Security Report

**CLIENT**

**Internal Network Security Assessment Report**

Table of Contents

[1. Document Map 4](#_Toc501216128)

[2. Introduction 4](#_Toc501216129)

[2.1 Scope 4](#_Toc501216130)

[2.2 Objective 7](#_Toc501216131)

[2.3 Time Duration 7](#_Toc501216132)

[2.4 Findings 7](#_Toc501216133)

[3. Executive Summary 7](#_Toc501216134)

[3.1 Summary 7](#_Toc501216135)

[3.2 Vulnerability Chart 8](#_Toc501216136)

[3.3 Findings by Category 8](#_Toc501216137)

[3.4 Table of Findings 9](#_Toc501216138)

[3.5 Attack Surface 9](#_Toc501216139)

[4. Detailed Vulnerability Information 11](#_Toc501216140)

[5. Conclusion 12](#_Toc501216141)

# Document Map

This report consists of the following sections:

* [**Introduction and Objectives**](#_2._Introduction)

In this section, we will discuss about the general information about project, including the scope duration and findings.

* [**Executive Summary**](#_4._Executive_Summary)

High level view of the information gathered during the assessment, usually using graphs or comparative numbers. This section is meant to provide a general understanding of the security status of the application.

* [**Vulnerability Chart**](#_4.2_Vulnerability_Chart)

This section is meant to provide a glance of the vulnerability found during security assessment. This sections hold overview of the found vulnerabilities sorted by their severity.

* [**Detailed Vulnerability Information**](#_5._Detailed_Vulnerability)

For each issue, this section includes all relevant details, including a detailed security advisory, and all variants, affected URLs, examinations, screenshots, and fix recommendations. This section is used both to educate on the nature and impact of the different issues, and to guide their remediation.

# Introduction

This report holds the results of a network security assessments performed on internal network of CLIENT by the XXX security team.

## Scope

CLIENT requested an internal penetration test and technical risk analysis for its corporate network on the 4th December, 2017. The assessment was to be done with no prior or internal knowledge of the infrastructure, systems or applications etc. scope of this assessment was limited to Internal IPs of 11 AWS regions. Following AWS region was in the scope.

|  |  |  |  |
| --- | --- | --- | --- |
| **Region** | **IP** | **Region** | **IPs** |
| Tokyo | 10.A.B.5 | Organ | 10.A.B.134 |
| 10.A.B.6 | 10.A.B.137 |
| 10.A.B.26 | 10.A.B.132 |
| 10.A.B.74 | 10.A.B.138 |
| 10.A.B.90 | X.Y.3.92, X.Y.3.69 |
| 10.A.B.135 | X.Y.3.162, X.Y.3.133 |
| 10.A.B.138 | X.Y.3.45, X.Y.3.5 |
| 10.A.B.140 | 10.A.B.37, 10.A.B.36 |
| 10.A.B.141 | 10.A.B.14, 10.A.B.4 |
| 10.A.B.12 | 10.A.B.23, 10.A.B.20 |
| 10.A.B.21 | 10.A.B.47 |
| 10.A.B.47 | 10.A.B.89 |
| 10.A.B.50 | 10.A.B.17 |
| 10.A.B.38 | 10.A.B.39 |
| 10.A.B.115 | 10.A.B.21 |
| X.Y.254.13 | 10.A.B.87 |
| X.Y.254.28 | 10.A.B.74 |
|  | 10.A.B.90 |
|  | X.Y.254.12 |
|  | X.Y.254.21 |
|  | 10.A.B.20 |
|  | 10.A.B.46 |
|  | 10.A.B2.10 |
| Sydney | X.Y.0.133 | Frankfart | X.Y.0.138 |
| X.Y.0.140 | X.Y.254.5 |
| X.Y.0.139 | X.Y.254.27 |
| X.Y.0.138 | X.Y.0.133 |
| X.Y.3.52, X.Y.3.5 | X.Y.0.137 |
| X.Y.3.121, X.Y.3.69 | X.Y.0.132 |
| X.Y.3.139, X.Y.3.133 | X.Y.0.18 |
| X.Y.0.9, X.Y.0.4 | X.Y.0.8 |
| X.Y.0.24, X.Y.0.20 | X.Y.1.62 |
| X.Y.0.36, X.Y.0.38 | X.Y.0.74 |
| X.Y.1.22 | X.Y.3.99 |
| X.Y.1.38 | X.Y.0.41 |
| X.Y.1.80 | X.Y.3.8 |
| X.Y.1.71 | X.Y.1.30 |
| X.Y.1.59 | X.Y.0.90 |
| X.Y.1.17 | X.Y.1.45 |
| X.Y.0.74 | X.Y.1.78 |
| X.Y.0.90 | X.Y.0.44 |
| X.Y.254.7 | X.Y.3.135 |
| X.Y.254.27 | X.Y.0.27 |
|  | X.Y.1.24 |
|  | X.Y.1.92 |
| Ireland | X.Y.254.29 | Ohio | X.Y.0.138 |
| X.Y.254.5 | X.Y.254.12 |
| X.Y.0.133 | X.Y.254.26 |
| X.Y.0.137 | X.Y.0.141 |
| X.Y.0.140 | X.Y.0.140 |
| X.Y.1.94 | X.Y.0.137 |
| X.Y.3.143 | X.Y.0.44 |
| X.Y.0.29 | X.Y.1.92 |
| X.Y.1.45 | X.Y.0.90 |
| X.Y.0.11 | X.Y.1.8 |
| X.Y.3.91 | X.Y.0.24 |
| X.Y.3.47 | X.Y.1.86 |
| X.Y.1.56 | X.Y.1.5 |
| X.Y.1.92 | X.Y.0.5 |
| X.Y.1.6 | X.Y.1.41 |
| X.Y.0.44 | X.Y.0.74 |
| X.Y.0.90 | X.Y.1.39 |
| X.Y.0.74 | X.Y.3.41 |
| X.Y.1.28 | X.Y.3.71 |
| X.Y.0.138 | X.Y.3.142 |
|  | X.Y.0.46 |
| Mumbai | X.Y.0.138 | Singapore | X.Y.0.138 |
| X.Y.254.8 | X.Y.254.11 |
| X.Y.254.30 | X.Y.254.29 |
| X.Y.0.137 | X.Y.0.136 |
| X.Y.0.136 | X.Y.0.133 |
| X.Y.0.133 | X.Y.0.132 |
| X.Y.0.14 | X.Y.1.24 |
| X.Y.3.83 | X.Y.1.38 |
| X.Y.0.5 | X.Y.1.17 |
| X.Y.3.53 | X.Y.0.30 |
| X.Y.1.36 | X.Y.3.70 |
| X.Y.1.12 | X.Y.0.7 |
| X.Y.0.90 | X.Y.0.27 |
| X.Y.0.26 | X.Y.3.50 |
| X.Y.1.47 | X.Y.0.74 |
| X.Y.0.74 | X.Y.0.90 |
| X.Y.1.11 | X.Y.1.56 |

## Objective

The objective of this assignment was to perform controlled attack and penetration activities to simulate an attack to assess the organizations immunity level, to assess the overall level of security of the Client internal network, discover weak links and provide recommendations and guidelines to vulnerable entities discovered.

This report relates to the security testing against the internal network from the perspective of an un-privileged user.

## Time Duration

The security assessment for performed for a period of ten days from 4th December 2017 to 15th December 2017.

## Findings

The XXX security team performs real-time security assessments on internal network. These assessments aim is to uncover any security issues in the assessed network, explain the impact and risks associated with the found issues, and provide guidance in the prioritization and remediation steps.

The security assessment revealed 0 critical severity security issues, 0 high severity security issue, 0 medium severity issues, 0 low severity issues and 0 informational severity issues. The consolidate summary of assessment has been presented in Executive Summary section. Additional information is contained within the Detailed Vulnerability Information section of this report.

# Executive Summary

## Summary

Overall, our assessment indicate that security postures of external network is very strong. We were not able to find any critical or high security risk. Pnly SSH ports open and a few SSL ports open for Alien Vault, RedHat Identity Management and Vormetric Data Security appliances. The SSH services running did not have any known vulnerability and the appliances were up to date on the vendor patches. Brute-force attacks on SSH did not reveal any weak credentials. The appliances did not have any SSL related vulnerabilities or weak credentials to the console.

## Vulnerability Chart

The discovered vulnerabilities table and chart illustrated below, provides a snapshot view of the number and severity of issues discovered during this security assessment.

**Critical** - This issue can impact the application severely and should be addressed immediately. Attackers can gain root or super user access or severely impact system operation.

**High** -This issue can cause a problem like unprivileged access and should be addressed as soon as possible.

**Medium** - This issue may pose a significant threat over a longer period of time.

**Low** - This issue is more likely an information disclosure and may be an acceptable threat.

**Info** - This is not a security problem but included as commentary on security controls examined.

## Findings by Category

Below given chart shows the vulnerability matrix based on category of vulnerabilities.

## Table of Findings

| S. No | Findings | Hosts (IPs) | Severity |
| --- | --- | --- | --- |
|  |  |  |  |

## 

## Attack Surface

The following Systems in the table below are visible and/or interactive targets within the test-scope. All those systems provide visibility or TCP and/or UDP services accessible.

|  |  |  |  |
| --- | --- | --- | --- |
| IP | Port | Service | Version |
| X.Y.0.14 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.23 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.44 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.140 | 80 | http | Apache httpd |
| X.Y.0.140 | 443 | ssl/http | Apache httpd |
| X.Y.0.142 | 80 | http | Apache httpd |
| X.Y.0.142 | 443 | ssl/http | Apache httpd |
| X.Y.0.29 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.44 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.133 | 80 | http | Apache httpd |
| X.Y.0.133 | 443 | ssl/http | Apache httpd |
| X.Y.0.140 | 80 | http | Apache httpd |
| X.Y.0.140 | 443 | ssl/http | Apache httpd |
| 10.A.B.37 | 22 | ssh | OpenSSH 7.4 (protocol 2.0) |
| 10.A.B.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| 10.A.B.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| 10.A.B.132 | 80 | http | Apache httpd |
| 10.A.B.132 | 443 | ssl/http | Apache httpd |
| 10.A.B.134 | 80 | http | Apache httpd |
| 10.A.B.134 | 443 | ssl/http | Apache httpd |
| X.Y.254.12 | 22 | ssh | Cisco SSH 1.25 (protocol 2.0) |
| X.Y.254.21 | 22 | ssh | Cisco SSH 1.25 (protocol 2.0) |
| X.Y.0.8 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.27 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.44 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.133 | 80 | http | Apache httpd |
| X.Y.0.133 | 443 | ssl/http | Apache httpd |
| X.Y.0.137 | 80 | http | Apache httpd |
| X.Y.0.137 | 443 | ssl/http | Apache httpd |
| X.Y.0.7 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.27 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.132 | 80 | http | Apache httpd |
| X.Y.0.132 | 443 | ssl/http | Apache httpd |
| X.Y.0.133 | 80 | http | Apache httpd |
| X.Y.0.133 | 443 | ssl/http | Apache httpd |
| X.Y.0.38 | 22 | ssh | OpenSSH 7.4 (protocol 2.0) |
| X.Y.0.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.133 | 80 | http | Apache httpd |
| X.Y.0.133 | 443 | ssl/http | Apache httpd |
| X.Y.0.139 | 80 | http | Apache httpd |
| X.Y.0.139 | 443 | ssl/http | Apache httpd |
| 10.A.B.5 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| 10.A.B.26 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| 10.A.B.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| 10.A.B.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| 10.A.B.135 | 80 | http | Apache httpd |
| 10.A.B.135 | 443 | ssl/http | Apache httpd |
| 10.A.B.141 | 80 | http | Apache httpd |
| 10.A.B.141 | 443 | ssl/http | Apache httpd |
| X.Y.0.12 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.23 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.132 | 80 | http | Apache httpd |
| X.Y.0.132 | 443 | ssl/http | Apache httpd |
| X.Y.0.133 | 80 | http | Apache httpd |
| X.Y.0.133 | 443 | ssl/http | Apache httpd |
| X.Y.0.11 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.30 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.133 | 80 | http | Apache httpd |
| X.Y.0.133 | 443 | ssl/http | Apache httpd |
| X.Y.0.137 | 80 | http | Apache httpd |
| X.Y.0.137 | 443 | ssl/http | Apache httpd |
| X.Y.0.5 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.24 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.44 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.137 | 80 | http | Apache httpd |
| X.Y.0.137 | 443 | ssl/http | Apache httpd |
| X.Y.0.141 | 80 | http | Apache httpd |
| X.Y.0.141 | 443 | ssl/http | Apache httpd |
| X.Y.0.26 | 22 | ssh | OpenSSH 6.6.1 (protocol 2.0) |
| X.Y.0.74 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.90 | 443 | ssl/http | Apache httpd 2.4.6 ((Red Hat Enterprise Linux) mod\_auth\_gssapi/1.5.1 mod\_nss/1.0.14 NSS/3.28.4 mod\_wsgi/3.4 Python/2.7.5) |
| X.Y.0.18 | 22 | ssh | OpenSSH 7.2 (protocol 2.0) |
| X.Y.0.18 | 443 | ssl/https | DSM |
| X.Y.0.18 | 8080 | http-proxy | DSM |
| X.Y.0.18 | 8443 | ssl/https-alt? |  |

# Detailed Vulnerability Information

There were no vulnerabilities found in the IP’s that were in scope. The Apache which seem to be out dated are not, they are back ported and do not have any vulnerability. Issues like weak SSL is also not present, the only devices on the network are appliances, and they do not have a known vulnerability. UDP scans over VPN did not yield any result.

# Conclusion

This analysis is based on the technologies and known threats as of the date of this report. To keep infrastructure secure following action should be taken.

1. Continue updating the appliances that are there in the network.
2. Block IPs when attacks such as SSH brute forcing and web credential brute forcing/enumeration are detected.