IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 11, November 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.524

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311074|

Development of an Ubuntu Hardening Tool with a Graphical User Interface for Enhanced Security

Jayendra Kumar[1], J.Revanth Kumar[2], K.Mukesh[3], R.Manikanth[4]

Department of Computer Science and Engineering, Anurag University, Hyderabad, India[1,2,3,4]

ABSTRACT: The realistic security of Linux production systems is the main topic of this study. It goes over the fundamental security needs for Linux on systems that must pass different audits in an office setting.This document also describes how to identify system vulnerabilities by analyzing configuration files, server files, log files, and computer activities.The system is then secured by swapping out vulnerable properties with secured ones. Examining the signatures of different apps and presenting all the features in a graphical user interface (GUI) format makes application security more user-friendly. Determining the main purpose or job of the Linux server is a crucial first step in safeguarding a Linux system. You ought to be fully aware of everything that is on your machine. If not, it will be impossible for you to comprehend what has to be guarded, making proactive Linux system security ineffective. Examining the default list of software packages that don't adhere to your security policy is therefore crucial. In the event that security updates and patches are provided, you will have fewer packages to maintain and update.

I. INTRODUCTION

"Hardening" is the term for system security. Similar to other operating systems, Linux is susceptible to many malicious attacks due to security weaknesses at the application level. Many tools and methods have been created over time to "harden" Linux systems in an effort to lessen the risk that malfunctioning software poses. The Linux operating system offers a great degree of customisation because to its many options and permissions, but this very feature also makes it difficult to secure effectively. The fact that anyone can write a program for this operating system and that it is an opensource software environment means that there are countless alternative setups. Utilizing these characteristics to build a safe system that satisfies user requirements is the aim.

As technology develops, assaults are becoming more deliberate and targeted, necessitating strong system security, which many businesses have prioritized. A crucial step in protecting the infrastructure is hardening a system, which is the process of reducing a security system's vulnerability—in this case, the operating system—in order to fend off potential threats. One of the most widely used operating systems for laptops and businesses, Ubuntu, has a lot of security features, but because most users are not experts in software security, using layering techniques to increase security can be challenging and time-consuming.

The goal of this project is to create a hardening script for the Ubuntu operating system so that the user may access a graphical user interface (GUI). The goal of the project is to automate some of the challenging manual system configuration tasks in order to enhance the security hardening of the Ubuntu OS. Unlike the command line interface, which moves most security measures away from users, the GUI format arranges actions so that they follow the order in which they were completed.

The fact that it has been demonstrated that enterprises can modify the system's security settings to comply with compliance and internal security standards is another crucial feature of the solution. Since the inventory had just recently been built, companies would typically have handled management activities like depot tracking inventory from managers.

Computer system security has elevated to the top of the priority list as the globe grows increasingly interconnected. This is particularly valid for businesses that use the Ubuntu operating system. Ubuntu has a lot of extra security features, but the system isn't very user-friendly overall, especially when it comes to hardening it to make it less vulnerable to exploits. This is frequently a very laborious procedure that takes a great deal of experience. The goal of this project is to create a hardening script that targets Ubuntu and uses a graphical user interface (GUI) to make the

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311074|

hardening procedure easier and faster for users. With its flexible interface and ability to establish minimum security rules, this solution puts non-technical administrators on par with technical administrators.

II. RESEARCH METHODOLOGY

The goal of the research technique used to create a GUI-based hardening script for Ubuntu is to produce a tool that is safe, adaptable, and easy to use, capable of meeting a variety of organizational security standards. The procedure is divided into many stages. First, a review of the literature on hardening methods and technologies currently in use is conducted. Next, requirements from businesses are gathered to make sure the script takes into account actual security requirements. Development uses Python and frameworks such as GTK+ and Qt to do both backend programming and user-friendly GUI design. A crucial part of improving the product is testing it for usability, policy compliance, and security efficacy. The last stages put a strong emphasis on user input, documentation, and regular updates to make sure the script stays applicable and efficient in changing security settings.

Creating a GUI-based hardening script for Ubuntu is a thorough way to improve system security by giving businesses with varying security requirements an approachable, adaptable solution. The first step in the process is to identify any holes that can be filled with a GUI tool by investigating current hardening strategies, such as those suggested in the CIS Benchmarks and other best practices. After that, feedback from businesses in various industries is gathered to comprehend their security policies and provide design flexibility for the product. The frontend GUI streamlines these procedures, making security hardening accessible even to non-technical users, while the backend development concentrates on scripting crucial security configurations like firewall setup, SSH hardening, and encryption .The tool's capabilities, which include policy templates and adjustable security settings, enable it to be customized to meet the unique compliance requirements of various organizations, including those in the business, government, and healthcare sectors. Testing makes that the script is easy to use and effective at stopping vulnerabilities, and regular updates keep it current to defend against new threats. The end result is a potent tool that makes managing system security easier and fortifies Ubuntu's protection against intrusions.

III. THEORY AND CALCULATION

The idea behind creating a GUI-based hardening script for Ubuntu is based on system hardening concepts, which minimize potential vulnerabilities through the application of security best practices. This entails installing firewalls, implementing robust authentication procedures, turning off superfluous services, and making sure that encryption is configured correctly. Calculating improvements in system security, such as decreased attack surfaces, fewer vulnerability counts, and improved compliance with security standards like CIS Benchmarks, is one way to assess the efficacy of these hardening actions. The tool's flexibility is calculated by its capacity to adapt to multiple corporate regulations, with metrics such as customization choices and usability comments indicating the success of the interface in meeting various security needs.

A few important points come up when talking about the creation of a GUI-based hardening script for Ubuntu. Through the project, complicated command-line hardening procedures will no longer be the only way that security administration is made easier for both technical and non-technical users. A user-friendly, visual interface will be provided. Through the integration of crucial security features, like firewall configuration, SSH policy enforcement, and data encryption, into an adaptable interface, the tool enables enterprises to customize security configurations to their own rules. The debate also centers on striking a balance between usability and flexibility: the tool must be accessible for those with less technical knowledge while still providing extensive customization for more experienced users. Furthermore, the tool's ability to adjust to changing threats and integrate seamlessly into a variety of organizational environments will be evaluated, necessitating ongoing testing, user input, and frequent updates. Thus, this project addresses the growing requirement for accessibility in security management as well as the need for strong, automated system hardening.

IV. RESULTS AND DISCUSSION

The Ubuntu Hardening Tool with GUI was created to make hardening an Ubuntu system easier and more automated. It provides important security settings via a user-friendly graphical user interface.SSH hardening, firewall management, user management, and system upgrades are among the main aspects of the program that have been put into practice and

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311074|

evaluated to guarantee their efficacy.An examination of the testing phase's outcomes is provided below, along with a discussion of the tool's wider application in system management and security.

Results

Ubuntu 18.04, 20.04, and 22.04 versions were used to test the tool's compatibility and efficiency.
The primary outcomes of the tests are as follows:

1.SSH Hardening:
Root Login Disabled:
After executing the “Disable Root Login” option in the GUI, the /etc/ssh/sshd_config file was correctly updated to prevent root access. Upon attempting to log in via SSH using the root account, the connection was refused, demonstrating the success of this feature.
Custom SSH Port: The tool was successful in changing the SSH port to a user-specified custom port from the default port of 22. Connections to the custom port were permitted, but attempts to connect via port 22 were refused. By using this feature, the likelihood of brute-force attacks against the default SSH port is reduced.

Disabling Password Authentication:
Only key-based authentication was allowed because the tool automatically disabled password authentication. The inability to access SSH connections without a valid key increased security by removing the avenue for password-based brute-force attacks.

2. Configuring the firewall:
UFW Management:
Users could activate or deactivate the UFW firewall with this tool. The default deny-all rule applied to incoming connections and the allow-all rule applied to outgoing connections were applied correctly when enabled. The GUI was used to add and remove firewall rules, and the system's firewall configuration accurately reflected each rule. For example, after the rule was applied, accessing a web server successfully confirmed that HTTP traffic (port 80) was allowed.
Display of Firewall Status:
All currently active firewall rules were listed in the UFW status, which was precisely retrieved and presented. System administrators could now easily review and manage security rules thanks to this feature.

3. Handling Users:
Adding/Removing Users:
New user accounts with the appropriate permissions were successfully added by the tool. Passwords were safely configured, and new users had access to the necessary privileges after logging in. Additionally, the tool eliminated user accounts without granting any further access or permissions, guaranteeing that there were no possible security gaps left.

4. Updates for the System:
Automated Updates:
The "Update and Upgrade" feature of the tool downloaded and applied system updates through the GUI as planned. This made sure the system always had the most recent security patches installed, which is crucial for reducing known vulnerabilities.

5. Auditing Features:
Service Auditing:
Administrators were able to check the system for vulnerable or superfluous services by using the tool, which listed open ports and active services. This feature gave users the ability to halt services like FTP that, if left open, might be a security risk.

Security Audit Report:
The tool's audit function gave a summary of the security posture of the system and included alerts regarding password weakness or needless port opening. System administrators can now take advantage of practical insights from this report to further harden their systems.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311074|

Discussion

The Ubuntu Hardening Tool has proven to be a successful tool for system administrators, especially those who are not accustomed to utilizing command-line interfaces, as evidenced by its smooth implementation and testing. The following are the main ideas raised regarding the findings:

1. Ease of Use and Accessibility:

Even for individuals who are not familiar with conventional command-line tools for Linux system hardening, the tool's graphical user interface (GUI) makes it very easy to use. The tool makes tasks like disabling root login, changing SSH ports, and configuring firewalls easier by combining multiple security configurations into a single interface. These tasks would otherwise require manual editing of system configuration files.

Because of its simplicity of use, there is less chance of manual configuration errors, which can be a significant source of security flaws. Additionally, without requiring in-depth knowledge of Linux security procedures, the GUI makes it simple to audit the system and apply security settings quickly.

2. Impact on Security Posture:

By enforcing best practices for SSH, firewalling, and user management, the tool considerably enhances the security posture of an Ubuntu system. For instance, common attack vectors like brute-force attacks are effectively mitigated by disabling password-based authentication and root login. Protecting systems that are exposed to the internet, such as web servers, database servers, and other vital infrastructure, requires taking these hardening steps.

Additionally, the tool helps prevent vulnerabilities that could be exploited if software is not kept up to date by automating the application of security patches through system updates. By itself, this feature can significantly lower the system's vulnerability to known exploits.

V. CONCLUSIONS

Our primary contribution is the planning and construction of a safe file system and network that was built with the express objective of strengthening file data security and network Linux kernel security. The primary goal is to identify system vulnerabilities by looking through configuration files, server files, and log files. Once these are found, the system will be secured by replacing the vulnerable attributes with secured ones and determining computer activities. We offer security for web servers, SSH servers, and other systems under network security. Application security is guaranteed by carefully examining each application's signature and by presenting every feature in a graphical user interface (GUI) manner, which enhances user experience.

DECLARATIONS

Study Limitations

None.

Acknowledgements

With great appreciation, we would like to thank Mr. Jayendra Kumar for his invaluable advice and assistance during this project. Their knowledge and experience were crucial to this project's successful conclusion. We also thank the Anurag University faculty and staff, especially the Department of Computer Science and Engineering, for providing the infrastructure and resources needed to complete this project. We would especially like to thank our coworkers and fellow students for their supportive comments and constructive criticism. Finally, we would like to express our gratitude to the open-source community for its contributions, particularly to those who maintain Ubuntu and other security tools that served as the basis for this study.

We could not have completed this project without their combined efforts.

Funding source

None.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.524

|www.ijirset.com |A Monthly, Peer Reviewed & Referred Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 13, Issue 11, November 2024

|DOI: 10.15680/IJIRSET.2024.1311074|

Competing Interests

Regarding the publication of this research, the authors declare that they have no conflicts of interest or competing interests. The project was carried out impartially and without any financial, personal, or professional conflicts influencing the outcomes or conclusions in any way during its design, development, or analysis.

HUMAN AND ANIMAL RELATED STUDY

Not applicable as the research does not involve human or animal subjects

REFERENCES

[1]. Mick Bauer, "Securing Ubuntu is a straightforward as installing it."- Secure Features in Ubuntu.
[2] Canonical Ltd, "UFW (Uncomplicated Firewall) Documentation" – Ubuntu Official Documentation.
[3] Andrés G. Aragoneses and The GUFW Team, "GUFW (GUI for UFW) Documentation" - GUFW Official Documentation
[4] Ric Messer and Michael Jang, "Security Strategies in linux platforms and applications".

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details