SEMINAR REPORT

ON

"GUI BASED HARDENING SCRIPT FOR UBUNTU"

BY

Mr. ARCHIT BARVE	Roll No. 81
Ms. SHREYA NAIK	Roll No. 104
Mr. SATVIK NALAVADE	Roll No. 105
Mr. MAYUR PATIL	Roll No. 117

Under the guidance of

Mr. GIRISH NAVALE

DEPARTMENT OF COMPUTER ENGINEERING

ALL INDIA SHRI SHIVAJI MEOMRIAL SOCIETY'S

INSTITUTE OF INFORMATION TECHNOLOGY

PUNE 411041

SAVITRIBAI PHULE PUNE UNIVERSITY

2023-2024

3005

AISSMS

INSTITUTE OF INFORMATION TECHNOLOGY

ADDING VALUE TO ENGINEERING

Approved by AICTE New Delhi, Recognized by the Government of Maharashtra
and Affiliated to Savitribai Phule Pune University.
Accredited by NAAC with A grade

Department of Computer Engineering

CERTIFICATE

This is to certify that **Mr. ARCHIT BARVE Roll No.81 , Ms. SHREYA NAIK Roll No.104 , Mr. SATVIK NALAVADE Roll No.105 , Mr. MAYUR PATIL Roll No.117** from **Third Year Computer Engineering** have successfully completed their seminar work titled

"GUI BASED HARDENING SCRIPT FOR UBUNTU"

at All India Shri Shivaji Memorial Society's Institute of Information Technology, Pune in the partial fulfillment of the Bachlors Degree in Computer Engineering

Mr. Girish Navale
Internal Guide

Mr. Girish Navale
Seminar Coordinator

Seal/Stamp of the college

Mrs. S. N. Zaware
Head of the Department
Computer Engineering

Place: PUNE
Date: 30-10-2023

ABSTRACT

This project aims to address the crucial task of securing Ubuntu operating systems through a Graphical User Interface (GUI) based hardening script, providing a user-friendly approach for implementing security measures in alignment with an organization's security policies. The purpose is to create a tool that streamlines the hardening process, making it accessible to individuals with limited IT skills.

The hardening script will offer a comprehensive range of security functions designed to fortify the Ubuntu OS. Users will have the flexibility to configure settings in accordance with their organization's specific security requirements. This includes features such as blocking SSH, USB access, Tor, and more, allowing administrators to tailor security configurations based on their organization's IT security policies.

The effectiveness of the tool will be assessed based on the diversity and effectiveness of the hardening functions it implements, as well as the emphasis on user experience. The script's success will be contingent on its ability to accommodate user settings, ensuring it caters to a wide range of security needs while prioritizing the paramount importance of safeguarding system integrity.

ACKNOWLEDGEMENT

With immense pleasure, I present the seminar report as part of the curriculum of the T.E. Computer Engineering. I wish to thank all the people who gave us unending support right from when the idea was conceived.

I express sincere and profound thanks to our Seminar Guide Mr. Girish Navale, and HOD Mrs. S. N. Zaware, who is always ready to help with the most diverse problems that I have encountered along the way. I express sincere thanks to all staff and colleagues who have helped directly or indirectly in completing this seminar successfully.

Mr. ARCHIT BARVE

Ms. SHREYA NAIK

Mr. SATVIK NALAVADE

Mr. MAYUR PATIL
AISSMS IOIT, Pune.

INDEX

Abstract **i**

Acknowledgement **ii**

Index **iii**

List of Tables **iv**

1 INTRODUCTION **1**

1.1 CONTEXT 1

1.2 PROBLEM STATEMENT 1

1.3 OBJECTIVE 2

2 LITERATURE SURVEY **3**

3 METHODOLOGY **4**

3.1 Designing User Interface 4

3.2 Implementing the Hardening Functions 5

4 CONCLUSION **7**

5 FUTURE SCOPE **8**

Bibliography **9**

List of Tables

2.1 Literature Survey 3

Chapter 1

INTRODUCTION

1.1 CONTEXT

In today's digital landscape, security is a paramount concern for organizations. Ensuring the security of computer systems and networks is essential to protect sensitive data, maintain the integrity of operations, and safeguard against potential threats. Ubuntu is a popular Linux distribution widely used in various organizations, and hardening it is a crucial task to align with an organization's security policies. However, this process can often be complex and require IT expertise. To address this challenge, the objective is to create a GUI-based hardening script that simplifies the hardening process and provides flexibility to cater to the specific security policies of different organizations.

1.2 PROBLEM STATEMENT

The problem at hand is to develop a GUI-based hardening script for the Ubuntu operating system. This script should be user-friendly, **allowing individuals with minimal IT skills to perform system hardening.** The script's flexibility is crucial to enable organizations to customize the hardening process based on their specific security policies. This means that the script should allow users to make decisions regarding security settings, like blocking SSH, USB devices, or Tor, in alignment with their organization's IT security policy.

1.3 OBJECTIVE

The primary objective of this project is to create a GUI-based hardening script for Ubuntu that addresses the following aspects:

1. **Ease of Use:** The script should be intuitive and user-friendly. Individuals with minimal IT skills should be able to use the GUI to initiate the hardening process without needing extensive technical knowledge.

2. **Customization:** The script should provide a high degree of flexibility. Users should be able to customize security settings based on their organization's IT security policy. This may include options to enable or disable specific services, restrict user privileges, or enforce specific firewall rules.

3. **Security Compliance:** The script should implement a set of hardening functions that enhance the security of the Ubuntu OS. This may include actions like updating the OS, configuring firewall rules, disabling unnecessary services, and applying access controls.

4. **User Experience:** Attention should be given to the user experience. The GUI should be well-designed, with clear instructions and meaningful feedback to guide users through the hardening process.

5. **Scalability:** The script should be designed in a way that it can be easily updated to accommodate new security measures or changes in Ubuntu OS versions.

Chapter 2

LITERATURE SURVEY

A literature survey represents a study of previously existing material on the topic of the report. This includes (in this order) -

1. Existing theories about the topic which are accepted universally.
2. Books written on the topic, both generic and specific.
3. Research done in the field usually in the order of oldest to latest.
4. Challenges being faced and ongoing work, if available.

Refer the table 2.1 for the Literature Survey.

Table 2.1: Literature Survey

S.No.	Name/Title of Paper Referred	Name & Year of Publication	Author
1	Linux Server and Hardening Security	Research Gate, 2013	Amit Nepal
2	Enhancing security of Docker using Linux hardening techniques	IEEE, 2016	Amith Raj MP, Ashok Kumar, Sahithya J Pai and Ashika Gopal
3	Linux Security: A Survey	IEEE, 2019	Matthew R. Yaswinski, Md Minhaz Chowdhury and Mike Jochen

Chapter 3

METHODOLOGY

3.1 Designing User Interface

In this phase, we focused on creating an intuitive user interface for our GUI-based hardening script. The goal was to make the configuration process as user-friendly as possible, especially for individuals with limited IT skills. We categorized security settings logically, offered explanations for each option, and used visual elements to enhance the interface's usability. By guiding users through the hardening process with a wizard-style approach and providing clear feedback, we aimed to ensure that the system could be securely configured in a straightforward and user-friendly manner.

1. **Categorization:** Grouped security settings logically. Categories like "User Management," "Network Security," "SSH Configuration," "Firewall Rules," and "USB Device Control" were created to help users easily locate and configure specific settings.

2. **Explanations:** Provided clear and concise explanations for each security setting. Tooltips, help buttons, or contextual information were used to explain the settings to users.

3. **Visual Feedback:** Elements like checkboxes, radio buttons, input fields, sliders, and dropdown menus were used to make it easy for users to interact with the settings. Visual feedback was provided when settings were changed or actions were performed.

4. **Error Handling:** Error messages or warnings were included for incorrect input or configuration conflicts. Users received meaningful feedback when they made mistakes.

5. **Customization:** Users were allowed to save and load configurations to create and apply predefined hardening profiles suitable for different scenarios.

6. **Progress Indicators:** For actions that took time to complete, such as updating packages or applying firewall rules, progress indicators or status bars were included to keep users informed.

7. **Responsiveness:** Ensured that the GUI was responsive and didn't freeze during hardening operations. Users were able to interact with the interface while the script was running.

3.2 Implementing the Hardening Functions

In this step, we concentrated on developing the core functionality of the hardening script. The primary objective was to enable users to configure their Ubuntu system in line with their organization's security policies. We implemented essential hardening functions, including disabling unnecessary services, defining firewall rules, managing software updates, configuring user accounts, SSH access, USB device control, network settings, and intrusion detection measures. These functions were designed to ensure a secure system while giving users the flexibility to make choices aligned with their specific security requirements. Each hardening function was thoroughly validated to prevent misconfigurations and adhere to best security practices.

1. **Service Management:** Unnecessary services were identified and disabled based on user choices. Critical services were protected from disruption.

2. **Firewall Rules:** A firewall management module was implemented to allow users to define and apply custom firewall rules. Presets for common scenarios, like "Block All Inbound Traffic" and "Allow SSH from Trusted IPs," were created.

3. **Manage Software Updates:** Implemented a mechanism to check for and apply software updates. Users were allowed to schedule updates or perform them manually. The script used secure sources for updates.

4. **SSH Configuration:** Users were provided with the ability to configure SSH

settings, such as changing the default SSH port, disabling root login, and specifying allowed IP addresses for SSH access.

5. **USB Device Control:** USB device policies were implemented, allowing users to restrict or allow USB devices based on user roles or specific devices

6. **Configure Network Settings:** Allowed users to configure network-related settings, such as DNS server preferences, network interfaces, and network security measures like enabling or disabling specific network protocols.

7. **Intrusion Detection:** Implemented intrusion detection features, such as log monitoring and alerting. Users set up alert thresholds and actions to be taken when suspicious activities were detected.

8. **Idempotency:** The script was designed to be safely run multiple times without causing conflicts or errors. It checked the system's current state before making changes.

Chapter 4

CONCLUSION

In conclusion, the development of a GUI-based hardening script for the Ubuntu operating system, offering flexibility to accommodate organizational security policies, is a vital step in enhancing the security of systems while ensuring ease of use for personnel with varying levels of IT expertise. By creating an intuitive interface that empowers users to configure security settings based on their organization's specific requirements, this script can significantly contribute to the overall security posture of Ubuntu systems. This initiative underscores the critical importance of security in today's digital landscape, and it emphasizes the need for user-friendly tools that can adapt to evolving security policies.

The GUI-based hardening script for Ubuntu OS offers several advantages. First, it simplifies the complex task of system hardening, making it accessible to individuals with limited IT skills, thereby reducing the potential for misconfigurations and security vulnerabilities. Second, it provides flexibility, allowing organizations to tailor security settings to their unique requirements, ensuring compliance with their security policies. Third, the script contributes to the overall improvement of security by enabling users to implement a wide range of hardening functions, making it an invaluable resource for system administrators. Lastly, by integrating a user-friendly graphical interface, the script fosters a smoother user experience and facilitates efficient system hardening.

Chapter 5

FUTURE SCOPE

The future scope of this project is promising and involves several avenues for enhancement and expansion. Firstly, more hardening functions can be incorporated into the script to cover a broader spectrum of security aspects, including network security, application security, and data protection. This will enable organizations to have a more comprehensive and robust security posture. Additionally, the script can evolve to support other Linux distributions, extending its utility to a wider user base. Integration with security standards and best practices, such as CIS benchmarks, can further improve its effectiveness in aligning with industry-specific security guidelines. Furthermore, the script can incorporate automatic update features to ensure ongoing security compliance. In the future, the development of a community-driven repository of security policies and configurations can be considered, allowing organizations to share and benefit from standardized hardening profiles. These potential enhancements will enable the script to adapt to the evolving landscape of IT security and continue to serve as a valuable tool in safeguarding Ubuntu-based systems.

Bibliography

[1] Arora, Namita, Tejasvi Bhosale, Vishakha Sharma, and Jyoti Supe. "Linux Hardening." International Journal on Recent and Innovation Trends in Computing and Communication 2, no. 5 (2014): 1019-1022.

[2] Jogi, Martin. "Establishing, Implementing and Auditing Linux Operating System Hardening Standard for Security Compliance." University of Tartu, Tartu (2017).

[3] Turnbull, James. "Hardening the Basics." Hardening Linux (2005): 1-77.

[4] Pal, Rajesh Kumar, and Indranil Sengupta. "Enhancing file data security in linux operating system by integrating secure file system." In 2009 IEEE Symposium on Computational Intelligence in Cyber Security, pp. 45-52. IEEE, 2009.