**{{ companyName }} – {{ networkType }}**

**Blackbox Vulnerability Assessment Report**

Prepared by RNS Technology Services (hereafter referred to as RNS) for {{ companyName }}. Portions of this document and the templates used in its production are the property of RNS and cannot be copied (in full or in part) without its permission. While precautions have been taken in the preparation of this document, RNS the publisher, and the author(s) assume no responsibility for errors, omissions, or for damages resulting from the use of the information contained herein.

Table of Contents

[Executive Summary 3](#_Toc93907115)

[Scope and Detailed Findings](#_Toc93907118) 6

[Summary of Recommendations](#_Toc93907136) 7

[Conclusion and Next Steps](#_Toc93907137) 13

## Executive Summary

RNS Offensive Security Services team conducted a blackbox vulnerability assessment and penetration testing on {{ companyName }} public facing infrastructure based on

{{ assessmentDate }} request on

RNS Offensive Security Services team conducted an external black box penetration testing, excluding any unsafe checks, on External Network as part of ongoing Managed Security Services Contract on

The purpose of this testing was to:

* Conduct a penetration testing on the External IP addresses to identify technical vulnerabilities and discover whether a malicious user may leverage these flaws to compromise the security of {{ companyName }} External Network.
* Provide recommendations for the identified vulnerabilities to ensure timely remediation and minimize the risk of successful exploitation.

The identified vulnerabilities have been classified into severity categories as depicted below:

A total of five (5) findings have been identified during this assessment and are listed below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| # | Title | Risk | CVSS | Finding ID |
| 1 | - | High | 7.5 | - |
| 2 | - | Medium | 5.3 | - |
| 3 | - | Low | 3.7 | - |
| 4 | - | Low | 3.7 | - |
| 5 | - | Low | 2.6 | - |

### Findings Severity Matrix

The following matrix that considers likelihood and consequence of an exploit based on CVSS framework has also been applied as applicable and can be referred to:

|  |  |  |  |
| --- | --- | --- | --- |
| P1 | Critical | 9.0-10.0 | CVSS Score |
| P2 | High | 7.0-8.9 |
| P3 | Medium | 4.0-6.9 |
| P4 | Low | 0.1-3.9 |
| P5 | Informational | 0.0 |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| FINDINGS SEVERITY MATRIX | | Likelihood | | | | |
| Very Low | Low | Medium | High | Very High |
| Consequence | Very High | Medium | Medium | High | Critical | Critical |
| High | Medium | Medium | High | High | Critical |
| Medium | Low | Medium | Medium | High | High |
| Low | Informational | Low | Low | Medium | Medium |
| Very Low | Informational | Informational | Low | Low | Low |

### 

### Vulnerability Assessment Methodology

The Network penetration testing was carried out based on the steps depicted below.

***Identification of Target***

The scope as provided by {{ companyName }} team is taken as the target for the vulnerability assessment.

***Port Scanning***

Port Scanning is one of the most popular reconnaissance techniques used to discover open ports. A variety of scans are used to check for every possible occurrence of open ports.

***System Finger Printing, Enumeration & Checking of Information Flow***

Various passive and active techniques are used to determine the operating system, services running on the server and their versions. This helps in identifying the OS and the service-related vulnerabilities. It also helps in identifying if any Network applications are hosted on the server.

***Automated Vulnerability Scanning***

Various passive and active techniques are used to determine the operating system, services running on the server and their versions. This helps in identifying the OS and the service-related vulnerabilities. It also helps in identifying if any Network applications are hosted on the server.

***Eliminating False Positives and Exploitation***

Based on the information gathered in the above steps, vulnerabilities and risks are tested. False positives are filtered, and their impacts are considered while rating the vulnerabilities.

***Result Collation, Analysis and Reporting***

Once the assessment is complete, the results are collated and analysed to prepare a report. It details the identified the vulnerabilities, risk, mitigation criteria and proof of concept.

## Scope and Detailed Findings

Following section documents the scope of network black box penetration testing and associated technical information about identified vulnerabilities.

The assessment started with reconnaissance to gather passive intelligence on the targeted scope. It involved gathering information that can be used in the later phases of the penetration testing through the following sources:

1. Port Scanning.
2. Service Enumeration.

No sensitive data exposure issue was found during the reconnaissance phase. A full vulnerability scan was initiated to identify vulnerabilities that can potentially be exploited. Below table lists is defined scope of the engagement.

|  |  |
| --- | --- |
| # | IP Address |
| 1 | - |
| 2 | [-](https://localhost:8834/) |

The threat exposure was limited to External Network Black box pen-testing.

Following section provides detailed specific findings with associated recommendations to mitigate and/or remediate the open vulnerability.