# ANALYZE THE LINUX PERFORMANCE IN NETWORK MANAGEMENT

**Dr Mohammad Salim Hamidi**[1],
**Sikandar zulqarnin**[2,]
**Wahdatullah Sharafat** [3],
**Mohammad Ilyasl**[4]

## ABSTRACT

*Computational models for experiments in high-energy physics are increasingly globally distributed and grid-based, both for technical reasons (e.g. proximity of computing and data resources and demand) and strategic reasons (e.g. investment). To support such computing models, network and end systems, computing and storage face unprecedented challenges. One of the biggest challenges is to reliably and efficiently transfer scientific data sets – now in the range of many petabytes (1015 bytes) and expected to grow to Exabyte's within a decade – between devices and computing centers around the world. Both the network and the end systems should be able to provide capabilities to support broadband continuous data transmission with end tones. Recent trends in technology show that although the raw data rates used in networks are increasing rapidly, the pace of development of microprocessor technology has slowed. Therefore, the processing overhead of network protocols has skyrocketed compared to the time spent transmitting packets, resulting in reduced throughput for network applications. Increasingly, the network end system, rather than the network, is responsible for the degraded performance of network applications. In this paper, the process of receiving Linux packets from the NIC to the application is studied. We develop a mathematical model to characterize the process of receiving packets in Linux. The key factors that affect the network performance of Linux systems are analyzed. 2006 Elsevier B.V. All rights reserved. The main goal of my work is to find out the use of Linux in network management. Find out the Linux tools and functionality used for management. Know the best Linux distribution for network administration. Secondary data collection methodology is used in this post, I collected data from books, articles and valuable sources. As a result, we have come to the conclusion that Linux, like other commercial operating systems, is not secure out of the box. We have recommended some things that can be done to make Linux more secure.*

**Keywords:** Linux, Management, OS (Operating system), Open source, performance

## I. Introduction

Since its birth in 1991, Linux has become one of the most popular operating systems in the world. Students love it for the price and flexibility of open source. Network administrators like it because it can communicate with many other operating systems and runs on virtually any processor. Internet Service Providers (ISPs) like it because of the native Internet support it provides. Despite all of Linux's strengths, many argue that Linux is insecure due to its open source nature. Some believe that open source code makes it easier for attackers to find and exploit bugs in the operating system. This article will cover Linux as an open source operating system. We will look at the types of attacks that are used to gain access to a Linux network. We will also see how secure Linux is compared to other commercial operating systems. We conclude this document with some recommendations on what can be done to make Linux more secure.

## II. Literature review

According to Matthew R. Yaswinski, Md Minhaz Chowdhury & Mike Jochen inux is the kernel on which various operating systems run. This kernel is open-source, which means that anyone can use and modify it. A large number of operating systems, known as distributions (or distros), run on this kernel.

According to Ali Mohammed Sachin himself and Majeed Mohameed, to prevent attacks, we need to improve the network security mechanism of the operating system.

[1,2,3,4.] *Jehan University*

Linux is the best choice for its open source and secure environment. According to Sri Krishna Arts and Science College & TamilnaduIt's, it is better to upgrade to the latest version of Linux to prevent attackers from exploiting the vulnerability. By Matthew R. Yaswinski, Md Minhaz Chowdhury & Mike Jochen This operating system is often considered more secure than Windows or Mac OS X, but that doesn't mean there are no security concerns when running it. Attackers can crack simple passwords over the network, vulnerabilities can be exploited if firewalls don't close enough ports, and malware can be downloaded and run on Linux.

## III. Objectives

1. To find out the performance of linux in network management

2. To find out the Linux monitoring tools and functions that are used in network management.

3. To know which Linux distribution is good for network management.

## IV. Range

In this topic we will discuss about Linux operating system and why Linux OS is used in network management.

## V. Research methodology

### 1. Linux OS:

Linux OS is an open source operating system that is used on both the client side and the server side.

### 1.1 Features of Linux

Some of the features of Linux are as follows.

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

- **Stability:** If a new program or software is installed in Linux, it does not need to be restarted regularly. It thus maintains the performance level of the system.

- **Performance:** It does not reduce the performance level of the system, even if it serves a large number of users at the same time.

- **Network friendliness**: Linux is a user friendly operating system when it comes to networking features like; it can be easily configured as a server system or a client system depending on the requirements in the network.

- **Security:** The Linux operating system is equipped with security features as it provides a file access authorization mechanism that prevents unauthorized users from accessing files.

Networking for Linux was developed to support remote login for large networks. Linux machines are not expensive and Linux has few hardware requirements. it can run on different types of hardware. Linux also supports different types of servers such as Apache and SSH server server to run on it. Linux is one of the leading server operating systems, with more than 90% of supercomputers currently running some variant of Linux. Linux is used in networking 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 system management tools.

### 1.2 Linux Security

it's no secret that the operating system you choose is a key factor in your online security. After all, your operating system is the most critical software running on your computer—it manages its memory and processes, as well as all of its software and hardware. The general consensus among experts is that Linux is a highly secure operating system - arguably the most secure OS by design. This article will explore the key factors that contribute to robust Linux security and evaluate the level of protection against vulnerabilities and attacks that Linux offers to administrators and users. Linux security has features such as authentication, which identifies users, and log management, which records network activity. Linux is a much safer option. Here are ways Linux can improve security.

- **Linux is open source:** which means anyone can examine the code to find security vulnerabilities. It allows faster patching of all found vulnerabilities.

- **Linux uses a different architecture:** than Windows, which makes it harder for viruses and other malware to infect the system.

- **Security tools:** There are a number of security tools available for Linux that can further strengthen system security.

- **Privilege:** Linux has clearly defined permissions at several levels, thereby limiting access. For example, there are "root" level access rights (which you can link to "administrator" in any operating system) that are not granted to any regular user. Users can only access lower-level accounts with limited access. When a Linux system is compromised, a virus or malware cannot gain root access to damage the entire system.

• **System Event Log:** A log file is kept that records file accesses and system accesses in Linux. If any user tries to access the secure system file, they can be checked by the system administrator. Log files contain messages about the system, kernel, services, and applications running on it. Different types of log files are available

Overall, Linux is a much more secure option than Windows for both individuals and businesses. The open source nature of Linux allows security vulnerabilities to be patched more quickly, and the different architecture makes it harder for malware to infect the system. Additionally, Linux systems are typically configured to be more secure than Windows systems. Finally, a variety of security tools are available for Linux that can further enhance system security.

**2. Basic Linux tools for network and security**

• **Aircrack-ng for WI-FI Security:** Aircrack-ng is a set of tools for testing the security of wireless networks and Wi-Fi protocols. Security professionals use this wireless scanner for network management, hacking and penetration testing.

**• Burp Suite Pro focuses on web application security:**

It is a web application testing suite used to evaluate the security of websites online. Burp Suite acts as a local proxy solution that allows security professionals to decrypt, trace, manipulate and replay web requests (HTTP/websockets) and responses between a web server and a browser.

**• Impacket for pen testing network protocols:**

This collection of tools is essential for testing network protocols and services with a pen. Developed by the company

Secure Auth, Impacket works as a collection of Python classes for working with network protocols. Impacket focuses on providing low-level access to packets, security professionals can create packets from scratch as well as analyze from raw data.

**• Metasploit: Super exploit detection tool:**

Security professionals consider it an exploitation framework used for general penetration testing and vulnerability assessment a "super tool" that contains working versions of almost all known exploits in existence.

**• Responder simulates attacks on DNS systems:**

It is used by penetration testers to simulate an attack aimed at stealing credentials and other data during the name resolution process when no record is found by the DNS server.

**3. Network monitoring tools:**

Network monitoring refers to the practice of monitoring traffic on a computer network using various network management tools. The availability and performance of network services and hosts are ensured by network monitoring tools or systems.

Linux is one of the best platforms for learning network troubleshooting techniques. It offers a number of built-in command-line tools for network problem detection and diagnosis. In addition, there are several open-source network monitoring tools with both graphical and command-line interfaces that help visualize and analyze network traffic.

Below are some of the monitoring tools we used in implementing our thesis:

- **Nmap**
- **Wiershark**
- **IP traf**

**3.1 Nmap:** stands for Network mapper, Nmap is an open source tool widely used in network exploration or security auditing. It is also used as a hacking tool to gather information about the target computer. It is primarily used by network administrators to perform tasks such as:

- Network inventory management.
- Manage service upgrade tasks.

**3.2 wireshark host or service startup time monitoring:**

Wireshark is a free and open source network packet analyzer that was originally named Ethereal. The main task of this network packet analyzer is to capture network packets and display these packet data in detail. It can be used by many people in different situations. Some examples of situations where wireshark is useful are:

- To troubleshoot the network used by network administrators.

- To investigate security issues – used by network security engineers.

• To implement the debug protocol - used by developers.

• For analysis and education 3.3 IP traffic: In Wire shark, we get a lot of detailed information about the traffic passing through the network, and a lot of time can be lost to understand every single point of information. Therefore, to make things more precise, we used IPtraf. It is a reliable console-based network monitoring tool for Linux. It collects the following information:

• Number of TCP connection packets and bytes.

• Interface statistics and activity indicators.

• TCP/UDP traffic failures.

• The number of packets and bytes of the LAN station.

## 4. Linux Networks

Linux is used to manage networks in critical environments and the system/network administrators who work in them the environment must have a much deeper knowledge than ever before. Advanced Linux Networking picks up where conventional Linux networking helps experienced Linux system and network administrators do more and solve more problems than they can with any other book. Its breadth and depth make it an exceptional one-volume reference for any Linux professional [9]. Linux networks are structured into four sections, each essential to a 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 backup, iptables firewalls , and VPNs. An extensive section on Internet services shows how to handle virtual domains and secure sites; analyze Apache log files; and operate FTP servers; and includes detailed coverage of SMTP-based email systems. Among the topics that are covered in extraordinary depth: Kerberos configuration; running time servers, font servers and chroot jails; and using Samba's scripting capabilities to burn CDs and create PDFs. For anyone experienced with Linux systems or applications and embedded systems. b. Stability: If a new program or software is installed in the Linux system, it does not need to be restarted regularly. It thus maintains the performance level of the system.

**Performance:** It does not reduce the performance level of the system, although Serves a large number of users simultaneously.

**Network friendliness:** Linux is a user friendly operating system when it comes to networking features like; it can be easily configured as a server system or a client system depending on the requirements in the network. E. Security: The Linux operating system is equipped with security features as it provides a file access authorization mechanism that prevents unauthorized users from accessing files.

## 5. Overview of Network Servers

Servers commonly found on the network are described in the following sections. • Apache web server: Apache web server is one of the most widely used web servers in the world because it has multi-threaded concepts. Both HTTP and HTTPS services are available on Apache. The HTTP protocol is designed to provide communication between clients and servers. By default, it runs on port number 80. HTTP is used to establish normal connections. By default, HTTPS runs on port number 443 and establishes a secure connection. When establishing an HTTPS connection, the server responds to the client with a list of encryption techniques. In return, the client prefers a better connection mechanism. Therefore, server and client authentication is verified by exchanging certificates and encrypted information to ensure that they both use the same keys. HTTPS is most widely used on login pages of banks and corporate companies.

**• OpenSSL (Open Secured Socket Layer):** SSL is an open source toolkit implemented by two layered protocols. They are: SSL v2/v3 and Transport Layer Protocol. It uses a strong cryptographic library. The current version of openSSL is 1.0.0e, which includes bugs and security fixes.

OpenSSL supports many cryptographic algorithms and protocols. SSL provides better security for web services. OpenSSL records the confidentiality and integrity of SSL connections and also provides better security features for higher layer protocols. For HTTP, it provides a transport service for web client/server interaction that can work over SSL [19]. There are also three other higher level protocols that play a key role in managing the SSL exchange, they are:

• Handshake protocols.

• Change the encryption protocol.

• Warning logs [20].

• **Mail server:** Send mail server is one of the best mail servers used in most real world environments. By default, the server can only send send emails; cannot receive any mail. It is very important that incoming mail is properly scanned and inspected. Send Mail supports a variety of mail transfers and delivery methods, such as SMTP, which is used to transmit electronic mail over the Internet.

• **OpenSSH:** is a free version of SSH and provides encrypted communication over the Internet. Tools like telnet and rsh are insecure because they transmit passwords in plain text. OpenSSH provides a better security service when transferring files. To connect clients, SSHD (the SSH server component) listens continuously from any client tools. OpenSSH uses different types of authentication methods such as common passwords and public keys [21]. In general, telnet, rsh, and rlog are not secure remote applications because they are susceptible to eavesdropping. For this reason, most companies will prefer SSH for remote login.

• **DNS Server:** DNS stands for Domain Name System and is a hierarchical distributed database. Converts domain names to IP addresses and vice versa. Because domain names are alphabetical, they are easier to remember than IP addresses, which contain numbers. However, all public or private networks are based on IP addresses, not domain names. Every time we use a domain name, it is the DNS server that translates the name to the corresponding IP address. For example, the domain name www.example.com can be translated to 192.168.40.132. Each network contains one or more DNS servers. If one server fails to translate a particular domain name, another server will take care of it, and so on. In short, DNS serves as a telephone directory for the Internet by mapping a directory of domain names to IP addresses and vice versa. Therefore, DNS server security is an important part of network security.

**Linux as an open source operating system:** The GNU Project (GNU is a recursive acronym for ``GNU's Not Unix") was started in 1984 by Richard Stallman, a researcher at MIT's Artificial Intelligence Labs, in response to the (then) new practice of keeping source code secrecy and software licensing enforcement [8]. Stallman saw downloading the source code as a restriction on the programmer's freedom to modify and improve the software [8]. He also saw that licensing restrictions on copying conflicted with his philosophy of being a good neighbor and sharing ideas. Stallman's goal was to recreate a complete operating environment without such restrictions, with all the tools and utilities a computer user would ever need [8]. He decided to model this new operating environment after the Unix operating system (OS). Stallman realized that if he just made his code available to everyone, it could easily be copied by someone else who could modify it, authorize it, and not make the new code available to everyone. Because of this, Stallman decided to copyright his material with the restriction that if any code was copied, the new modified code had to be made available to everyone. The condition is that anyone who modifies the code for later redistribution must make their source code public under the same conditions [8]. This copyright became known as the GNU General Public License. Stallman did not manage to create a completely new operating environment, but he created many peripheral utilities. In 1991, Finnish computer science student Linus Torvalds wrote the first version of the Unix kernel for his own use and posted the code on the Internet asking other programmers to help him build it into a working system [8]. He incorporated the work Stallman had created and called this new operating system Linux. Torvalds released Linux under the GNU General Public License as did the GNU project.

**Network Management System:** Like telecommunication networks increasingly complex, telecommunications network service providers require increasingly capable network management systems. Network management systems face significant barriers to adoption by network service providers. One such obstacle is that network management systems must manage networks composed of network devices that conform to different interface standards. An example of such an interface standard is the well-known CMIP (Common Management Interface Protocol). A telecommunications network management system must not only manage the various elements of the network, but also manage network growth and/or modifications. Conventional telecommunications network management systems do not provide a mechanism for representing the physical network in an efficient way to facilitate network design and maintenance. Nor do they adequately represent the evolution of the physical network to the new configuration. 1.2 Zero Price Tag: Other commercial operating systems require the purchase of a new license for each computer on which it is installed. Because of the GNU General Public License, Linux does not have the same restrictions. This can significantly reduce costs for a company with multiple computers. We also have to remember that even though Linux is free, it wouldn't have any benefits if it didn't do the job.

**Flexibility:** If you were using an open source operating system and needed something special for your company, you would have to ask the manufacturer to make the change for you. Most commercial OS manufacturers are not interested in customizing an OS for each company. Even if they were, it would be worth it a lot of money. With Linux, you have source code that you can freely adapt to your needs.

**Stability:** Unix is known for its stability. This is one of the reasons Linux was modeled after it. Linux has the benefit of a quarter century of Unix experience to draw upon. The open source model of Linux seems to ensure that bugs are detected and fixed in a timely manner [8]. Compliance: Due to the GNU General Public License, Linux cannot have proprietary features. Thus, the license ensures that the only changes to the system that persist are those accepted by the "community" [8]. The community has no interest in creating proprietary standards and protocols, so the OS will naturally blend in with industry standards [8]. Linux is a POSIX (Standards Defining Unix) compliant operating system and supports ANSI, ISO, IETF and W3C standards.

**Hardware support:** Linux will run on virtually any known processor, whether RISC or CISC, 32-bit or 64-bit. The most common processor for Linux is of course the Intel x86 family, but it also runs on 68k Motorola, IBM/Apple/Motorola PowerPC, Compaq/Digital's Alpha, MIPS chips, Sun SPARC and UltraSparc, and Intel's Strong ARM [8] . Intel recognized the popularity of Linux and made it their goal to make Linux run fastest on their chips. Intel is promoting its Uniform Driver Interface (UDI) as a common Unix approach to device drivers and is trying to get the Linux community to help write drivers [8]. Another strength of Linux is that Linux has the ability to run on older computers at less cost Memory and disk capacity than other operating systems. The only downside is that not all peripherals and cards are supported by Linux, but that will change as Linux grows in popularity.

**Native Internet Support:** Open Source Apache, the world's most popular web server, runs natively on Linux. Add-on modules such as mod_perl allow Perl CGI scripts to be interpreted and executed in the Apache memory space. The mod_jserv module allows Apache to use Java servlets [8]. The mod_php module allows Apache to run scripts embedded in HTML in a Perl-like Hypertext Pre-Processor language called PHP, a program that works exactly analogously to Microsoft's Active Server Pages [8]. Linux also supports firewalls like ipchains. These things and more have made Linux a very popular server OS among Internet Service Providers (ISPs). Linux is an excellent standard platform for web applications. You can use it to create a complete, secure Internet site, including a router, firewall, proxy, web server, mail server, database server, and directory server [8].

**Types of Attacks:** In order to evaluate the security of Linux, we need to look at the attacks that are used against it. We do not intend to examine every attack that has been used against Linux, but we will discuss some of the more common ones. For a complete list of all security flaws, visit http://www.linuxsecurity.com. Attackers have several ways to attack a server. The tools to carry out these attacks are readily available on the Internet to anyone who cares to find them. These attacks can range from a simple test to find out what version of the operating system you have running to give you complete control over your system. Attacks can come from an external source, such as a hacker on the Internet, or from an internal source, such as an employee at a workstation. Some of the different types of attacks an attacker can use will be described in more detail below.

**Scanning:** The first thing an attacker will do is figure out who they can attack. They can't attack you if they don't even know you exist. Attackers typically use what is called War Dialing to find networks to attack. Once they know you exist, they can use other tools to find out what type and version of operating system you're running on your system. An attacker can use what is called a packet sniffer. Sniffer listens on the ethernet port for things like passed, logged in, etc. When these things are detected, an attacker can obtain passwords that allow them to access the network. Packet sniffers are deployed on an already compromised port or can be done internally from a laptop or other computer. Using sash or other encrypted password methods will defeat this attack. Things like APOP for POP accounts also prevent this attack. (Normal POP logins are very vulnerable to this, as is anything that sends plaintext passwords over the network.) [10]

**Data analysis and discussion:**

Linux is an open source operating system that has gained a lot of popularity. More and more people are using it for various tasks. However, given its open source nature, how secure is Linux? And are these people just going to attack? These are viable questions that every Linux user should be aware of. Therefore, this report will explore the overall security of Linux as a server and also provide some possible solutions to increase security.

## Conclusion

Linux is an open source operating system that has gained a lot of popularity. More and more people are using it for various tasks. However, given its open source nature, how secure is Linux? And are these people just going to attack? These are viable questions that every Linux user should be aware of. Therefore, this report will explore the overall security of Linux as a server and also provide some possible solutions to increase security. Since its birth in 1991, Linux has become one of the most popular operating systems in the world. Students love it for the price and flexibility of open source. Network administrators like it because it can communicate with many other operating systems and runs on virtually any processor. Internet Service Providers (ISPs) like it because of the native Internet support it provides. Despite all of Linux's strengths, many argue that Linux is insecure due to its open source nature. Some believe that open source code makes it easier for attackers to find and exploit bugs in the operating system. This article will cover Linux as an open source operating system. We will look at the types of attacks that are used to gain access to a Linux network. We will also see how secure Linux is compared to other commercial operating systems. We conclude this document with some recommendations on what can be done to make Linux more secure. In this issue, we will discuss the security rating of the Linux operating system.

In this article, we evaluated the Linux operating system. We looked at how Linux was created and it is an open source environment. We have looked at many of the strengths that make Linux popular today. Several attacks that can be used to gain access to a Linux network have been discussed. Using information obtained from Security Focus Online, we Compared the security of Linux with other commercial operating systems. We have come to the conclusion that Linux, like other commercial operating systems, is not secure out of the box. We have recommended some things that can be done to make Linux more secure.

## REFERENCE

[1] http://www.linux-box.org/http://www.itworld.com/nl/lnx_se/05072002

[2] http://www.itworld.com/nl/lnx_sec/05142002

[3] http://www.itworld.com/nl/lnx_sec/04302002

[4] http://www.itworld.com/nl/lnx_sec/12182001