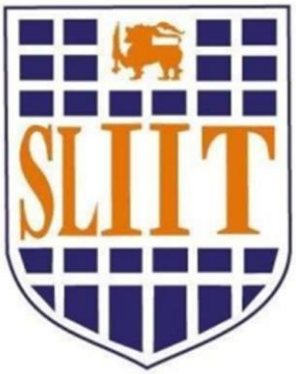
Sri Lanka Institute of Information Technology



Secure operating system IE2032
Year 2, Semester 1- 2024

B.Sc. (Hons) Degree in IT (sp. cyber security)

	Student registration Number	Student Name
01.	IT23390546	SEMAL K.M
02.	IT23209534	A.A.I NETHMIKA
03.	IT23325296	C.L.D JAYAWARDHANA

Group details

Group ID	SOS_38
Research paper	Linux Security: A Survey
Campus/Center	Malabe

Workload matrix

Student ID	Student Name	Topics
IT23390546	SEMAL K.M	• Abstract • Introduction • Conclusion • Methodology
IT23209534	A.A.I NETHMIKA	• Explanation of the problem being addressed and why it is important • Solution or approach proposed by the authors • References
IT23325296	C.L.D JAYAWARDHANA	• Terms of Reference • Acknowledgement • Critical Evaluation of the paper I. Strengths II. Weaknesses III. Areas for Further Research

Table of Contents

1. Terms of Reference

The report created on topic "Linux Security: A Survey"
This report is submitted to the Sri Lankan Institute of Information Technology for the completion of the IE2032 module in partial fulfillment of the BSc. (Hons) in Information Technology Specializing in Cyber Security.

Security in Operating Systems:
Linux Security A Survey

2. Acknowledgement

We recognize the efforts of all SOS module lecturers who guided us this semester towards the success of this report's completion. We will equally appreciate our team members for their efforts in taming this initiative into a fruitful educational one. Lastly, we would wish to thank all those who assisted us in the successful completion of our task with regard to the nuances inherent in OS security.

3. Abstract

Linux, despite its reputation for being more secure than Windows or Mac OS X, still faces various security challenges across its diverse applications, from personal computers to business servers handling sensitive data. Common threats include password cracking, exploitation of firewall vulnerabilities, malware infections, and unauthorized access to sensitive Despite its reputation for being more secure than Windows or Mac OS X, Linux information due to improper file permissions. However, most of these risks can be mitigated by proactive measures: keeping systems updated, maintaining robust firewalls, employing antivirus software, using complex passwords, and implementing strong file permissions. The text indicates that the paper will delve into detailed methods for safeguarding Linux systems against both external and internal security threats, emphasizing the importance of a comprehensive approach to Linux security.

4. Methodology

his essay analyzes in detail the mentioned above article “A Review of Android and iOS Operating System Security” as published on the IEEE Xplore database. The aim is to study the self-defense aspects of mobile operating systems, Android and iOS the importance of these in the general security of the devices.

Desk study approach was utilized, whereby the writer’s collected materials from IOS study libraries. IEEE library was sort after in order to have access to up to date and right studies. This included reviewing literature on various security features including virtual machines, cryptography, address space layout randomization and anti-malware systems.

As a result, we came across common security threats such as hacking and malware extending its boundaries. Hence this interdisciplinary approach gave us an opportunity to relate practical situations such as data leaks to systemic problems posed by computer security.

In the end it has also enhanced the overall understanding of how mobile devices especially Android and iOS are secured.

5. Introduction

This document explores the growing adoption of Linux and the critical need for robust security measures in Linux systems. It discusses various security threats and countermeasures, including firewall configuration, file permission management, password security, and virus scanning. The paper emphasizes the importance of these practices for both personal computers and business servers, particularly those hosting sensitive data. While highlighting Linux's cost-effectiveness and versatility, the document stresses that out-of-the-box Linux distributions require additional security enhancements. It touches on the risks associated with running Windows software on Linux through compatibility layers like Wine and the necessity of user vigilance on potentially insecure networks. The paper concludes that implementing these security practices, though not overly complex, is crucial for protecting systems from infections and unauthorized access, ultimately saving time and money by preventing data breaches and system compromises.

6. Explanation of the problem being addressed and why it is important

The paper addresses the security vulnerabilities in Linux operating systems. Even though it is considered more secure than other Operating Systems like Windows, Linux is not completely immune to security threats. Since it is used by a very large number of users for both personal and official purposes and contains sensitive data, it is immune to issues such as network-based password cracking, exploitation of open ports, malware infections and unauthorized physical access.

Since Linux is widely used for servers used for business operations and personal computers it is very important and required to understand this problem. Since it can damage the reputation and finance of the business as well as can leak personal information of the personal clients that is stored in servers, it is critical to secure these data.

7. Solution or approach proposed by the authors

However, there are plenty of solutions to prevent Linux operating systems from vulnerabilities. Using Repositories is the safest way to download and install software. Users should refrain from installing software from the internet as much as possible. But if the user must install software from the internet, it is better to check if it has a virus through an antivirus program such as CalmAV.

And, users be cautious when they are using compatibility layers like Wine to run windows software in Linux because some malware can successfully run on Linux system through these layers. Keeping software up to date is also important to ensure that the installed software has the latest security patches so exploits are abused.

In order to prevent unauthorized access to computers on the same network firewalls can be set up. Using tools such as iptables package rules can be set to prevent these attacks and unauthorized access. Creating a strong and unique password that in not easy to guess using password crackers for users and root accounts and setting different file access permissions to different users is also helps to prevent unauthorized access. Users can even use password crackers to check the strength of the passwords.

8. Critical Evaluation of The Paper

➢ Strengths:

1. General Coverage of Security Issues: In this paper, security issues concerning Linux are covered, from user-level password management to system-level firewalls and malware concerns. It is thus expected to help in identifying an all-rounded understanding of the general threats to Linux systems.

2. Relevance to Real-World Concerns: This paper discusses some concrete risks related to running Windows software on Linux by means of compatibility layers such as Wine. In fact, this is a common problem when switching from Windows to Linux.
This applies to business and personal users because the paper addresses Linux security in terms of both personal and enterprise use. This actually broadens the scope of applicability, since it will be useful for all kinds of audiences, ranging from mere individual users to companies that handle Linux servers.

3. Best Practice: Focusing attention on the use of repositories with respect to the installation of software and on antivirus software such as ClamAV is an unusually well-read approach to security. Trying not to have users download software from third-party vendors is a responsible way of acting.

4. Comprehensive coverage of Linux security practices: It effectively outlines the different ways of securing Linux systems on the repositories, antivirus software, firewall rules, password management, and access permission. It reflects a broad view on major areas in Linux security.

5. Attention to User Behavior: The paper highlights that very critical security issues are related to human factors, such as managing root passwords and understanding how to correctly set permissions. This is because the mistakes of users are often the major cause of a vulnerability in security.

6. Overview: The paper elaborates on general opinions on a broad range of security features that should not go unnoticed by Linux users-from simple firewalls and file permissions to specialized ones concerning the management of passwords. It also illustrates how to secure Linux systems.

➢ Weaknesses:

1. Lack of In-Depth Technical Analysis: While the paper gives a good overall view, the detailed technical analysis for some special attacks or security mechanisms is missing. Advanced security topics, such as encryption, intrusion detection systems, and other security models like SELinux, will not be discussed in-depth.

2. Too Much Emphasis on Basic Security Practices: While basic security best practices such as updating software and setting good passwords are important, the paper would have done better by discussing higher-order best practices of Linux security. For instance, new security frameworks such as AppArmor or SELinux, which are critical in the hardening of Linux systems against complex attacks, are hardly discussed.

3. Discussion of Evolving Threats: No discussion on recently evolved security threats has been made, such as ransomware, phishing attacks, or zero-day exploits. In the face of rapid evolution for cybersecurity threats, such an omission only serves to narrowly curtail the relevance of this paper in dealing with contemporary risks.

4. Too Much Dependence on Antivirus: The suggestion for antivirus software such as ClamAV is quite pragmatic. Generally, though, antivirus tools are less crucial in Linux compared to more systemic security measures like regular updates, secure configurations, or sandboxing. This paper could have shifted the emphasis towards security practices inherent in the operating system rather than porting practices from Windows-based approaches.

5. Shallow Depth in Vulnerability Analysis: Although the paper mentions that Linux systems are very well-positioned to pose some sort of threat, it fails to delve into the specifics of which type of vulnerabilities or in what particular ways such an attack could be perpetrated. What should have been done is deeper analysis with respect to a variety of types of Linux exploits, including, but not limited to, privilege escalation attacks and buffer overflows.

6. Lack of depth for important topics: Paper seems to cover almost all, but all superficially. This perhaps should be witnessed within the malware and Wine section by identifying some research work without substantial details on how the Wine malware can be mitigated or what precise measures the users are supposed to take. In addition, updating of the software could be more technical concerning the automation of updating or compatibility issues with enterprise environments.

➢ Areas for Further Research:

1. Advanced Malware Analysis for Linux: Advanced malware threats have the capability to focus on the "Linux" operating system. Much further research is needed on the malware landscape of threat detection strategies and advanced defense techniques.

2. Comparative Security Analysis: Clear comparisons of security vulnerabilities in Linux with other operating systems like Windows and macOS will make for many useful inferences about unique strengths and weaknesses associated with Linux.

3. Emerging Threats within the Linux Ecosystem: The paper could be brought up to date to explore new and emerging threats in Linux security, including those emanating from IoT devices on Linux, cloud-based threats, and container vulnerabilities in environments running Docker or Kubernetes.

4. Advanced Network Security: Linux systems' protection over networked environments should be given more prominence. Further research may investigate some aspects, like the use of VPNs, the establishment of intrusion detection systems, or the implementation of security policies in cloud environments where Linux is in common usage.

5. Antivirus Tool Comparison: While the paper focuses on ClamAV, a comparison of ClamAV with other antivirus tools, such as Sophos or BitDefender for Linux, would give users an overview of the different tools available.

6. Usable Security Practices: Since most of the Linux users are not security experts, further research may be conducted into more user-friendly utilities and interfaces that would enable non-technical users to make the security practices easier.

7. Comparative Analysis of Security on Different OSs: Also, it could be value-added to compare the security practices carried out on Linux with other operating systems like Windows and macOS. This would include examining how effective similar security measures are across these environments and provide insight into how Linux fares well or does not fare so well in a particular place.

8. Automation of Security Practices: Although the paper has touched on the updating of systems, further research needs to be conducted on automation in regard to security tasks such as updating software, firewalls configurations, and scanning for vulnerabilities. Ansible, Chef, or Puppet can be quite helpful in automated hardening for a Linux system in an enterprise environment.

9. The Impact of Newer Malware on Linux: Greater proliferation and sophistication have given rise to newer types of malware exclusively for Linux systems, cryptojackers, or ransomware. Further studies can be done on how the current security practices in Linux hold against these newer threats and how those can be adapted to mitigate them.

9.Conclusions

This passage emphasizes the importance of securing Linux systems against various attacks through multiple strategies. These include keeping systems updated, maintaining secure firewalls, using antivirus software, creating complex passwords, and setting strong file permissions. The text highlights that these measures are crucial for both personal and business Linux users to prevent data theft and system compromise. It stresses the importance of obtaining software from trusted sources and scanning downloads, particularly given the risk of Windows malware running through Wine on Linux. The passage concludes that implementing these security practices is relatively straightforward and vital for protecting sensitive information. It also suggests future research areas, including detailed analysis of specific malware, their origins, prevention methods, and comparative studies of security measures across different operating systems, underlining that proper security can save both individuals and corporations from data loss and potential financial damages.

10. References

[1] M. Chowdhury and K. Nygard, Machine Learning within a Con Resistant Trust Model, The 33rd International Conference on Computers and their Applications (CATA 2018), March 19-21, 2018, Flamingo Hotel, Las Vegas, Nevada, USA.
[2] M. Chowdhury, K. Nygard, K. Kambhampaty and M. Alruwaythi, Deception in Cyberspace: Performance Focused Con Resistant Trust Algorithm, The 4th Annual Conference on Computational Science & Computational Intelligence, December 2017, Las Vegas, NV, USA.
[3] M. Chowdhury and K. Nygard, An Empirical Study on Con Resistant Trust Algorithm for Cyberspace, the 2017 World Congress in Computer Science, Computer Engineering, & Applied Computing, July 17-20, 2017, Athens, Greece.
[4] M. Chowdhury and K. Nygard, Deception in Cyberspace: An Empirical Study on a Con Man Attack, The 16th Annual IEEE International Conference on Electro Information Technology, May 14-17, 2017, Lincoln, Nebraska, U.S.A.
[5] I. Jahan and S. Sajal, Stock Price Prediction using Recurrent Neural Network Algorithm on Time-Series Data, the Midwest Instruction and Computing Symposium 2018, April 6-7, 2018 Duluth MN, USA.
[6] I. Jahan and S. Sajal, "Prediction on Oscar Winners Based on Twitter Sentiment Analysis Using R, the 2018 SDSU Data Science Symposium, February 11, 2018, Brookings, SD, USA.
[7] R. Gomes, M. Ahsan and A. Denton, Random Forest Classifier in SDN Framework for User-Based Indoor Localization, the 2018 IEEE International Conference on Electro/Information Technology, Rochester, Michigan, USA.
[8] M. Ahsan, R. Gomes and A. Denton, SMOTE Implementation on Phishing Data to Enhance Cybersecurity, the 2018 IEEE International Conference on Electro/Information Technology, Rochester, Michigan, USA.
[9] M. Chowdhury, J. Tang and K. Nygard, An Artificial Immune System Heuristic in a Smart Grid, the 28th International Conference on Computers and Their Applications, 2013, Waikiki, Honolulu, Hawaii, USA.
[10] A. S. Tanenbaum and H. Bos, Modern Operating Systems, Boston: Pearson, 2015.
[11] B. Hatch, J. Lee and G. Kurtz, Hacking Linux Exposed: Linux Security Secrets & Solutions, New York, The McGraw-Hill Companies, 2001, pp. 284-314.
[12] Duncan, Rory and Z. C. Schreuders, Security implications of running windows software on a Linux system using Wine: a malware analysis study, Journal of Computer Virology and Hacking Techniques, 2018, pp. 1-22.
[13] L. Yang, V. Ganapathy and L. Iftode, Enhancing Mobile Malware Detection with Social Collaboration, 2011 IEEE Third International Conference on Privacy, Security, Risk and Trust and

2011 IEEE Third International Conference on Social Computing, New Brunswick, 2011.
[14] Offensive Security, "Kali Linux - Official Documentation," [Online].
Available: https://docs.kali.org/. [Accessed 12 November 2018].
[Accessed 12 November 2018].
[15] R. Russel, M. Boucher, J. Morris, J. Kadlecsik, H. Welte and H. Eychenne, "Man page of IPTABLES," 25 June 2015. [Online].
Available: http://ipset.netfilter.org/iptables.man.html.
[16] J. A. Galindo, D. Benavides and S. Segura, Debian Packages Repositories as Software Product Line Models. Towards Automated Analysis, the 1st International Workshop on Automated Configuration and Tailoring of Applications, September 20, 2010, Antwerp, Belgium.
[17] Allen, Lee, Tedi Heriyanto, and Shakeel Ali. Kali Linux–Assuring security by penetration testing. Packt Publishing Ltd, 2014.
[18] T. Taylor, "Linux security concerns rise as hackers target the OS," TechGenix Ltd., 9 January 2018. [Online].
Available: http://techgenix.com/linux-security-concerns/.
[Accessed 27 November 2018].
[19] D. Barrera, I. Molloy and H. Huang, IDIoT: Securing the Internet of Things like it's 1994, arXiv preprint arXiv:1712.03623 (2017).