International Journal of Basic and Applied Science 8 (2) (2019) 36-46

Published by: IOCSCIENCE

International Journal of Basic and Applied Science

Journal homepage: www.ijobas.pelnus.ac.id

Ubuntu Linux Server Security Analysis and Simulation With Port Knocking & Iptable

Onno Widodo Purbo
Institut Teknologi Tangerang Selatan, Indonesia

Article Info

Article history:

Received February 10, 2019
Revised August 19, 2019
Accepted Sept 30, 2019

Keywords:

Simulation;
Network;
Linux Ubuntu.

ABSTRACT

Computer network security is very important to maintain the confidentiality of data and information contained on the server. This data and information is only intended for administrators and users who have the right to access it through the service port. Leaving an important port open is a fatal mistake that can result in an attack on the server. The existence of Linux as an operating system kernel developed with a copyright or opensource model, computer networks using Linux servers are able to manage all internet services, including routers, database servers, proxy servers and FTP servers, in addition to the distributions. also easy to find in the market. One of them is ubuntu, ubuntu is one of the distributions that has been used by many people because Ubuntu has a user-friendly interface and many developers and is supported by a very large community. The method used in this study is the method of observation, interview and design of the Linux Ubuntu iptables operating system security, and the results of this study explain that the use of Iptables configuration on the Ubuntu Linux operating system can be done on a LAN and Wifi cable connection, as long as all clients are on the same class then the Iptables configuration can block client access to the server and can be done the other way around, namely blocking server access to the client. By using the accept setting, this system can also reject certain IP addresses or ports, in addition to accepting other connections. If you want to reject all connections and want to specify what connections you want to do manually, then you have to change the default setting from chain to drop. This method can only be useful for servers that have sensitive information, and only use the same IP address to connect to that server.

Corresponding Author:

Onno Widodo Purbo
Institut Teknologi Tangerang Selatan, Indonesia
Komplek Komersial BSD, Jl. Raya Serpong Jl. Komp. Bsd No. Kav. 9, Banten
Email: onnowidodo@gmail.com

1. INTRODUCTION

It is undeniable that the development of technology and information from year to year has always experienced a very significant increase, this role certainly has an impact on various aspects of human life, such as in the fields of education, economy, and government, but these developments will certainly accompanied by various acts of fraud and crime by irresponsible parties, such as data theft and destruction of a network, as for some of the ways that have been done is by implementing a firewall as

a barrier to restrict access. Technology is starting to be utilized optimally and accompanied by the rapid development of software in various parts of the world, and Indonesia is no exception, especially in the use of operating systems [1]. Computer network security is indeed very important to pay attention to, especially in this technological era, the fact is that there are many institutions or public organizations that do not care about these security problems, but when the network is capable of being hacked and resulting in overall control of the computer system, the repair costs will also increase [9]. will be very high and more and more complicated. Therefore, the need for a very high security increase in order to avoid various damages and threats to the computer network system, of course the most important point in the service of a network is the security of access on ports and servers that are able to connect directly to the internet [2] [5].

Advances in technology, especially computer networks, are very helpful in the field of information and information data processing. Computers play an important role in information technology, through computers, the desired information will be obtained without the limitations of space and time, and by maximizing the use of computer systems in an integrated computer network, data information will be obtained quickly and precisely. In this digital era, the existence of a computer is one of the communication tools that always plays an important role in human life. In line with that, computer users must be balanced with the ability of the user to be able to use it as well as possible. In line with the development of information technology, computer network support equipment is still very much needed, especially in the construction of computer networks.

One of the most widely used Open Source Software by the world community, especially in the use and management of computer network systems, is the Linux operating system. Linux is an operating system kernel developed under an open copyright model. The availability of open source applications on the Linux operating system makes many government institutions and educational institutions choose to use an operating system that is open. A computer network using a Linux server is able to manage all internet services, including routers, database servers, proxy servers and FTP servers, and so on. Linux development was first carried out by Linus Benedict Torvalds. All Linux source code including kernel, device drivers, libraries, programs and tools are distributed freely under the GPL (General Public License). As for the basis, Linux distributions are divided into several types, including (1) Debian such as Knoppix, Ubuntu, Kuliax, BlankON (2) RPM (RedHat Package Manager) such as PCLinuxOS, FedoraCore, IGOS, CentOS, EduLinux (3) Slackware such as Slackware , Kate OS, Truva Linux, ZenCafe Linux, Wolfix [7] [11].

The Linux operating system is an alternative that is used to replace the Windows operating system. The development of Linux is very fast, because this operating system was developed by everyone who wants to develop it, while the basic difference between Linux and other operating systems lies in the Linux Kernel and the components in the system that are free and open. Linux is not the only operating system that is open source, although Linux is the most widely used open source operating system. Some free and open source software licenses are based on the principles of copyleft, a concept that adheres to the principle that works produced from a copyleft section must be copylefted. Linux distribution is a project developed with the aim of managing a set of software packages based on the Linux operating system and facilitating the installation of a Linux operating system. Linux distributions are developed by individuals, teams, volunteer organizations and commercial entities. Linux distributions have software packages specifically designed for system installation and configuration.

The GNU GPL is a free software license in copyleft form, and is used by the Linux kernel and components of the GNU project. Some of the advantages of Linux, include, being free, complete and powerful, supported by many communities around the world in terms of documentation and use of troubleshooting and fixing errors, more resistant to viruses, compatible with various computer processors, as for some disadvantages such as, less popular, dependency application packages that must be downloaded manually. and detection of unsupported hardware [10] [13].

Based on some of the descriptions above, the author is interested in developing the Linux Luxpati distribution based on Ubuntu as a support for human work processes in various fields of expertise such

as offices and government institutions, as for several solutions in developing the Linux operating system so that it can be applied easily and is able to provide various conveniences for its users, In addition, the use of the Linux operating system is also expected to meet the need for a computer network system, adding a new variant within the scope of computer networks, namely an Iptables configuration in a Linux operating system, and most importantly this operating system is able to make it easier for users to filter ports. and reduce the level of risk of destruction or theft of files or information and protect computer applications that are being used [6].

2. RESEARCH METHOD

In the process of this research the researcher tries to use the experimental method, then integrates it with learning from the results of the planned intervention after making a detailed diagnosis of the object of the problem, while the experimental method is a research used to find the effect of certain treatments on their effects under controlled conditions, as for the diagram The flow in this experiment includes:

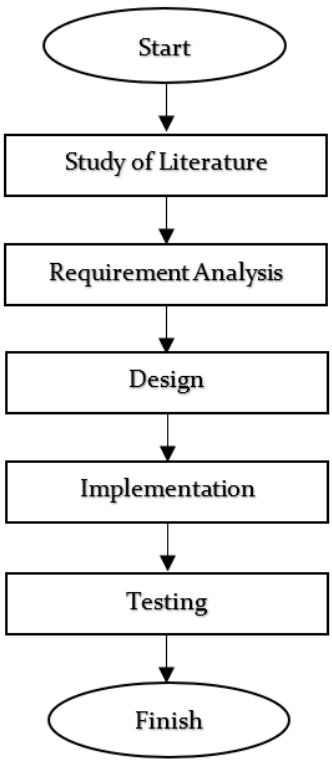

Figure 1. Research flowchart

3. RESULTS AND DISCUSSIONS

3.1. Login Security Using Ubuntu Linux Operating System

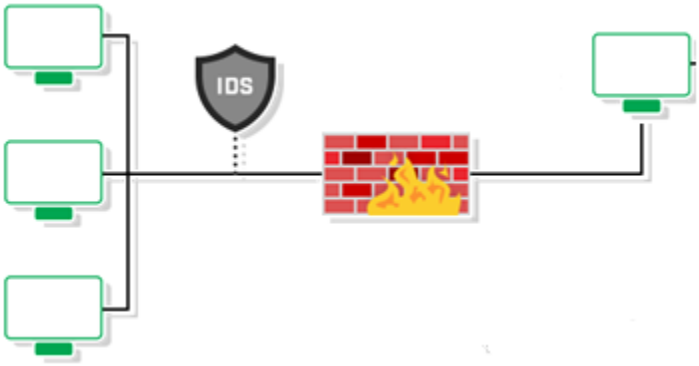

Figure 2. Server network topology designed

In the topology image above, it is known that the internet source comes from a modem that is routed to an FTP Server server with an FTP Server IP of 192.168.100.1 and a Proxy Server with a Manual Proxy IP of 192.168.100.1 and port 3128. Then the client is given a DHCP-Server IP from the Linux routing server. Ubuntu so that the IP Address is 192.168.100.2-192.168.100.254. To access the internet client must fill in the proxy ip and port in the Mozilla Firefox browser and input the proxy username and password.

Table 1. System Analysis

Applications Used (platform Windows)	Application Package Alternative Options (Debian GNU/Linux)
Borland C++	Geany
Borland C++	Geany
MS Office Word, MS Office PowerPoint, MS Office	OpenOffice Word, OpenOffice Presentation, OpenOffice
Excel, MS Access,	Spreadsheet,
MS Visio	Kivio
Borland C++	Geany
EWB (Electronics Workbench)	Dia
JRE, Textpad, Netbeans	Netbeans, Geany
JRE, Textpad, Netbeans	Netbeans, Geany
Apache, Wamp, MySQL	Apache2
Borland C++ Builder	dhcp, ssh, ftp, bind9
Turbo Prolog	Apache2, phpmyadmin, Quanta
Apache, Wamp, MySQL, phpmyadmin, Macromedia Dreamweaver	Borland C++

The points that become important references in this Ubuntu remastering include, the resulting Linux operating system is in the form of a LiveCD, the Linux distribution used is based on Ubuntu, this research refers to the use of Linux Desktop, modifications in the form of enhancements and highlighting of the characters of the remastered distribution, the existence of file system support, hardware and features, and a user-friendly interface [3] [8]

3.2. Configuring IP Address on Ubuntu Server

In this study, the author uses a static internet configuration. And the step for configuring the IP Address is to edit the interfaces file which is located in "etc/network/interfaces" to edit the file, type the nano command. etc/networks/interfaces.

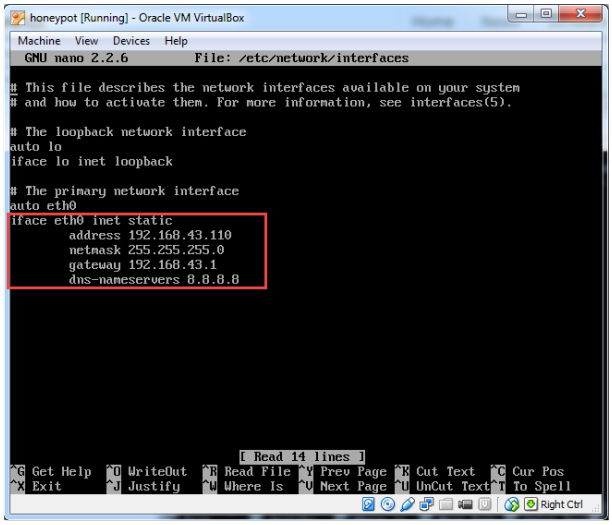

Figure 3. IP Address Configuration Display.

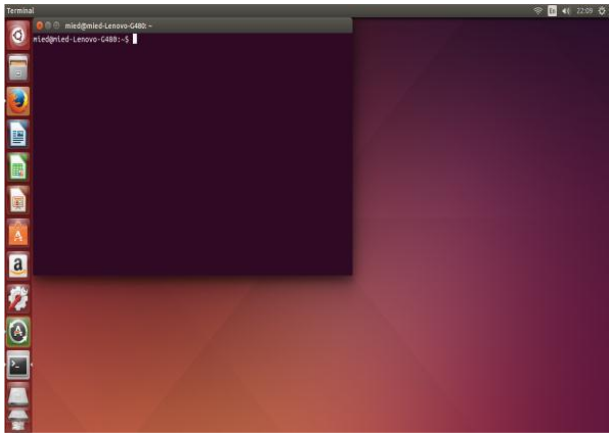

Figure 4. Terminal display on Linux Ubuntu

Before configuring certain settings, you must first determine what the default behavior of the three chains is. In other words, it must determine what iptables should do if a connection does not match the existing rules. To find out what settings are in use, run the iptables command. By using the accept setting, you can use this Linux Firewall to reject certain IP addresses or ports, in addition to accepting other connections. If you want to reject all connections and want to specify what connections you want to do manually, then you have to change the default setting from chain to drop. This method can only be useful for servers that have sensitive information, and only the same IP address is used to connect to that server [4] [12]

3.3. Configure Port knocking on Server

To configure port knocking, the author uses the knocd program from Slackbuilds.org. And to install knocd, type the command apt-get install knocd.

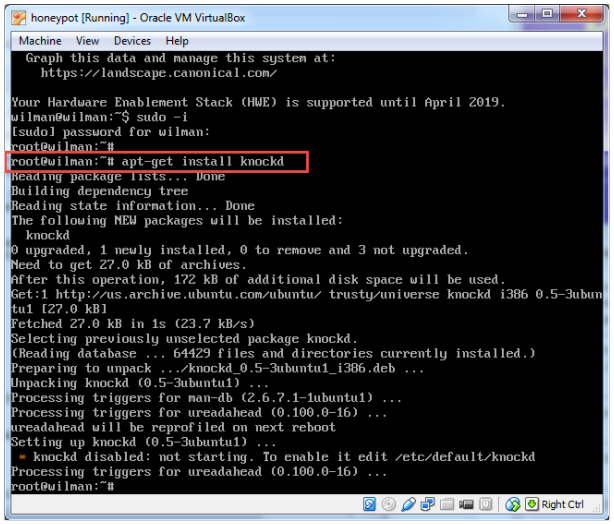

Figure 5. Display Knocd already installed

The process of copying the Ubuntu Linux system begins by copying it into the system before starting the development process. Development begins with creating an ubuntu virtual filesystem mounted from the copied ubuntu.

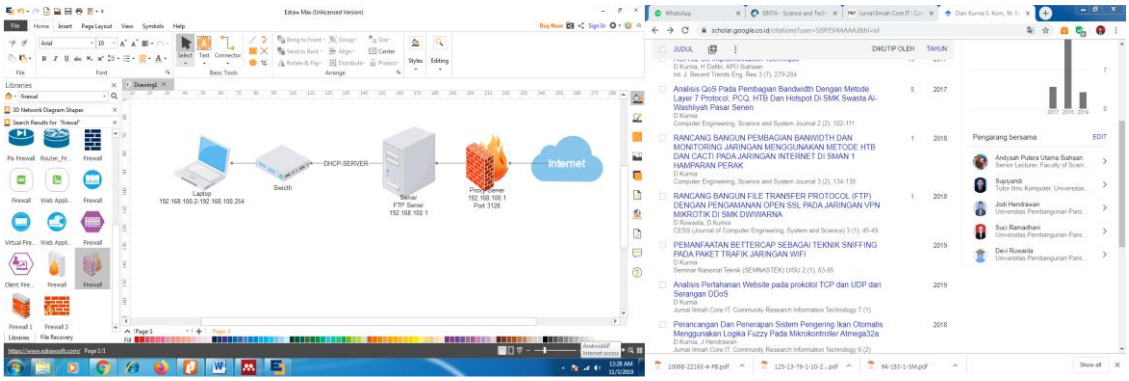

Figure 6. Ubuntu Linux system copy process

3.4. Server Security Testing

In the first test using the putty application, it was found that the instruder was successfully transferred to the shadow server. In this test, the intruder tries to remotely use ports 22.8000, and 9000 by using the IP Address 192.168.43,231.

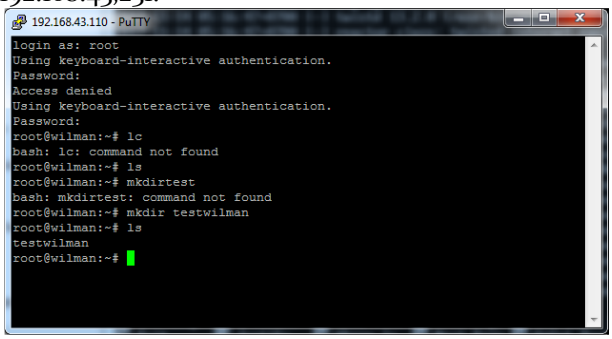

Figure 7. Ubuntu system security

Then in order to accept the connection by default, the system uses the following command, iptables –policy INPUT ACCEPT iptables –policy OUTPUT ACCEPT iptables –policy FORWARD ACCEPT, by using the accept setting, you can use this Linux Firewall to reject certain IP addresses or ports, in addition to receiving other connections. If you want to reject all connections and want to specify what connections you want to do manually, then you have to change the default setting from chain to drop. This method can only be useful for servers that have sensitive information, and only use the same IP address to connect to that server. iptables –policy INPUT DROP iptables –policy OUTPUT DROP iptables –policy FORWARD DROP. The first thing to do is open a terminal on the Ubuntu linux operating system then after opening the terminal, enter root mode with the sudo command, enter the password. scan the ip connected to the server. Then configure which IP will be blocked with the Iptables configuration. Test results This stage is the process of testing the system with several IPs that will be blocked. At this stage the author tries to block all computers in the research location with LAN and Wifi connections.

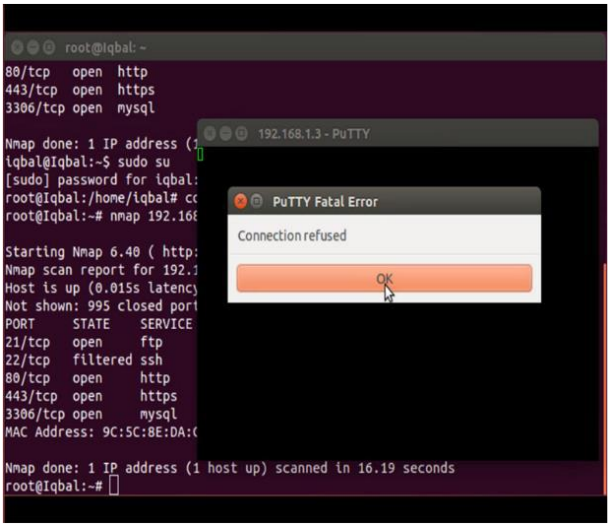

Figure 8. Connection Refused

The picture above is the result of a port scan using nmap on the client and server SSH service status: filtered and the connection to the SSH service will be refused. This shows that the security of IPtables is safe in protecting services by filtering ports.

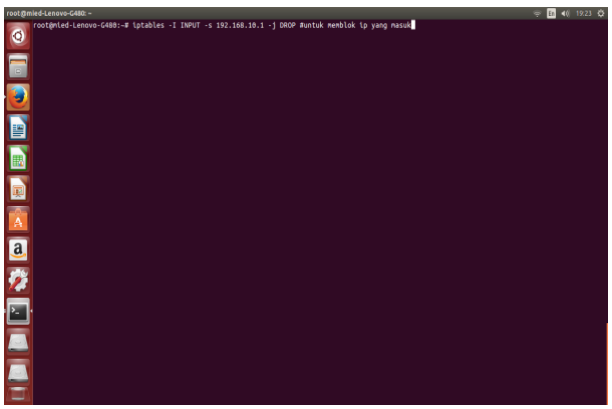

Figure 9. Iptables configuration to block ip

In the picture above, you can see the Iptables configuration to block other computers' IPs, if you want to reconnect then change the configuration from DROP to ACCEPT, then the computer will reconnect.

4. CONCLUSION

After the analysis and implementation in the research The use of Iptables configuration on the Ubuntu Linux operating system can be done on a LAN and Wifi cable connection, as long as all clients are in the same class then the Iptables configuration can block client access to the server and can be done the other way around, namely blocking access server against the client, then from the results of research conducted on several PCs with several network connections, the Iptables configuration can work and does not affect the OS used, because this Iptables configuration uses Linux OS whose client uses Windows OS. Then using Honeypot can prevent someone from trying to scan ports and brute force, then what will appear on the scan application is fake ports. Using IPtbales can block incoming packets so that the port service will not open.

REFERENCES

[1] Arjuni, S. (2010). Perancangan dan Implementasi Proxy server dan Manajemen Bandwidth Menggunakan Linux Ubuntu Server. Studi Kasus di Kantor Manajemen PT. Wisma Bumiputera Bandung). Tugas Akhir. Tidak diterbitkan. Institut Teknologi Bandung: Bandung.

[2] Asmara, L. S. (2013). Pembuatan Distro Linux Linarta (Linux Surakarta) Sebagai Upaya Peningkatan Ketertarikan Masyarakat Surakarta Pada Sistem Operasi Linux (Doctoral dissertation, Universitas Muhammadiyah Surakarta).

[3] Khadafi, S., Pratiwi, Y. D., & Alfianto, E. (2021). KEAMANAN FTP SERVER BERBASISKAN IDS DAN IPS MENGGUNAKAN SISTEM OPERASI LINUX UBUNTU. Network Engineering Research Operation, 6(1), 11-24.

[4] Majid, A. (2021). KONEKSI INTERNET DENGAN MODEM HANDPHONE PADA SISTEM OPERASI LINUX UBUNTU 9.04 (Studi Kasus Pada Aga Prima Computer). JURNAL ILMIAH FAKULTAS ILMU TERAPAN, 1(1), 10-22.

[5] Mangunkusumo, I. E., Lumenta, A. S., & Wowor, H. (2013). Analisa dan Perancangan Keamanan Mail Server Zimbra pada Sistem Operasi Ubuntu 8.04. Jurnal Teknik Elektro dan Komputer, 2(2).

[6] Marzuki, I. (2017). Perancangan dan Implementasi Sistem Keamanan Jaringan Komputer Menggunakan Metode Port Knocking Pada Sistem Operasi Linux. Jurnal Teknologi Informasi Indonesia (JTII), 2(2), 18-24.

[7] MOTONG, Y. (2015). REMASTER DISTRO LINUX UBUNTU 10.04 LTS MENGGUNAKAN REMASTERSYS (Doctoral dissertation, University of Muhammadiyah Malang).

[8] Mulyana, I., & Mukiman, K. (2020). APLIKASI KAZAM SEBAGAI MEDIA PEMBELAJARAN BEBASIS LINUX UBUNTU. JOURNAL INFORMATICS, SCIENCE & TECHNOLOGY, 10(2), 46-51.

[9] Mulyanto, E. (2021). Membangun jaringan internet Wi-Fi menggunakan sistem operasi linux ubuntu 8.04 LTS di SMK PGRI 3 Malang. SKRIPSI Mahasiswa UM.

[10] Novianto, Y. (2017). ANALISA PENGGUNAAN PROGRAM APLIKASI PADA SISTEM OPERASI WINDOWS XP DAN LINUX UBUNTU DITINJAU DARI KEBUTUHAN PEMBELAJARAN MAHASISWA. Jurnal Processor, 8(1).

[11] Nugroho, A., & Handrianto, Y. (2016). File Sharing Server menggunakan Samba Server dan Linux Ubuntu 12.04 Server. Paradigma-Jurnal Komputer dan Informatika, 18(2), 11-17.

[12] Widianto, E. D., Hakim, M. A., Insani, A. A., Khoirunnisa, Z. D., & Baharsyah, Y. R. (2021). PEMBUATAN SISTEM INFORMASI DATA PEGAWAI MENGGUNAKAN KERANGKA KERJA LARAVEL PADA UBUNTU SERVER. Jurnal Pasopati: Pengabdian Masyarakat dan Inovasi Pengembangan Teknologi, 3(3).

[13] Zabar, A. A., & Novianto, F. (2015). Keamanan Http Dan Https Berbasis Web Menggunakan Sistem Operasi Kali Linux. Komputa: Jurnal Ilmiah Komputer dan Informatika, 4(2), 69-74.