf

IV. PROCEDURES

Steps followed in obtaining results in both scenarios are:

Step 1: First, is known by pinging the target IP address domain name of PC-1 from PC-4.
Step 2: Then, a **reconnaissance attack** is generated using **nmap**, to gather information of the target machine.
Step 3: Attack-related information is shown using **IPtraf** and **Wireshark** in PC-1.
Step 4: An attempt to access the **HTTP server** in PC-1 is done from PC-4.
Step 5: The access information of different servers is shown as log messages in PC-1.

V. COMPARATIVE STUDY

Securities Applied in Scenario II are:
(1) Firewall
(2) Send mail server
(3) DNS server
(4) Apache web server
(5) SSH Server

Steps	Task	Scenario I (Without Security)	Scenario II (with security)
Step 1	Ping IP Address of client	IP identified	IP not identified
Step 2	Reconnaissance attack with nmap	IP Identified	IP not identified
Step 3	IP traf and wire shake attack	Access provided	Access Derived
Step 4	HTTP server Access	Browser Accessed	Browser not Access
Step 5	Log Message Access	Access Provided	File does exist

VI. CONCLUSION

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. 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 help in securing the network by providing information about the network access. In the network security system is a wide area of research in which policies and procedures used for security implementation are updated frequently, based on types of new attacks discovered.

VII. FUTURE WORK

It is likely that some form of labelled networking will be implemented for Enhancing Network Security in Linux Environment .In this network traffic itself is labelled and typically is used in military and government environments dealing with classified information. An earlier version of Network System used IP options to label packets, although it was dropped before merging with the upstream kernel as the hooks it needed were too invasive.

A possible alternative is to integrate Linux network system with IPSec and label the Security Associations instead of the packets. A packet arriving on specific networks would be labelled implicitly with the context of the Network systems. A prototype of this scheme was implemented for the preceding Flask Project, and it should be useful as a guideline. More general integration of Linux systems with network security components, such as cryptography and firewalling, also are areas for future exploration.

The topic can be extended by using any Intrusion Prevention System or Intrusion Detection System. The model Use of IDS with any IPS is highly recommended, because IDS detects the attack whereas IPS can be used to prevent that particular attack.

VIII. 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 International conference on Electrical and control Engineering, pp 4598 – 4601, 2010.

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.

23. Duane De Capite, "Self-Defending Networks: The Next Generation of Network Security", Cisco Systems, Inc., September 2006.

24. 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.

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

26. IBM Corporation" Understanding DNS Queries", iSeries Information Center, Version 5 Release 3,2002, 2005.

27. 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.

28. Paul Ferrill"Linux Network Monitoring Tools - Ping and Etherape", Tutorial, Quintet Inc, 2012.

29. Gordon Lyon,"Nmap.org", Source: http://nmap.org/ (Last accessed: February 06, 2012).

30. Richard Sharpe, Ed Warnicke "Wireshark", Source:http://www.wireshark.org/docs/wsug_html/#ChapterIntroduction (Last accessed: February 06, 2012).