Purple Team Report

Date: June 16, 2025

CONFIDENTIAL INFORMATION

Bernardo Walker Leichtweis
Enzzo Machado Silvino
Cassio Vieceli Filho

Contents

1 Executive Summary

This report presents the security vulnerabilities identified in the assets of the internal network and the DMZ, focusing on the hosts **192.168.8.34** (internal network) and **192.168.8.50** (DMZ). The analyses were conducted by **seven distinct groups** during *Graybox* penetration tests, with access to the environment as the test user: `cebolinha:c3b0l1nh4`.

The detected vulnerabilities were classified according to their severity and potential risk to the confidentiality, integrity, and availability of the evaluated assets.

The purpose of this report is to summarize the findings, prioritize the issues based on their criticality, and recommend corrective measures to mitigate the risks.

1.1 Scope

The assessment covers the following network assets:

- **192.168.8.34** – Host located in the **internal network**
- **192.168.8.50** – Host located in the **DMZ**

1.2 Vulnerability Summary

A total of **4 unique vulnerabilities** were identified, categorized according to the severity levels presented below:

- **1 Critical vulnerability**
- **1 High vulnerability**
- **2 Low vulnerabilities**

2 Vulnerabilities

2.1 Critical

- **[NOT REMEDIATED] Unauthorized access to the backup service password**
  Total affected assets: 1 – Remediated: 0 – Retested: 0 – Not remediated: 1

2.2 High

- **[NOT REMEDIATED] Improperly exposed services**
  Total affected assets: 2 – Remediated: 0 – Retested: 0 – Not remediated: 2

2.3 Low

- **[NOT REMEDIATED] Exposed SSH version (OpenSSH_9.6.p1)**
  Total affected assets: 2 – Remediated: 0 – Retested: 0 – Not remediated: 2
- **[NOT REMEDIATED] Exposed Nginx version (1.27.4)**
  Total affected assets: 1 – Remediated: 0 – Retested: 0 – Not remediated: 1

3 Identified Vulnerabilities

3.1 Unauthorized Access to the Backup Service Password

Severity: Critical
Affected Asset: `192.168.8.34` (internal network)
CVSS v3.1: 9.1 (AV:L/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H)
Reference: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Description: It was identified that the test user can read the backup service password stored in the `/etc/restic/pass` file on the host `192.168.8.34`. This represents a critical flaw as it exposes sensitive credentials, potentially allowing complete compromise of the backup service and possible privilege escalation.

Recommended Fix: Change the permissions of the `/etc/restic/pass` file to `chmod 600`, ensuring that only the backup service owner has read and write permissions. Additionally, evaluate the use of password vaults (such as HashiCorp Vault) for secure storage of these credentials. Review access control policies to prevent exposure of sensitive files in the system.

3.2 Improperly Exposed Services in the DMZ and Internal Network

Severity: High
Affected Assets: `192.168.8.50` (DMZ), `192.168.8.34` (internal network)
CVSS v3.1: 7.5 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Reference: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Description: Services are exposed in both the DMZ and the internal network, allowing any attacker to perform port scans and identify open services in both environments. This configuration expands the attack surface and may facilitate reconnaissance and exploitation of subsequent vulnerabilities.

Recommended Fix: Conduct a thorough review of firewall rules and routing policies, blocking unauthorized access from the WAN to the internal network and the DMZ. Allow only essential ports to be open to the external public, such as 80 (HTTP) and 443 (HTTPS) in the DMZ.

3.3 Exposed SSH Version

Severity: Low
Affected Assets: `192.168.8.34`:2222, `192.168.8.50`:22
CVSS v3.1: 3.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Reference: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Description: The OpenSSH `9.6.p1` versions are exposed via banners in the SSH services accessible on the internal network and DMZ hosts. While not a direct vulnerability, this exposure can assist attackers in reconnaissance and planning specific attacks.

Recommended Fix: Modify the SSH configuration to hide the version banner. This

can be done by editing the `/etc/ssh/sshd_config` file and setting the `DebianBanner no` option. Restart the SSH service after the change to apply the configuration.

3.4 Exposed Nginx Version

Severity: Low
Affected Asset: `192.168.8.50`:8080 (DMZ)
CVSS v3.1: 3.1 (AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:N)
Reference: CWE-200: Exposure of Sensitive Information to an Unauthorized Actor

Description: The Nginx `1.27.4` version is exposed on the DMZ host, identified during the port scan. Exposing the HTTP server version can provide useful information to potential attackers.

Recommended Fix: Modify the Nginx configuration file (`nginx.conf`) to disable the `Server` header. For example, add the `server_tokens off;` directive in the `http` or `server` block. After the change, restart the Nginx service to apply the configuration.

4 Observations

During the analysis and consolidation of the security test results, some reported vulnerabilities were disregarded for the following reasons:

- **Vulnerabilities not considered:** Examples include access to the `/admin` path in the *mailcow* service, which did not configure any flaw beyond the expected standard access and does not represent a vulnerability in itself, as well as the read permission for the test user in the `/var/www/html` directory, given that there is no exposure of credentials, `.env` files, or `.git` directories.
- **Vulnerabilities categorized under other sections:** For example, the exposure of the *Wazuh* page on the internal network was considered part of the *Improperly Exposed Services* vulnerability, avoiding redundancies in the report.
- **Items outside the scope or control:** Self-signed SSL/TLS certificates were reported; however, as per the proposed scenario, this configuration could not be altered and was therefore not treated as a vulnerability.
- **Vulnerabilities with insufficient description or lack of evidence:** Some reports, such as the one from G9 mentioning *Sessions Vulnerable to XSS*, did not provide concrete evidence or sufficient technical details for validation and were discarded in this report.

This approach aims to ensure accuracy, relevance, and focus on resolving vulnerabilities that directly impact the security of the tested environment.

5 Conclusion

This report presents the vulnerabilities identified during security tests conducted in a controlled environment with test user access, as defined in the scope. Critical, high, and low severity flaws were detected, collectively indicating significant opportunities to enhance the infrastructure's security.

Critical vulnerabilities, such as unauthorized access to sensitive passwords, require immediate attention due to the high risk of complete compromise of the involved services. The improper exposure of services in both the DMZ and the internal network also represents a concerning attack vector that must be mitigated through stricter firewall rules and proper segmentation.

Additionally, low-severity vulnerabilities, such as the exposure of service versions, while not direct risks, provide information that could facilitate future attacks and should therefore be addressed to strengthen the security posture.

The recommendations provided in this report include clear and practical corrective actions that, if implemented effectively, will significantly reduce the attack surface and improve the environment's resilience against threats.

6 Suggested Action Plan

Vulnerability	Severity	Maximum Deadline	Responsible
Access to the backup service password	Critical	24h (until 06/17)	Infrastructure Team
Improperly exposed services	High	72h (until 06/19)	Network Administrator
Exposed SSH version	Low	Until 06/21	Linux Sysadmin
Exposed Nginx version	Low	Until 06/21	DevOps / Web

7 Appendices

7.1 General Definitions

Term	Description
Total Unique Vulnerabilities	Distinct vulnerabilities identified within the scope.
Zero-Day Vulnerability	Flaw unknown to the vendor, exploitable before patches are available.
Critical Vulnerability	High impact on confidentiality, integrity, or availability.
High Vulnerability	Requires immediate attention due to potential impact.
Medium Vulnerability	Less urgent but can cause serious issues.
Low Vulnerability	Not imminent but should be mitigated in the long term.

7.2 Severity Levels

Level	Description
Critical	CVSS 9.0–10.0: High probability and impact.
High	CVSS 7.0–8.9: Medium to high probability and impact.
Medium	CVSS 4.0–6.9: Low to medium probability or impact.
Low	CVSS 0.1–3.9: Low probability and impact.
Informational	No direct impact but provides useful information.