PRAGYA

Defending against digital threats

Sample Network Report

Defending Against Digital Threats

www.pragyacyber.com

Table of Contents

Document Confidentiality

This document contains sensitive information which needs to be shared with appropriate personnel of ORGANIZATION on a purely need to know basis. The following recommendations are issued with respect to distributing this document

- Distribute to authorized personnel only
- Comply with the appropriate security measures according to the classification level of the document

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. Pragya prioritized the assessment to identify the weakest security controls an attacker would exploit. Pragya recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact Information

Version	Author	Date
1.0	Pragya Cyber	27 - 05 - 2025

1. Information

Security assessment is a method for better understanding threats and defending against them. Penetration testing simulates intruder's methods for gaining illegal access to a company's network systems and then compromising them. To attempt a penetration, most attackers use traditional methods.

2. Objective & Methodology

To detect hidden vulnerabilities in web application interfaces and simulate an attackto estimate the risk of compromise, cover all attack pathways, and trace the attack surface.

Running a PT test on the target infrastructure / apps has the primary goal of determining how easy it is to get unauthorized access to the system by utilizing various sorts of real-world exploits and typical attack patterns to gain access to the network or data. Using numerous approaches a malevolent hacker would try, the exercise provides visibility into the likely impact of the fault on the underlying network, operating system, database, and so on.

Our testing methodologies, investigative process and procedures are aligned with SANS, NIST and OWASP standards, testing guides and best practices for application / infrastructure security appraisal. These guidelines are followed to elevate the level of risk awareness to globally recognized standards.

3. Assessment Components

3. 1 Internal Penetration Testing

Simulates an attack from within the organization to identify internal threats and security gaps.

4. Severity Ratings

The following table defines levels of severity and the corresponding CVSS score range 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.
Medium	**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.

5. Executive Summary

This report presents the results of the "Grey Box" penetration testing for **ORGANIZATION** internal network perimeter. The recommendations provided in this report are structured to facilitate remediations of the identified security risks. This document serves as a formal letter of attestation for the recent ORGANIZATION "Grey Box" internal network penetration testing.

Evaluation ratings compare information gathered during the engagement to "best in class" criteria for security standards. We believe that the statement made in this document provide an accurate assessment of **ORGANIZATION's** current security.

5.1 Scope of the assessment

Scope Information	
Assessment	**Targets**
Internal Penetration Testing	1. xxx.xxx.xx.xx 2. xxx.xxx.xx.xx 3. xxx.xxx.xx.xx

5.2 Vulnerability Summary

The following table illustrates the Vulnerabilities found by severity.

4	0	4	8	16
Critical	**High**	**Medium**	**Low**	**Total**

5.3 Report Card

The following report card illustrates detailed explanation of the findings of a Target.

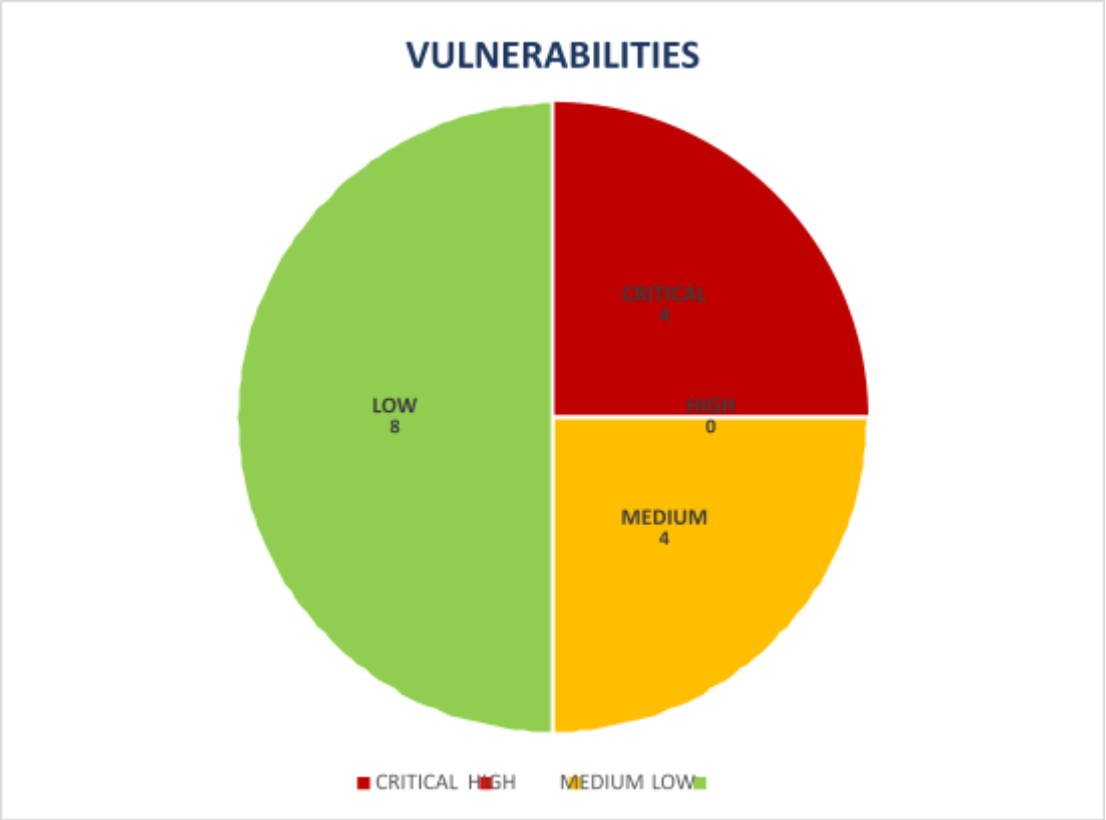
Internal Penetration Testing				
S.no	**Target**	**Finding**	**Description**	**Severity**
1	xxx.xxx.xx.xx, xxx.xxx.xx.xx	SSH Protocol Authentication Bypass (Remote Exploit Check)	A remote attacker can bypass authentication on the SSH server.	Critical

2	xxx.xxx.xx.xx	SSL Certificate Cannot Be Trusted	The SSL certificate presented by the service is invalid, untrusted, or expired, indicating a potential risk of man-in-the-middle attacks or data interception.	Medium
3	xxx.xxx.xx.xx	SSL Self-Signed Certificate	The service uses a self-signed SSL certificate, meaning it wasn't issued by a trusted certificate authority. This poses a security risk because clients cannot verify the server's identity, making it vulnerable to man-in-the-middle attacks and data interception.	Medium
4	xxx.xxx.xx.xx, xxx.xxx.xx.xx	SSH Weak Algorithms Supported	The SSH server allows weak or no encryption, making it vulnerable to attacks.	Medium
5	xxx.xxx.xx.xx	ICMP Netmask Request Information Disclosure	An attacker can exploit this vulnerability to obtain sensitive information about the target network by sending ICMP netmask requests and analyzing the responses.	Low
6	xxx.xxx.xx.xx	ICMP Timestamp Request Remote Date Disclosure	The ICMP timestamp request allows an attacker to determine the exact time set on the remote host by sending an ICMP timestamp request and receiving a response containing the remote host's timestamp.	Low

7	xxx.xxx.xx.xx, xxx.xxx.xx.xx	SSH Server CBC Mode Ciphers Enabled	The SSH server allows the use of Cipher Block Chaining (CBC) mode ciphers, which are vulnerable to various attacks like padding oracle attacks if not properly implemented. This weakness can potentially enable attackers to decrypt encrypted traffic or even inject malicious data.	Low
8	xxx.xxx.xx.xx, xxx.xxx.xx.xx	SSH Weak MAC Algorithms Enabled	The SSH server allows weak MD5 and 96-bit MAC algorithms, making it vulnerable to attacks like man-in- the-middle attacks that can compromise authentication and data integrity.	Low
9	xxx.xxx.xx.xx , xxx.xxx.xx.xx	SSH Weak Key Exchange Algorithms Enabled	The remote SSH server allows weak key exchange algorithms, making it vulnerable to attacks like man-in- the-middle attacks where an attacker can intercept and decrypt the communication.	Low

6. Details of Vulnerabilities found

6.1 Summary of findings



6.2 Critical Severity Findings

6.2.1 SSH Protocol Authentication Bypass (Remote Exploit Check)

Description	A remote attacker can bypass authentication on the SSH server.
Severity	**CRITICAL**
CVSS	**n/a**
Recommendations	Update to libssh version 0.7.6, 0.8.4, or a later version if available. If an update is not feasible, contact your vendor for support and guidance.
References	http://www.nessus.org/u?6f6b157e http://www.nessus.org/u?505261f8 http://www.nessus.org/u?58a0f73d
Assets Affected	xxx.xxx.xx.xx, xxx.xxx.xx.xx

6.3 High Severity Findings

None

6.4 Medium Severity Findings

6.4.1 SSL Certificate Cannot Be Trusted

Description	The SSL certificate presented by the service is invalid, untrusted, or expired, indicating a potential risk of man-in- the-middle attacks or data interception.
Severity	**MEDIUM**
CVSS	**n/a**
Recommendations	Obtain a valid SSL certificate from a trusted Certificate Authority (CA) and correctly configure it on the server hosting the service.
References	https://www.itu.int/rec/T-REC-X.509/en https://en.wikipedia.org/wiki/X.509
Assets Affected	**xxx.xxx.xx.xx**

6.4.2 SSL Self-Signed Certificate

Description	The service uses a self-signed SSL certificate, meaning it wasn't issued by a trusted certificate authority. This poses a security risk because clients cannot verify the server's identity, making it vulnerable to man-in-the-middle attacks and data interception.
Severity	**MEDIUM**
CVSS	**n/a**
Recommendations	Obtain a publicly trusted SSL certificate from a reputable Certificate Authority (CA) like Let's Encrypt, DigiCert, or Comodo and install it on the server hosting the service. This replaces the self-signed certificate, ensuring clients trust the connection.
References	n/a
Assets Affected	**xxx.xxx.xx.xx**

6.4.3 SSH Weak Algorithms Supported

Description	The SSH server allows weak or no encryption, making it vulnerable to attacks.
Severity	**MEDIUM**
CVSS	**n/a**
Recommendations	Disable weak SSH cipher suites (e.g., DES, 3DES, and MD5) on both the client and server. Enable strong cipher suites like AES256-GCM-SHA384. Consult server and client documentation for instructions on configuring allowed ciphers.
References	https://tools.ietf.org/html/rfc4253#section-6.3
Assets Affected	**xxx.xxx.xx.xx**, **xxx.xxx.xx.xx**

6.5 Low Severity Findings

6.5.1 ICMP Netmask Request Information Disclosure

Description	An attacker can exploit this vulnerability to obtain sensitive information about the target network by sending ICMP netmask requests and analyzing the responses.
Severity	**LOW**
CVSS	**n/a**
Recommendations	Implement firewall rules or network filters to block incoming ICMP echo requests (type 8) and ICMP netmask requests (type 17). This prevents the remote host from responding to these requests, thereby mitigating the information disclosure vulnerability.
References	n/a
Assets Affected	**xxx.xxx.xx.xx**

6.5.2 ICMP Timestamp Request Remote Date Disclosure

Description	The ICMP timestamp request allows an attacker to determine the exact time set on the remote host by sending an ICMP timestamp request and receiving a response containing the remote host's timestamp.
Severity	**LOW**
CVSS	**n/a**
Recommendations	Configure firewalls or network filters to block ICMP timestamp request (type 13) packets and ICMP timestamp reply (type 14) packets. This prevents the server from receiving requests and sending responses, eliminating the date disclosure vulnerability.
References	n/a
Assets Affected	**xxx.xxx.xx.xx**

6.5.3 SSH Server CBC Mode Ciphers Enabled

Description	The SSH server allows the use of Cipher Block Chaining (CBC) mode ciphers, which are vulnerable to various attacks like padding oracle attacks if not properly implemented. This weakness can potentially enable attackers to decrypt encrypted traffic or even inject malicious data.
Severity	**LOW**
CVSS	**n/a**
Recommendations	Disable CBC cipher encryption on your SSH server and enable CTR or GCM mode encryption. This may involve updating server software, modifying SSH configuration files (e.g., sshd_config), and restarting the SSH service.
References	n/a
Assets Affected	**xxx.xxx.xx.xx, xxx.xxx.xx.xx**

6.5.4 SSH Weak MAC Algorithms Enabled

Description	The SSH server allows weak MD5 and 96-bit MAC algorithms, making it vulnerable to attacks like man-in-the-middle attacks that can compromise authentication and data integrity.
Severity	**LOW**
CVSS	**n/a**
Recommendations	Disable MD5 and 96-bit MAC algorithms in SSH server configuration. Consult vendor documentation for specific instructions.
References	n/a
Assets Affected	**xxx.xxx.xx.xx, xxx.xxx.xx.xx**

6.5.5 SSH Weak Key Exchange Algorithms Enabled

Description	The remote SSH server allows weak key exchange algorithms, making it vulnerable to attacks like man-in-the-middle attacks where an attacker can intercept and decrypt the communication.
Severity	**LOW**
CVSS	**n/a**
Recommendations	Disable weak key exchange algorithms (e.g., DSA, 3DES) in the SSH server configuration, enabling only strong algorithms like Diffie-Hellman group exchange (e.g., Diffie-Hellman group 14, 16, 18, or 24) and elliptic curve cryptography (ECC) algorithms.
References	https://datatracker.ietf.org/doc/html/rfc9142
Assets Affected	**xxx.xxx.xx.xx, xxx.xxx.xx.xx**

7. Conclusion

The internal penetration test of ORGANIZATION's network, encompassing three IPs and various assets, revealed sixteen vulnerabilities. Four critical, four medium, and eight low-severity issues were identified. The most critical finding was an SSH authentication bypass vulnerability (6.2.1) allowing remote exploitation. Importantly, several vulnerabilities, particularly concerning weak SSH algorithms and SSL certificates, affected multiple IPs, suggesting a systematic misconfiguration across the network. The majority of identified vulnerabilities are addressable through patching, configuration updates, or firmware upgrades, as detailed in the comprehensive report. We strongly recommend a risk-prioritized remediation approach focusing on the critical vulnerabilities first, followed by implementation of strengthened internal security practices and improved asset configuration management to prevent recurrence.