LazySysAdmin

Compliance & Risk Assessment Service

Demo Security Assessment Findings Report

January 30 2026: Version 1.0

Security/IT Operation Team
codibu.com

Table of Contents

1 Confidentiality Statement

This document is the exclusive property of Codibu.com and LazySysAdmin.
It contains proprietary and confidential information intended solely for demonstration and assessment purposes.

No part of this document may be copied, reproduced, distributed, or disclosed, in whole or in part, in any form, without prior written consent from Codibu.com.

Codibu.com may share this document with authorized auditors, partners, or government stakeholders under appropriate non-disclosure agreements (NDAs) for the purpose of demonstrating security assessment methodology, compliance awareness, and educational use.

This document does not represent an attack against a production environment and is provided strictly for demonstration, training, and security awareness purposes.

2 Disclaimer

This security assessment represents a point-in-time evaluation of the LazySysAdmin demonstration environment.
All findings and recommendations are based solely on the information observed during the assessment period and do not account for changes, configurations, or modifications made outside of that timeframe.

Due to the time-limited nature of the engagement, it was not feasible to test every security control or configuration in depth.
Codibu.com prioritized the assessment to identify high-risk and commonly exploited weaknesses that an attacker would most likely target in a real-world scenario.

Codibu.com recommends conducting regular security assessments, either internally or through qualified third-party assessors, on at least an annual basis to validate the effectiveness of security controls and maintain an acceptable security posture over time.

3 Contact Information

Name	Title	Contact Information
Demo Company		
John Smith	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.smith@demo.com
Jim Smith	IT Manager	Office: (555) 555-5555 Email: jim.smith@demo.com
Joe Smith	Network Engineer	Office: (555) 555-5555 Email: joe.smith@demo.com
TCM Security		
Heath Adams	Lead Penetration Tester	Office: (555) 555-5555 Email: hadams@codibu.com
Bob Adams	Penetration Tester	Office: (555) 555-5555 Email: badams@codibu.com
Rob Adams	Account Manager	Office: (555) 555-5555 Email: radams@codibu.com

4 Assessment Overview

During the assessment period, Codibu.com conducted a controlled security assessment against the LazySysAdmin demonstration environment to evaluate its security posture against commonly accepted industry best practices.

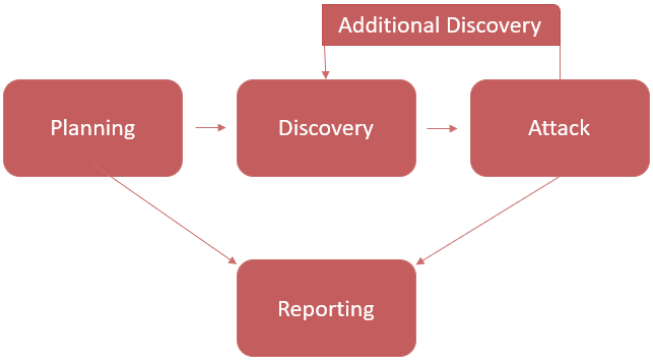
The assessment focused on identifying weaknesses that could be exploited by an external attacker through publicly exposed services.

All testing activities were conducted in alignment with recognized security assessment standards and guidelines, including:

- **NIST SP 800-115** – Technical Guide to Information Security Testing and Assessment
- **OWASP Testing Guide (v4)**
- Codibu.com's customized security testing methodology

The security assessment followed a structured, multi-phase approach:

- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



5 Assessment Components

5.1 External Penetration Test

An external penetration test simulates the perspective of an unauthenticated external attacker attempting to gain access to systems without prior knowledge, credentials, or internal resources.

For this assessment, Codibu.com evaluated the LazySysAdmin demonstration environment using publicly available information and exposed network services.

Activities included limited open-source intelligence (OSINT) review, such as identifying publicly accessible service information, system banners, and externally observable configurations that could be leveraged against the target environment.

Codibu.com also performed network scanning and service enumeration to identify exposed services, misconfigurations, and potential attack vectors that could be exploited to gain initial access.

Identified weaknesses were validated through controlled exploitation solely to demonstrate potential impact and risk.

All testing was conducted in a non-production environment and was restricted to demonstration and educational purposes.

6 Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

7 Scope

Assessment	Details
External Penetration Test	Admin.local

7.1 Scope Exclusions

Per client request, Denial-of-Service (DoS) testing was explicitly excluded from the scope of this assessment.

7.2 Client Allowances

No allowances or prior knowledge were granted by the client; the assessment was performed under full black-box conditions.

8 Executive Summary

Codibu.com conducted an external security assessment against the LazySysAdmin demonstration environment to evaluate its external security posture and identify weaknesses that could be exploited by an unauthenticated attacker.

The assessment identified multiple high-risk security weaknesses which, when combined, could allow an external attacker to progress from initial access to full system compromise.

These weaknesses did not require advanced exploitation techniques and were discoverable through basic reconnaissance and commonly used assessment methods.

The findings demonstrate how fundamental security misconfigurations, if left unaddressed, can significantly increase organizational risk and expose critical systems to unauthorized access.

Codibu.com strongly recommends addressing the identified issues in a timely manner and implementing defense-in-depth controls to reduce the likelihood of similar attack paths in a real-world environment.

This assessment was performed in a non-production environment and is intended for demonstration, training, and security awareness purposes only.

8.1 Attack Summary

The following table outlines how Codibu.com identified and validated a complete system compromise within the LazySysAdmin demonstration environment.

This assessment highlights how common misconfigurations and weak credential handling can lead to full system control.

Step	Action	Recommendation
1	Identified exposed SMB services allowing **unauthenticated (guest) access** to internal file shares.	Disable guest access on SMB services and restrict access to authenticated users only.
2	Discovered sensitive internal files containing **plaintext credentials** stored within shared directories.	Prohibit storing credentials in plaintext files. Implement secure credential storage solutions (e.g., password managers or secrets vaults).
3	Validated that exposed credentials were **reused across multiple services**, including SSH access.	Enforce unique credentials per service and prevent credential reuse across systems.
4	Successfully authenticated to the system via SSH using valid user credentials, obtaining standard user access.	Implement Multi-Factor Authentication (MFA) for all remote access services such as SSH.
5	Identified excessive privilege assignment allowing the authenticated user to execute all commands via sudo without restriction.	Apply the principle of least privilege. Restrict sudo access to only necessary commands and roles.
6	Leveraged misconfigured sudo permissions to escalate privileges and obtain full administrative (root) access to the system.	Regularly audit privilege assignments and monitor privilege escalation events through logging and alerting mechanisms.

9 Security Strengths

Detection of Suspicious Activity

- The LazySysAdmin environment successfully detected network reconnaissance and scanning activity.
- Early alerts allowed identification of unusual access patterns and rapid mitigation of scanning attempts.
- Demonstrates basic monitoring and incident response readiness.

10 Security Weaknesses

10.1 Missing Multi-Factor Authentication

- Remote access relied solely on username/password.
- Once valid credentials were exposed, full system access was possible.
- Recommendation: Implement MFA for all remote and administrative access to reduce impact of credential exposure.

10.2 Weak Password Policy

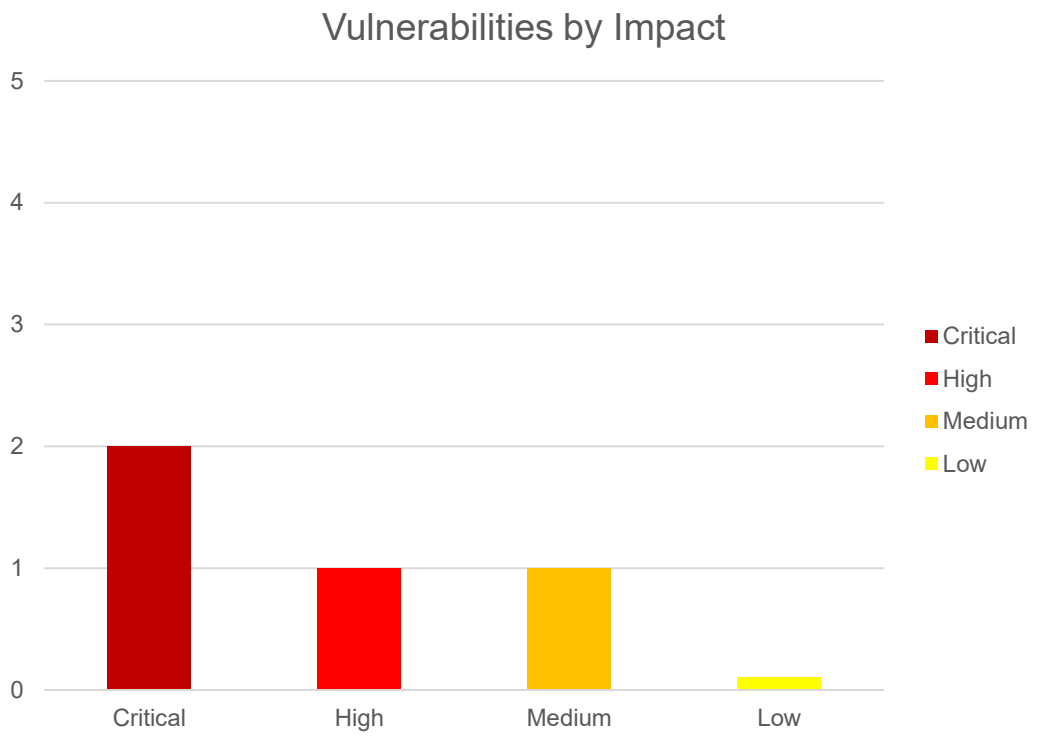
- Plaintext passwords were stored in shared directories and reused across services.
- Passwords followed predictable patterns (e.g., season + year + special character).
- Recommendation: Enforce unique, complex passwords per service and eliminate plaintext storage.

10.3 Unrestricted Logon Attempts

- Unlimited login attempts enabled brute-force success on external services.
- Excessive sudo privileges allowed standard users to escalate to root without restriction.
- Recommendation: Implement login attempt restrictions, account lockout policies, and least-privilege sudo assignments.

11 Vulnerabilities by Impact

The following chart illustrates the vulnerabilities found by impact:



11.1 External Penetration Test Findings

CSA-0001: Multiple External Service Exposure – Linux Web Server (High)

Description:	During the external assessment, multiple network services were discovered to be publicly accessible, including SSH, HTTP, SMB, MySQL, and IRC. Service enumeration revealed outdated software versions and misconfigurations that increased the attack surface. Particularly, SMB services permitted unauthenticated share enumeration, and web directories exposed configuration artifacts that could facilitate credential discovery.
Impact:	High
System:	192.168.55.36 – Linux Web Server
References:	OWASP ASVS 1.14 – Secure Configuration NIST SP800-53 CM-7 – Least Functionality NIST SP800-53 SC-7 – Boundary Protection

Evidence Summary (Redacted):

- SSH service publicly reachable
- HTTP server exposed multiple directories and legacy paths
- SMB guest session enabled with readable share
- MySQL service externally reachable without authorization
- Sensitive configuration files discovered within web-accessible paths

```
[+] IP: 192.168.59.36:445       Name: Admin.local               Status: NULL Session
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        print$                                                  NO ACCESS       Printer Drivers
        share$                                                  READ ONLY       Sumshare
        IPC$                                                    NO ACCESS       IPC Service (Web server)
```

Screenshot 1 – SMB Share Enumeration

Description: SMB enumeration confirmed a NULL session with readable share permissions.

Recommendation:

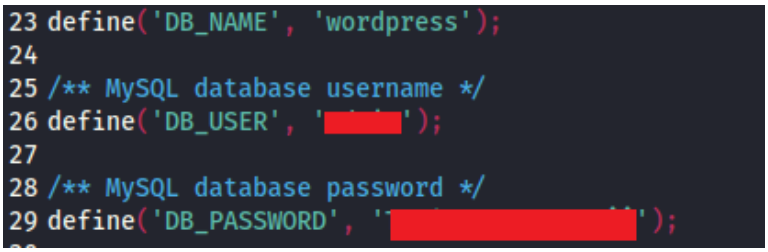
- Restrict external exposure to only required services
- Implement firewall rules and network segmentation
- Disable anonymous SMB access and enforce authentication
- Remove unused services and close unnecessary ports
- Apply regular patching and version updates
- Conduct periodic external vulnerability scans

CSA-0002: Plaintext Credential Exposure – Web Application Configuration (Critical)

Description:	Database credentials were identified in a web application configuration file stored in plaintext. Exposure of these credentials could allow unauthorized database access and full application compromise if obtained by an external attacker.
Impact:	Critical
System:	Web Application – HTTP Service
References:	NIST SP800-53 IA-7 – Cryptographic Key Management OWASP ASVS 2.10 – Sensitive Data Protection

Evidence Summary (Redacted):

- Configuration file contained database username and password
- File accessible through directory enumeration paths



Screenshot 2 – Plaintext Database Credentials in wp-config.php

Credentials were visible in plaintext and accessible through web directory enumeration.

Recommendation:

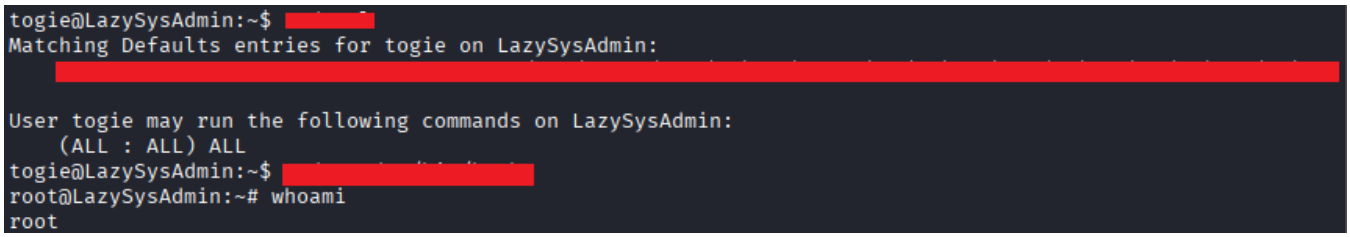
- Remove credentials from plaintext configuration files
- Use environment variables or a secure secret manager
- Rotate all exposed credentials immediately
- Move configuration files outside the web root
- Apply file permission hardening and access controls

CSA-0003: Excessive Privilege Assignment – Local User Account (Critical)

Description:	A standard user account possessed unrestricted administrative privileges through system policy, allowing potential full system compromise if credentials were obtained.
Impact:	Critical
System:	Linux Host – Local Account Policy
References:	NIST SP800-53 AC-2 – Account Management NIST SP800-53 AC-6 – Least Privilege

Evidence Summary (Redacted):

- Sudo policy allowed full administrative command execution



Screenshot 3 – Unrestricted Sudo Privilege Escalation

The standard user account successfully obtained root privileges through unrestricted sudo policy.

Recommendation:

- Enforce the Principle of Least Privilege
- Limit sudo permissions to required commands only
- Implement role-based access control (RBAC)
- Enable audit logging for privileged actions
- Review and validate administrative accounts periodically

CSA-0004: Weak Credential Storage Practices – File Share (Medium)

Description:	System artifacts indicated weak or default password usage practices, increasing susceptibility to brute force and credential stuffing attacks.
Impact:	Medium
System:	File Share / Web Directory
References:	NIST SP800-53 IA-5 – Authenticator Management OWASP ASVS 2.1 – Password Security

Evidence Summary (Redacted):

- Text files referencing simple or default credentials

Recommendation:

- Enforce strong password policy (length, complexity, rotation)
- Implement account lockout thresholds
- Deploy Multi-Factor Authentication (MFA)
- Conduct periodic credential audits and user awareness training

Remediation

Who:	Security / IT Operations
Vector:	Remote External Access
Action:	**Item 1 – Missing Multi-Factor Authentication (MFA)** **Observation:** External authentication services (e.g., SSH, Web Admin Panels, VPN-like access) relied solely on username and password. **Risk:** If credentials are exposed or reused, unauthorized access becomes trivial. **Recommendation:** • Enforce MFA across all remote administrative and external-facing authentication services. • Prefer hardware-based or app-based token authentication (FIDO2 / TOTP). • Apply conditional access policies where applicable. **Item 2 – Unlimited Login Attempts** **Observation:** Authentication services permitted unrestricted login attempts. **Risk:** Enables brute-force and password spraying attacks. **Recommendation:** • Implement account lockout thresholds (e.g., 5 failed attempts → 15-minute lock). • Enable rate limiting and IP throttling. • Deploy intrusion detection or fail2ban-style controls. **Item 3 – Weak Password Policy** **Observation:** Evidence of simple or reused credentials was discovered in shared files and configuration artifacts. **Risk:** Credential reuse significantly increases compromise probability across multiple services. **Recommendation (Aligned with CIS Guidelines):** • Minimum **14 characters** • Unique passwords per system/service • Avoid dictionary words, names, or predictable patterns • Enforce password history and rotation policies • Integrate breached-password screening where possible **Item 4 – User Enumeration Exposure** **Observation:** Authentication interfaces returned distinguishable responses for valid vs invalid usernames. **Risk:** Allows attackers to identify valid accounts before brute-force attempts. **Recommendation:** • Standardize authentication error messages. • Return generic responses such as *"Invalid credentials"* regardless of account validity. • Log enumeration attempts for monitoring. • **Additional Organizational Recommendations** • Conduct periodic **security awareness training** on password hygiene and phishing risks. • Audit employee credentials against public breach databases. • Prohibit reuse of corporate email addresses or usernames on third-party services. • Establish quarterly access reviews and privilege validation.