**A**

**Project**

**On**

Securing and Hardening Linux Server

**For the partial fulfilment of the Course**

***Linux Shell Programming (CSET-213/CBCA221)***

**Academic Year: 2024-24 (Odd Semester)**

**Submitted by**

**Anshula Lal**

**Under The Supervision of**

Dr Vimal Kumar/Dr. Debjani Ghosh/Dr Nitin Shukla

School of Computer Science Engineering & Technology

Bennett University (The Times Group), Greater Noida, UP-201310, India

****

**SCHOOL OF COMPUTER SCIENCE ENGINEERING & TECHNOLOGY**

**BENNETT UNIVERSITY (THE TIMES GROUP),**

**GREATER NOIDA, UP-201310, INDIA**

**November 2024**

**Contents**

[Introduction 4](#_Toc183769576)

[Background 4](#_Toc183769577)

[Project Scope 5](#_Toc183769578)

[In-Scope 5](#_Toc183769579)

[Out-of-Scope 5](#_Toc183769580)

[Deliverables 5](#_Toc183769581)

[Project Objectives 6](#_Toc183769582)

[Requirement Specification 7](#_Toc183769583)

[1. Hardware and Software Requirements 7](#_Toc183769584)

[2. Configuration and Management Requirements 7](#_Toc183769585)

[Functional and Non-Functional requirements 8](#_Toc183769586)

[Functional Requirements 8](#_Toc183769587)

[Non-Functional Requirements 8](#_Toc183769588)

[Implementation 10](#_Toc183769589)

[1. Creating A Linux Server: 10](#_Toc183769590)

[2. Installing System Updates and Patches 10](#_Toc183769591)

[3. Configure automatic Update 11](#_Toc183769592)

[4. Set Password Policy and Complexity 12](#_Toc183769593)

[5. Firewall Configuration 12](#_Toc183769594)

[6. Disable ssh access for root user 13](#_Toc183769595)

[7. Vulnerability Assessment 13](#_Toc183769596)

[Resources Used 15](#_Toc183769597)

[References 15](#_Toc183769598)

# Introduction

In an age where cyber threats are ever-evolving, securing and hardening Linux servers has become a critical aspect of IT infrastructure management. This project aims to reinforce the security of Linux servers by implementing a comprehensive set of best practices and advanced techniques. The project's scope includes identifying potential vulnerabilities, configuring firewall rules, enforcing strong authentication mechanisms, and employing system monitoring tools to detect and mitigate threats in real-time.

Furthermore, the project will cover the application of security patches, file integrity monitoring, and the use of intrusion detection systems to provide multiple layers of defences. By adopting a proactive approach to security, the project seeks to minimize the attack surface and ensure the Linux server environment is robust against unauthorized access and malicious activities. The outcome of this project will be a fortified Linux server setup, capable of withstanding a wide array of cyber threats, thereby enhancing the overall security posture of the organization.

# Background

Linux servers form the backbone of numerous organizations' IT infrastructures due to their reliability, scalability, and open-source nature. However, the very qualities that make Linux attractive also present unique security challenges. The growing sophistication of cyber threats necessitates robust measures to protect sensitive data, maintain service integrity, and ensure compliance with regulatory standards.

Historically, Linux servers have been targeted by various cyber-attacks, including unauthorized access attempts, malware infections, and denial-of-service attacks. These incidents underscore the critical need for a comprehensive security strategy. This project draws on well-established security principles and cutting-edge practices to address these threats. By focusing on proactive and reactive security measures, the project aims to build a resilient and secure Linux server environment.

The project builds upon established security frameworks and leverages the extensive range of security tools available in the Linux ecosystem. These tools are designed to minimize the attack surface, detect potential intrusions early, and respond effectively to security breaches. As cyber threats continue to evolve, the project emphasizes continuous monitoring, regular updates, and the adoption of the latest security practices to maintain a high level of security over time.

Ultimately, this project seeks to create a blueprint for securing and hardening Linux servers that can be adapted and implemented across various organizational contexts, ensuring that critical systems remain protected against emerging threats.

# Project Scope

## In-Scope

Vulnerability Assessment:

* Conduct a comprehensive audit to identify security vulnerabilities in the existing Linux server infrastructure.
* Use automated tools and manual methods to assess the server's security posture.

Configuration of Security Controls:

* Implement and configure firewalls, intrusion detection/prevention systems, and other security tools.
* Enforce strong authentication mechanisms and user access controls.
* Configure and enforce network security policies, including VPN setup for secure remote access.

System Hardening:

* Apply best practices for system hardening, including disabling unnecessary services and ports.
* Configure secure settings for server software and applications.
* Regularly update and patch the operating system and installed software to mitigate vulnerabilities.

Data Protection:

* Implement data encryption for sensitive information at rest and in transit.
* Set up secure backup and recovery processes.

Monitoring and Logging:

* Establish centralized logging and real-time monitoring systems to detect and respond to security incidents.
* Implement log analysis tools to identify patterns and potential threats.

## Out-of-Scope

Physical Security:

The project will not cover physical security measures for the data center or server location.

Non-Linux Systems:

The project will focus solely on Linux servers and will not include securing other operating systems.

Development of Custom Security Tools:

The project will use existing, widely accepted security tools and best practices rather than developing new security solutions from scratch.

## Deliverables

Security Assessment Report:

A detailed report identifying current vulnerabilities and risks.

Security Configuration Guidelines:

Documented best practices and configurations implemented during the project.

# Project Objectives

Identify Vulnerabilities: Conduct a comprehensive security assessment to identify potential vulnerabilities in the existing Linux server environment.

Implement Security Best Practices: Apply industry-standard security practices and configurations to enhance the baseline security of the Linux servers.

Strengthen Authentication Mechanisms: Enforce strong authentication and authorization protocols to ensure that only authorized users can access critical systems and data.

Configure Firewall and Network Security: Establish robust firewall rules and network configurations to protect against external threats and unauthorized access.

Apply Regular Security Updates: Develop a schedule for regular updates and patch management to ensure the system remains protected against newly discovered vulnerabilities.

Deploy Intrusion Detection and Prevention Systems: Implement intrusion detection and prevention systems to monitor and respond to suspicious activities in real-time.

Conduct Continuous Monitoring and Auditing: Establish continuous monitoring and auditing processes to detect and address security incidents promptly.

Enhance Data Protection: Ensure the protection of sensitive data through encryption, secure backups, and access controls.

These objectives aim to create a fortified, resilient Linux server environment that can withstand a wide array of cyber threats, ensuring the confidentiality, integrity, and availability of the organization's critical systems and data.

# Requirement Specification

Requirement Specifications: Securing and hardening a Linux Server

### Hardware and Software Requirements

#### Server Hardware:

Adequate CPU, RAM, and disk space to support the server and security tools.

Redundant power supplies and network interfaces for high availability.

#### Operating System:

Latest stable version of a Linux distribution (e.g., Ubuntu, CentOS, Debian).

#### Security Software:

Firewall software (e.g., iptables, firewalld).

Intrusion detection systems (e.g., Snort, OSSEC).

File integrity monitoring tools (e.g., AIDE, Tripwire).

Anti-virus and anti-malware software (e.g., ClamAV).

VPN software (e.g., OpenVPN) for secure remote access.

### Configuration and Management Requirements

#### User Authentication:

* Implement multi-factor authentication (MFA).
* Configure SSH with key-based authentication.
* Disable root login and enforce the use of sudo for administrative tasks.

#### Network Security:

* Define and enforce firewall rules to limit inbound and outbound traffic.
* Configure a VPN for remote access.
* Implement network segmentation and DMZ for separating critical services.

#### System Updates:

* Schedule regular updates and patch management for the OS and installed software.
* Automate security updates wherever possible.

#### Access Control:

* Define and enforce strict access control policies.
* Use role-based access control (RBAC) to limit user permissions.

#### Monitoring and Logging:

* Set up centralized logging (e.g., using syslog or a log management tool).
* Implement continuous monitoring tools (e.g., Nagios, Prometheus).
* Configure alerting for suspicious activities or potential breaches.

#### Data Protection Requirements

Encryption:

* Encrypt sensitive data at rest and in transit using strong encryption algorithms.
* Use tools like LUKS for disk encryption and SSL/TLS for data in transit.

#### Backup and Recovery:

* Establish regular backup schedules.
* Store backups securely and test recovery procedures periodically.

# Functional and Non-Functional requirements

## Functional Requirements

User Authentication and Authorization:

Implement multi-factor authentication (MFA).

Configure SSH with key-based authentication.

Enforce role-based access control (RBAC).

Firewall Configuration:

Establish robust firewall rules to limit inbound and outbound traffic.

Implement network segmentation and DMZ for separating critical services.

Intrusion Detection and Prevention:

Deploy intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor and respond to suspicious activities.

Set up alerting mechanisms for potential breaches.

System Updates and Patch Management:

Schedule regular updates and patches for the operating system and installed software.

Automate the application of security updates.

Data Encryption:

Encrypt sensitive data at rest and in transit using strong encryption algorithms.

Use SSL/TLS for secure data transmission.

Backup and Recovery:

Implement a regular backup schedule.

Store backups securely and test recovery procedures periodically.

Logging and Monitoring:

Configure centralized logging and monitoring tools.

Set up real-time monitoring for system health and security events.

## Non-Functional Requirements

Performance:

Ensure that security measures do not significantly impact server performance.

Optimize security tools and configurations to maintain high system efficiency.

Reliability:

Maintain high system availability and minimize downtime.

Implement redundancy for critical components to ensure continuous operation.

Scalability:

Design the security infrastructure to scale with growing demands.

Ensure that security measures can handle increased load and traffic.

Usability:

Provide clear documentation and guidelines for managing and maintaining security.

Ensure that security configurations are easy to implement and manage.

Compliance:

Adhere to relevant regulatory standards and industry best practices (e.g., GDPR, PCI-DSS).

Ensure that security measures meet compliance requirements.

Maintainability:

Implement modular security configurations to facilitate updates and maintenance.

Ensure that security tools and configurations can be easily modified and extended.

# Implementation

### Creating A Linux Server:

For the purpose of This Project A Linux Server is created on a HP Laptop (8GB RAM/ 250 GB HDD) Installing RedHat Enterprise Linux 9 on it by

1. Downloading RHEL 9 ISO image.
2. Downloading rufus utility
3. Using Rufus Utility, Creating bootable installation media on USB Flash drive.
4. Changed boot order in BIOS setting of Laptop to boot from USB drive
5. Inserted USB drive in laptop and powered in on.
6. Installed the Linux server on Laptop by following installation instructions.

### Installing System Updates and Patches

Package management Tools: DNF and YUM are package management tools used in RHEL distributions like Fedora, CentOS, and Rocky Linux. They simplify package management, installation, updates, and removal by handling all the package dependencies. YUM is the older tool, and DNF is its modern successor, offering improved performance and features. Both package managers are essential for maintaining a stable and updated Linux system.

The Apt (Advanced Package Tool) package management system is a set of tools to download, install, remove, upgrade, configure and manage Debian packages, and therefore all software installed on a Debian system. Ubuntu, Kali Linux, Linux Mint and MX Linux are some of the Debian based Distributions

To run the package Updates on Red Hat Enterprise Linux (RHEL) 9 open a terminal and login as root user or use sudo to gain administrative privileges as run following code:

Check for available updates:

sudo dnf check-update

This command will list all packages that have updates available.

To Update all packages run :

sudo dnf upgrade

Update security-related packages:

sudo dnf upgrade --security

This command will upgrade packages that have security errata.

Update minimal security-related packages:

sudo dnf upgrade-minimal --security

This command will upgrade only the minimal set of packages needed to address security issues.

After running these commands, your system should be up-to-date with the latest packages and security updates.

### Configure automatic Update

To set up automatic updates on RHEL 9, the dnf-automatic tool is used.

Install dnf-automatic:

sudo dnf install dnf-automatic -y

Configure dnf-automatic: Open the configuration file:

sudo vi /etc/dnf/automatic.conf

Edit the file to set desired options. Here's an example configuration:

ini

[commands]

upgrade\_type=security

apply\_updates=yes

emit\_via=stdio

Enable and start the dnf-automatic.timer:

sudo systemctl enable --now dnf-automatic.timer

This will configure the system to automatically check for and apply security updates. The configuration file can be adjusted to suit specific needs, such as setting the upgrade\_type to all to download all updates, or changing the emit\_via option to send notifications via email.

By default, dnf-automatic is set to check for updates daily. However, its interval can customize by editing the timer configuration.

Open the timer configuration file:

sudo vi /etc/systemd/system/dnf-automatic-install.timer

Modify the [Timer] section to set your desired interval. For example, to check for updates every week, use:

[Timer]

OnCalendar=weekly

Persistent=true

Save the file and exit the editor.

Reload the systemd manager configuration:

sudo systemctl daemon-reload

Restart the timer:

sudo systemctl restart dnf-automatic-install.timer

This will configure dnf-automatic to check for updates once a week. You can adjust the OnCalendar value to set different intervals, such as daily, monthly, or even specific times of the day.

### Set Password Policy and Complexity

To set password complexity and quality in RHEL 9, the pam\_pwquality module is used. Here's how to configure it to enforce following rules:

Number of attempts allowed before locking the account - 3.

Minimum password length 10 character.

Minimum number of character classes 3 (lowercase, uppercase, digits, special characters).

Maximum number of repeated characters 3.

Install authselect

sudo dnf install authselect -y

Switch to the profile that enforces password quality

sudo authselect select sssd

Edit PAM configuration file

sudo vi /etc/pam.d/password-auth

Add following line to enforce password quality

password required pam\_pwquality.so retry=3 minlen=12 minclass=3 maxrepeat=3

Save and exit editor

Restart PAM service

sudo systemctl restart sssd

This configuration will enforce password complexity rules for user accounts on RHEL 9 system. the parameters can be adjusted to meet specific security requirements.

### Firewall Configuration

Inatall firewalld

sudo dnf install firewalld -y

Enable and start firewalld service

sudo systemctl enable firewalld

sudo systemctl start firewalld

Check status of firewalld service

sudo systemctl status firewalld

List available zones

sudo firewall-cmd --get-zones

Set default zone (public)

sudo firewall-cmd --set-default-zone=public

Warning: ZONE\_ALREADY\_SET: public

success

To allow a specific service (eg HTTP) run

sudo firewall-cmd --zone=public --add-service=http --permanent

sudo firewall-cmd --reload

To allow a specific port(eg 8080) run

sudo firewall-cmd --zone=public --add-port=8080/tcp --permanent

sudo firewall-cmd --reload

### Disable ssh access for root user

Disabling SSH access for the root user is a crucial security measure to help protect your server from unauthorized access. Here's how it can be done on a RHEL 9 system

Open SSH configuration file

##### sudo vi /etc/ssh/sshd\_config

Find the line that says PermitRootLogin (it might be commented out with a #):

#PermitRootLogin yes

Change this line to:

PermitRootLogin no

If the line is commented out, make sure to uncomment it by removing the # at the beginning.

Open /etc/ssh/sshd\_config.d/01-permitrootlogin.conf in editor

Change PermitRootLogin yes to PermitRootLogin no

Save the file and exit the editor.

Restart the SSH service to apply the changes:

sudo systemctl restart sshd

After making these changes, the root user will no longer be able to log in via SSH. You should ensure that you have another user with sudo privileges to maintain administrative access to the server.

### Vulnerability Assessment

For this project we have implemented on our test Linux server OpenSCAP for conducting Vulnerabilities Scan. OpenSCAP is a powerful tool that leverages the Security Content Automation Protocol (SCAP) to check for vulnerabilities and ensure compliance with security policies. It is designed to help administrators and auditors manage system security and compliance. Here are some key points about OpenSCAP:

#### Key Features

* SCAP Compliance: OpenSCAP implements the Security Content Automation Protocol (SCAP), a U.S. standard maintained by the National Institute of Standards and Technology (NIST).
* Vulnerability Assessment: It provides tools for automated vulnerability checking, helping to identify and classify vulnerabilities on a system.
* Security Policies: OpenSCAP includes a variety of hardening guides and configuration baselines developed by the open-source community.
* Flexibility: The ecosystem offers great flexibility and interoperability, reducing the costs of performing security audits.
* Continuous Compliance: It supports continuous security compliance, including periodic assessment and risk monitoring.

#### Implementation Steps:

**Install OpenSCAP:**

##### sudo dnf install openscap openscap-scanner openscap-utils -y

**Run a basic scan:**

##### sudo oscap xccdf eval --profile xccdf\_org.redhat.scap\_security\_guide\_profile\_toplevel --results-id myscan results.xml system.xml

This command will perform a scan and save the results to results.xml.

**View the scan results:**

##### sudo oscap xccdf export --arf arf.xml results.xml

Locate the SCAP content provided by the scap-security-guide package:

##### sudo find / -name '\*ssg-rhel\*.xml'

Identify the relevant SCAP content file, such as ssg-rhel9-ds.xml (the exact name might vary).

**Run the scan using the identified SCAP content:**

##### sudo oscap xccdf eval --profile xccdf\_org.ssgproject.content\_profile\_standard --results results.xml /path/to/ssg-rhel9-ds.xml

Replace /path/to/ssg-rhel9-ds.xml with the actual path(/usr/share/xml/scap/ssg/content/) to the SCAP content file.

**Generate a report from the results:**

##### sudo oscap xccdf generate report results.xml > report.html

**View the generated report in a web browser:**

##### firefox report.html

No profile matching suffix "xccdf\_org.ssgproject.content\_profile\_standard" was found.

It seems like the profile xccdf\_org.ssgproject.content\_profile\_standard is not available on your system. Let's try listing the available profiles to find a suitable one for your scan:

List available profiles:

##### sudo oscap info /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml

This command will display the profiles included in the SCAP content file for RHEL 9.

Find a matching profile from the list and use it in the scan command:

##### sudo oscap xccdf eval --profile <profile\_id> --results results.xml /path/to/ssg-rhel9-ds.xml

Replace <profile\_id> with the appropriate profile ID from the list.

Generate a report from the results:

##### sudo oscap xccdf generate report results.xml > report.html

View the generated report in a web browser:

##### firefox report.html

# Resources Used

1. A Laptop to Install Red Hat Linux
2. Redhat Enterprise Linux Software ISO image
3. 64 GB USB 2.0 Flash Drive to Create bootable Installation media
4. Rufus utility to create bootable USB flash drive from RHEL 9 ISO image

# References

Red Hat Documentation:

<https://docs.redhat.com/en/documentation/red_hat_enterprise_linux/9>