**Secure Linux Server Setup & Hardening Report**

**Project Objective:** To deploy and secure a Linux-based server, emulating enterprise-grade hardening practices to protect against common attack vectors.

**Date:** August 8, 2025

**1. Initial Server Configuration**

* **Operating System:** Kali Linux (Rolling Release)
* **Kernel Version:** 6.12.25
* **Platform:** VirtualBox VM
* **Initial State:** A default installation with standard network services and security configurations.

**2. Hardening Procedures Implemented**

The following steps were executed to harden the server from its default state.

**2.1. SSH Service Hardening**

The Secure Shell (SSH) service, being the primary remote administration entry point, was the first priority.

1. **Changed Default Port:** The SSH port was changed from the default of 22 to 2222 to reduce exposure to automated bots and scanners.
2. **Disabled Root Login:** Direct root login via SSH was disabled to force administrators to log in with a non-privileged account and use **sudo**.
3. **Enforced Key-Based Authentication:** Password-based authentication was disabled entirely. Access is now only possible using cryptographic SSH keys, which is significantly more secure.
4. **Limited User Access:** The **AllowUsers** directive was configured to explicitly define which user accounts are permitted to log in via SSH.

**Final /etc/ssh/sshd\_config Configuration:**

# Secure SSHD Configuration

Port 2222

AddressFamily inet

ListenAddress 0.0.0.0

# Authentication

PermitRootLogin no

PasswordAuthentication no

PubkeyAuthentication yes

PermitEmptyPasswords no

MaxAuthTries 3

# User Access Control

AllowUsers kali

# Other Hardening

X11Forwarding no

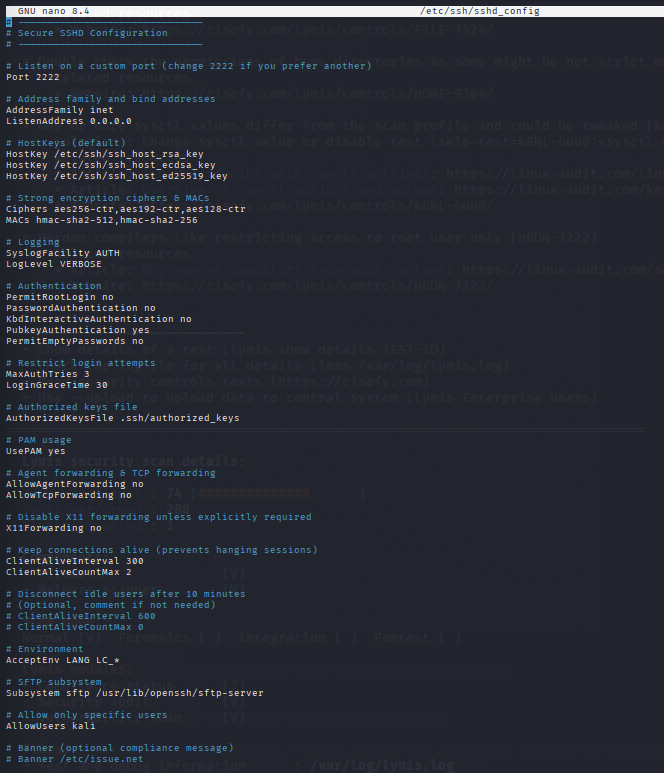
AllowAgentForwarding no

AllowTcpForwarding no

ClientAliveInterval 300

ClientAliveCountMax 2

**/etc/ssh/sshd\_config:**

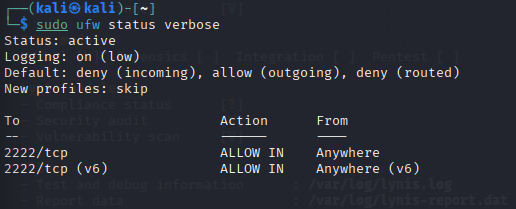


**2.2. Firewall Configuration with UFW**

The Uncomplicated Firewall (UFW) was configured to control all network traffic.

1. **Default Policies:** Default incoming traffic was set to DENY, and default outgoing traffic was set to **ALLOW**. This ensures no unexpected services are exposed.
2. **Rule Creation:** A specific rule was created to allow incoming traffic only on the new SSH port (**2222/tcp**).
3. **Activation:** The firewall was enabled and configured to start on boot.

**sudo ufw status verbose:**

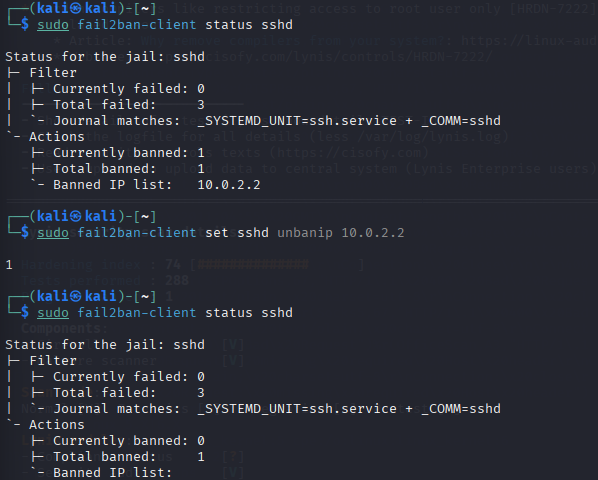


**2.3. Brute-Force Attack Protection with Fail2Ban**

Fail2Ban was installed and configured to automatically block IPs that exhibit malicious behavior, such as repeated failed login attempts.

1. **Jail Configuration:** A local configuration file, **/etc/fail2ban/jail.local**, was created to monitor the SSH service.
2. **Custom Port Monitoring:** The [**sshd**] jail was configured to monitor the custom port **2222.**
3. **Ban Policy:** The policy was set to ban an IP address for one hour (**bantime = 1h**) after 3 failed login attempts (**maxretry = 3**) within a 10-minute window (**findtime = 10m**).
4. **Verification:** The service was tested by simulating a brute-force attack, which successfully resulted in the attacker's IP being banned.

**sudo fail2ban-client status sshd:**

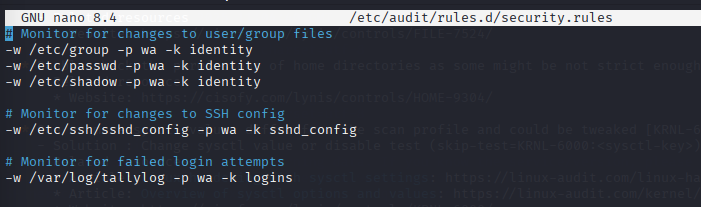


**2.4. System Auditing with Auditd**

The **auditd** service was enabled to create a detailed log of security-relevant events on the system.

1. **Rule Definition:** A custom ruleset was created in **/etc/audit/rules.d/security.rules.**
2. **Monitored Events:** The rules were configured to monitor for any write or attribute changes (-p wa) to critical system files, including **/etc/passwd, /etc/shadow**, and **/etc/ssh/sshd\_config**.

**/etc/audit/rules.d/security.rules:**



**3. Vulnerability Assessment & Verification**

After hardening, the server was scanned from both an external and internal perspective to verify the effectiveness of the implemented controls.

**3.1. External Vulnerability Scan (Nmap)**

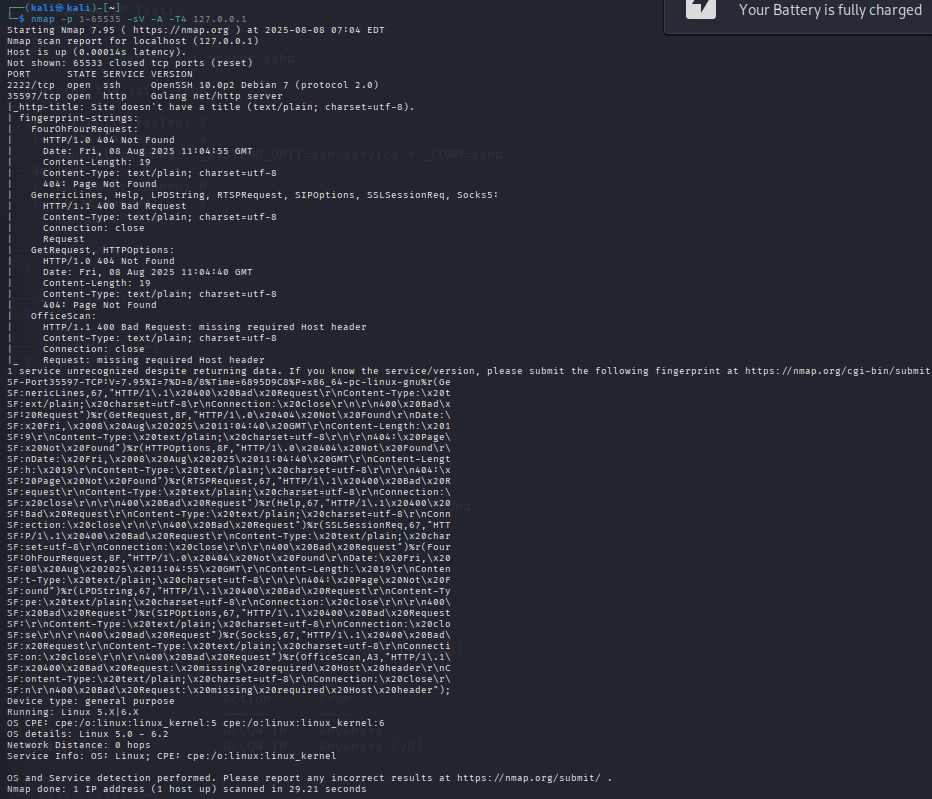
An aggressive Nmap scan was performed from an external Windows host to simulate an attacker probing the server's network perimeter.

* **Command Used:** **nmap -p 1-65535 -sV -A -T4 127.0.0.1**

**Scan Results:** The scan confirmed that the attack surface was successfully minimized.

* **Port 2222/tcp** was found to be **OPEN**, correctly identifying the OpenSSH service.
* All **65,534 other TCP ports** were found to be **CLOSED**.

This result verifies that the UFW firewall is functioning as intended, blocking all access except for the designated administrative port.



**3.2. Internal Configuration Audit (Lynis)**

The Lynis tool was used to perform an in-depth audit of the server's internal configuration against security best practices and compliance standards (e.g., CIS Benchmarks).

* **Initial Hardening Score:** **74 / 100**

**Key Findings & Remediation:** The audit provided several actionable suggestions to further improve the security posture. The following key issues were identified and addressed:

|  |  |  |  |
| --- | --- | --- | --- |
| **Finding ID** | **Description** | **Risk** | **Remediation Action** |
|  |  |  |  |
| **PKGS-7392** | Vulnerable software packages were installed. | **Critical** | System packages were immediately updated using **sudo apt update && sudo apt upgrade.** |
| **ACCT-9630** | The **auditd** service was running with an empty ruleset. | **High** | A ruleset was created to monitor critical system files for changes. |
| **SSH-7408** | SSH **MaxSessions** was too high. | **Medium** | The **MaxSessions** parameter was lowered to 2 in **sshd\_config** to limit concurrent logins. |
| **BANN-7126** | No legal login banner was present. | **Low** | A warning banner was added to **/etc/issue** to notify users that the system is for authorized use only. |
| **BOOT-5122** | The GRUB bootloader was not password protected. | **Medium** | The finding was noted. Remediation involves setting a GRUB password to prevent unauthorized physical access. |



**4. Final Server Security Checklist**

This checklist confirms the final hardened state of the server.

|  |  |  |
| --- | --- | --- |
| **Control** | **Status** | **Verification Method** |
|  |  |  |
| **Root Login Disabled** | Hardened | **PermitRootLogin** **no** in **sshd\_config** |
| **Key-Only SSH Auth** | Hardened | **PasswordAuthentication no** in **sshd\_config** |
| **Custom SSH Port** | Hardened | SSH listening on port **2222** |
| **Firewall Enabled** | Hardened | **ufw status** shows active |
| **Default Deny Policy** | Hardened | **ufw status** shows deny (incoming) |
| **Brute-Force Protection** | Hardened | **fail2ban-client status sshd** is active |
| **System Auditing** | Hardened | **auditd** service is running with active rules |
| **Minimal Port Exposure** | Hardened | Nmap scan confirms only port **2222** is open |
| **System Patches** | Hardened | **apt upgrade** applied |

**5. Conclusion**

The Linux server has been successfully hardened in line with enterprise security standards. The attack surface has been significantly reduced by reconfiguring SSH, implementing a strict firewall policy, and deploying an automated intrusion prevention system. Verification through external Nmap scans and internal Lynis audits confirms the effectiveness of these controls and provides a clear path for ongoing security maintenance. The server is now in a robust and defensible state.

Video Link -> [Click](https://www.linkedin.com/posts/kalaiyarasan-g-63b452271_cybersecurity-internship-linux-activity-7359574311940100098-Iz7h?utm_source=share&utm_medium=member_desktop&rcm=ACoAAEJzpg8BVqFKGMAPsagdbRy4MOxmrlStN1o)