

**BAHRIA UNIVERSITY, (Karachi Campus)**

*Department of Computer Science*

# PROPOSAL

**Course Title:** Operating Systems  **Course Code**:CSL-320

**Course Instructor:** Dr. Shahid Khan **Class**: BS (CS) - 5A

**Senior Lab Instructor:** Ms. Mehwish Saleem **Name:**

**Date:**

|  |
| --- |
| ***PROJECT TITLE: “Linux Security”*** |
| ***GROUP MEMBERS LIST:***  *Mania Imam 02-134212-013*  *Tayyaba Imam 02-134202-056 (TEAM LEAD)*  *Shavana Yousuf 02-134212-022* |
| ***PROJECT SCOPE:***  This project's successful implementation will significantly enhance the security posture of Linux Ubuntu systems, leading to:  Reduced Risk of Data Breaches: Enhanced access control and data encryption will minimize the risk of unauthorized access to sensitive information.  Improved System Availability: Resource monitoring and process control will ensure system resources are available to legitimate users, preventing service interruptions and denial-of-service attacks.  Simplified Security Management: User-friendly tools will be provided for managing access control, security policies, and monitoring logs, simplifying security administration. |
| ***PROJECT ABSTRACT:***  This proposal outlines the development of a comprehensive security system for Linux Ubuntu environments, addressing the critical aspects of data integrity, confidentiality, and system availability. By implementing robust access control mechanisms, user authentication, and encryption techniques, this system aims to significantly enhance the security posture of Ubuntu systems, mitigating the risk of unauthorized access, data breaches, and system disruptions.  The objectives of the project align with its educational purpose and defined scope.  By continuously evolving and adapting to the ever-changing threat landscape, this project strives to ensure the security and integrity of Linux Ubuntu systems, protecting valuable data and maintaining system functionality for users worldwide. |
| ***PROJECT FUNCTIONALITIES:*** Implementing a Multi-Layered Defense To effectively address the threats, the proposed security system will implement a multi-layered approach that focuses on: 1. Securing SSH Access: Dynamic SSH Port Disabling: An innovative algorithm will automatically disable the SSH port (22) upon unsuccessful login attempts from unauthorized IP addresses, preventing further attempts and safeguarding against brute-force attacks.  Granular Access Control: Utilizing UFW and TCP Wrapper, the system will define precise access rules, granting access only to authorized IP addresses and specific services, further minimizing the attack surface. 2. Enhancing File Security: Password and Key Phrase Protection: Sensitive files and folders will be secured with strong passwords and key phrases, acting as an additional barrier against unauthorized access.  Data Encryption: For highly confidential information, data encryption will be implemented to ensure its confidentiality even if compromised. 3. System Resource Management: Resource Monitoring: The system will monitor resource utilization to detect and prevent malicious actors from consuming excessive resources, ensuring system availability for legitimate users.  Process Control: Mechanisms will be employed to control and limit processes, ensuring efficient resource allocation and preventing denial-of-service attacks 4. User Management: Robust Authentication: Strong user authentication mechanisms, such as two-factor authentication, will be implemented to verify user identities and prevent unauthorized access attempts.  Access Control Lists: Granular access control lists will be employed to define user privileges and permissions, ensuring access is granted on a need-to-know basis. |
| ***MODULE DISTRIBUTION:***  **Tayyaba’s tasks:**   1. Dynamic SSH Port Disabling:  * Research and choose tools * Develop script for automatic disabling * Configure logging and notifications  1. UFW and TCP Wrapper Configuration:  * Install and configure UFW * Define access rules * Configure TCP Wrapper for service restrictions   **Mania’s tasks:**   1. Password and Key Phrase Protection:  * Research and choose encryption tools * Implement encryption for sensitive files and folders * Develop automated encryption/decryption scripts * Create user guides for file encryption features   2. Data Encryption:   * Evaluate and choose data encryption solutions * Implement chosen solution for specific folders or partitions * Configure key management and recovery mechanisms * Document encryption process and key management procedures   **Shavana ‘s tasks:**   1. Resource Monitoring and Process Control:  * Research and choose monitoring tools * Develop scripts or utilize existing tools for: * Monitoring resource usage (CPU, memory, disk) * Identifying and terminating resource-intensive processes * Configuring thresholds and alerts   2. User Management and Access Control:   * Configure user accounts with appropriate privileges * Implement robust authentication * Create and manage user groups and access control lists * Develop user guides for managing accounts and access |

**Teacher Signature**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Remarks**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Submission Date**: