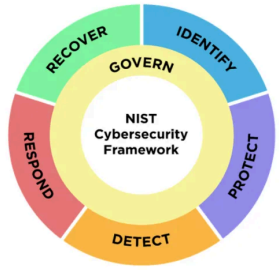
Linux Server Security Assessment and High-Risk Remediation (NIST Cybersecurity Framework 2.0 Controls)

Introduction:

This report documents the results of a security configuration and posture review performed against the target Linux system. The assessment was aligned to the NIST Cybersecurity Framework (CSF) 2.0, with findings mapped to the relevant controls. The goal of this exercise was to identify gaps, assess associated risks, and recommend practical remediation steps.



The review covered user authentication, package management, configuration management, data protection logging, and system hardening. Findings were categorized by risk severity and mapped to NIST CSF 2.0 functions (Identify, Protect, Detect, Respond, Recover).

Target System:

Device / System Details	Description
Hostname	vm-ubuntu-test
IP Address	192.168.xx.xxx
Operating System / Version	Ubuntu 24.04
Kernel Version	6.8.0
Architecture	x86_64
Virtualization / Hypervisor	VirtualBox
Assessment Tool	Lynis 3.0.9
Assessment Date	2025-09-09

User / Assessor	Catherine Czarnonycz / System Administrator
Purpose / Notes	Evaluate the system against NIST CSF 2.0 controls, identify configuration and security gaps, assess associated risks, and provide actionable remediation guidance to improve overall security posture. Baseline remediation captured.

Executive Summary:

The assessment identified several gaps across authentication, system configuration, and data protection.

- **High-risk issues (5 total):** Weak password enforcement, unprotected bootloader, outdated packages, insecure sudoers directory, and USB storage driver enabled.
- **Medium-risk issues (6 total):** Sysctl misconfigurations, unused firewall rules, lack of partition separation, missing integrity tools, unconfigured remote logging, and unrestricted core dumps.
- **Low-risk issue (1 total):** Absence of legal login banners.

Addressing the **high-risk items** should be prioritized to reduce the likelihood of unauthorized access and system compromise. Medium- and low-risk issues should be remediated as part of a structured hardening program.

Detailed Findings and Remediation:

The following table summarizes findings, mapped controls, risks, and recommended remediation actions:

Security Gap Analysis and Recommended Remediation					
System Category	**Issue**	**Description**	**Risk**	**NIST CSF 2.0 Control**	**Remediation**
Users, Authentication	Missing password strength module	Weak passwords can compromise accounts.	High	PR.AA-03: Users, services, and hardware are authenticated	Install and configure pam_pwquality:
Packages	Found vulnerable packages (PKGS-7392)	Outdated packages increase risk of compromise.	High	PR.PS-02: Software is maintained, replaced, and removed commensurate with risk	Update all packages to latest security versions

Security Gap Analysis and Recommended Remediation

System Category	Issue	Description	Risk	NIST CSF 2.0 Control	Remediation
GRUB Boot	No password protection	Bootloader unprotected, allowing unauthorized system access.	High	PR.PS-01: Configuration management practices are established and applied	Set GRUB boot password
File Permissions	/etc/sudoers.d directory has insecure permissions	Directory permissions could allow privilege escalation	High	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Restrict permissions to root-only access
USB, External Media	USB storage driver not disabled	Unauthorized data transfer via USB is possible	High	PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	Disable USB storage driver
PAM Authentication	libpam-tmpdir not installed	User temporary files are shared, risking tampering between accounts	Medium	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Install and configure libpam-tmpdir to isolate /tmp per user. Verify PAM configuration and document
Kernel Hardening	Sysctl values differ from recommended profile	System hardening profile not fully applied, increasing exposure	Medium	PR.PS-01: Configuration management practices are established and applied	Adjust /etc/sysctl.conf to recommended security values
Firewalls	Check iptables for unused rules	Unused firewall rules may allow unintended access	Medium	PR.IR-01: Networks and environments are protected from unauthorized logical access and usage	Review iptables rules and remove unused entries
File Systems	/home, /tmp, /varnot on separate partitions	Lack of partition separation increases risk of privilege escalation, data corruption, and resource exhaustion	Medium	PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	To decrease impact, place each on separate partitions according to best practice

Security Gap Analysis and Recommended Remediation

System Category	Issue	Description	Risk	NIST CSF 2.0 Control	Remediation
Logging	External logging not enabled	Logs may be lost or destroyed, limiting incident detection	Medium	DE.CM-01: Networks and network services are monitored to find potentially adverse events	Configure remote logging for centralized archival; Enable logging to an external logging host for archiving purposes and additional protection
Core Dumps	Core dumps not restricted	Sensitive information may be exposed via core dumps	Medium	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Restrict access in /etc/security/limits.conf
File Integrity	Integrity tools missing or disabled (dm-integrity, dm-verity)	Lack of file or disk integrity tools increases risk of undetected system tampering or data corruption	Medium	PR.DS-01: The confidentiality, integrity, and availability of data-at-rest are protected	Install and enable file integrity tools (e.g., AIDE, dm-verity, dm-integrity) and configure regular checks
Banners	No legal banner on /etc/issue or /etc/issue.net	Lacks formal security/legal notification	Low	PR.AA-05: Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties	Add standard security and legal banners

Remediation of High-Risk Items:

Due to the sensitive nature of the high-risk items, remediation was carried out on these vulnerabilities during the audit review.

- **Missing password strength module**
  Weak authentication controls
  Risk Level: **HIGH**

- **Vulnerable packages (PKGS-7392)**
  Outdated versions expose system to exploits
  Risk Level: **HIGH**

- **GRUB Boot - No password protection**
  System vulnerable to unauthorized access and changes during boot
  Risk Level: **HIGH**

- **Insecure file permission (/etc/sudoers.d directory**
  Privilege escalation risk
  Risk Level: **HIGH**

- **USB storage driver not disabled**
  Unrestricted USB access may allow data exfiltration or malware installation
  Risk Level: **HIGH**