**** **State Bank of India (YONO)**

**Internal Segmentation Penetration Test Report**

Version 1.1

September 26, 2023

Statement of Confidentiality

This Confidential Information is being provided to **State Bank of India (YONO)** as a deliverable of this engagement. The sole purpose of this document is to provide you with the results of, and recommendations derived from this consulting engagement. Each recipient agrees that, prior to reading this document, it shall not distribute or use the information contained herein and any other information regarding **ControlCase** for any purpose other than those stated.

Table of Contents

[1 Executive Summary 4](#_Toc146635737)

[1.1 Introduction 4](#_Toc146635738)

[1.2 Result 4](#_Toc146635739)

[1.3 Steps for Remediation 4](#_Toc146635740)

[2 Approach, Methodology, Scope & Timing 5](#_Toc146635741)

[2.1 Approach 5](#_Toc146635742)

[2.2 Methodology Description 5](#_Toc146635743)

[2.3 Scope 7](#_Toc146635744)

[2.4 Project Team 8](#_Toc146635745)

[2.5 Penetration Timeline 8](#_Toc146635746)

[3 Details of Work Performed 9](#_Toc146635747)

[3.1 Reconnaissance and Documentation Review 9](#_Toc146635748)

[3.2 Rule-Set Review 10](#_Toc146635749)

[3.3 Port Scanning 11](#_Toc146635750)

[3.4 Observations 12](#_Toc146635751)

[3.5 Exploitation 12](#_Toc146635752)

# Executive Summary

## Introduction

**ControlCase** was engaged by **State Bank of India (YONO) to** perform Internal Segmentation Penetration Testing as per PCI DSS Requirement 11.3.4 of their internal network segment. PCI DSS Requirement 11.3.4 requires penetration testing to validate that segmentation controls and methods are operational, effective, and isolate all out-of-scope systems from systems in the Cardholder Data Environment (CDE).

Throughout all testing, **ControlCase** did not perform any tests that would deliberately lead to system outages or affect availability, such as denial-of-service tests.

The engagement began on **August 29, 2023,** and included multiple phases of testing, analysis and documentation. Segmentation test has been conducted from **State Bank of India (YONO)’s** internal network in order to replicate the scenario where attacker is having access of out-of-scope network.

## Result

ControlCase assessor observed that none of the systems from CDE scope are accessible from out-of-scope systems located in the **State Bank of India (YONO)’s** network. As a result, ControlCase concludes that **State Bank of India (YONO)** has **PASSED** the Internal Segmentation Penetration Test.

## Steps for Remediation

It is recommended to follow below best practices to implement proper segmentation as per PCI DSS 11.3.4, and pass the segmentation penetration testing:

* Rule-set review shall be done to verify the rules against the business requirements.
* All unused rules shall be removed
* All ACLs shall be configured in a way that they do not allow access to CDE from Out-of-Scope zone and vice versa.
* All changes in the network shall be done through change management process only by following segmentation policy and procedure.

# Approach, Methodology, Scope & Timing

## Approach

The segmentation check is performed by conducting tests used in the initial stages of a network penetration test (i.e., host discovery, port scanning, etc.). It verifies that all isolated LANs do not have access into the CDE. The penetration tester verifies that each network segment reported to be isolated from the CDE truly has no access to the CDE. For environments with a large number of network segments considered to be isolated from the CDE, a representative subset is used for testing to reduce the number of segmentation checks that need to be performed. Testing of each unique segmentation methodology is used to ensure that all security controls are functioning as intended.

## Methodology Description

**ControlCase** engineers follow the below given methodology while performing Internal Segmentation Penetration Testing. This methodology was created to promote a more consistent and thorough approach to segmentation penetration testing. The methodology is broken down into multiple phases as follows:

**Information Gathering and Analysis**

* **R**econnaissance – is an information gathering phase for the target IP address/IP addresses range in the scope of penetration test a well as about the company to understand the business.
* **D**ocumentation Review – is a process where all documents which are related with the segmentation process and implementation can be reviewed and the information can be used for further analysis.
* **R**ule-Set Review – helps to understand the traffic flow and rules configured for the different VLANs or segments. It is useful process to perform the segmentation penetration testing for large environment.

**Penetration Testing**

* **D**iscovery - aims at identifying all potential assets for investigation. The information gained through the discovery process creates a road map for the Investigation module.
* **I**nvestigation - utilizes the list of assets from the discovery process and thoroughly examines them for potential network as well as application vulnerabilities. The raw data resulting from the investigation must be analyzed and verified.
* **V**erification - tests vulnerabilities to ensure that all false positives and inaccuracies are removed from the raw investigation data. This often-neglected step ensures accuracy, painting a nearly complete picture of the security posture
* **E**xploitation - involves the in-depth analysis and execution of advanced testing techniques against all verified vulnerabilities. This effort completes the security picture and provides the information necessary to fully mitigate the findings.

**Reporting**

This provides an overview of the assessment methodology, vulnerability and threat assessment findings, recommendations and corrective actions and a copy of all data collected.

The above methodology was based on the best practices from Open-Source Security Testing Methodology Manual (OSSTMM), Open Web Application Security Project (OWASP) and NIST SP800-115.

**ControlCase** engineers used this methodology to perform the segmentation penetration test and to assess the security of the **State Bank of India (YONO)’s** internal network. Specifically, the following sections highlight the various tests that were used to complete each step of the methodology.

**Discovery**

**ControlCase** used the security tool NMAP to identify live services on the tested hosts in these subnets. NMAP is designed to identify live systems, as well as services being offered by those systems.

**Investigation**

As a follow-up to the information gathered, ControlCase used the security tool Nessus to perform checks for known vulnerabilities on the **State Bank of India (YONO)’s** internal network. Nessus is a security-scanning tool that checks for over 89000 different known vulnerabilities on networked systems. The Nessus tool performs extensive checks for vulnerabilities based upon predefined attack signature criteria. All tests were complemented with additional manual checks performed by ControlCase engineers to ensure accuracy of the results.

**Verification**

**ControlCase** manually verified the outputs of all security tools to determine if any results were inconsistent and warranted additional examination and review. Outputs from the various tools used were compared and crosschecked for accuracy. False positives and duplicate entries were removed from the Investigation results. Vulnerabilities that could be neither confirmed nor disputed were categorized separately for follow-up checks and review. Those vulnerabilities that could not be tested and confirmed without endangering the systems on which they exist are noted as well.

**Exploitation**

**ControlCase** performed exploitation attempts against any internal network host exhibiting vulnerability symptoms. These attempts included numerous manual exploitation attempts, information gathering and password guessing for well-known accounts using techniques developed and tested in our lab environment. All attacks were designed to limit the danger to services on the systems in order to prevent disruption of service during the testing.

## Scope

**State Bank of India (YONO)** provided **nine** (**09**) network segments for the internal network to be reviewed by **ControlCase**. The network segments which were provided are shown below:

**Internal IP/Subnet:**

|  |
| --- |
| **Network Range** |
| * 10.176.195.0/24 |
| * 10.176.194.0/24 |
| * 10.189.194.160/24 |
| * 10.191.177.0/24 |
| * 10.30.28.0/24 |
| * 10.191.177.0/24 |
| * 10.189.194.160/24 |
| * 10.30.28.0/24 |
| * 10.30.25.0/24 |

Below scope was determined by **State Bank of India (YONO)** as per the PCI Scope which is **Seven** (07) CDE zone and assessor verified the segmentation to PCI Scope from Two (02) out-of-scope VLAN locations.

**CDE In-scope Network Segments:**

|  |
| --- |
| **Network Range** |
| * 10.176.195.0/24 |
| * 10.176.194.0/24 |
| * 10.189.194.160/24 |
| * 10.191.177.0/24 |
| * 10.30.28.0/24 |
| * 10.191.177.0/24 |
| * 10.189.194.160/24 |

Testing was performed from the following network segments which are considered to be **Out-of-Scope** VLANs:

**Out-Of-Scope Network Segment:**

|  |
| --- |
| **Network Range** |
| * 10.30.28.254 |
| * 10.30.25.27 |

As per discussion with **State Bank of India (YONO)** team, above VLANs / IP were segregated and considered to be out of scope from PCI environment which should be isolated from CDE.

Attack perspective of the engagement was defined as internal user having access in the out-of-scope network and what he can see/exploit in the CDE. Type of testing was defined as Network Layer Penetration Test. Assessor performed manual as well as automated testing as part of assessment.

.

## Project Team

The engagement involved contributions from the following team members:

|  |  |
| --- | --- |
| ControlCase Team | **State Bank of India (YONO)** |
| Ninad Khade | Satyabrata Nath |
| Shashank Vaidya |  |

## 

## Penetration Timeline

The following table outlines key milestones during the penetration test:

| Penetration Timeline | |
| --- | --- |
| Date | Milestone |
| August 29, 2023 | Start of Test |
| September 26, 2023 | First Report Release Date |
| September 26, 2023, | Final Deliverable |

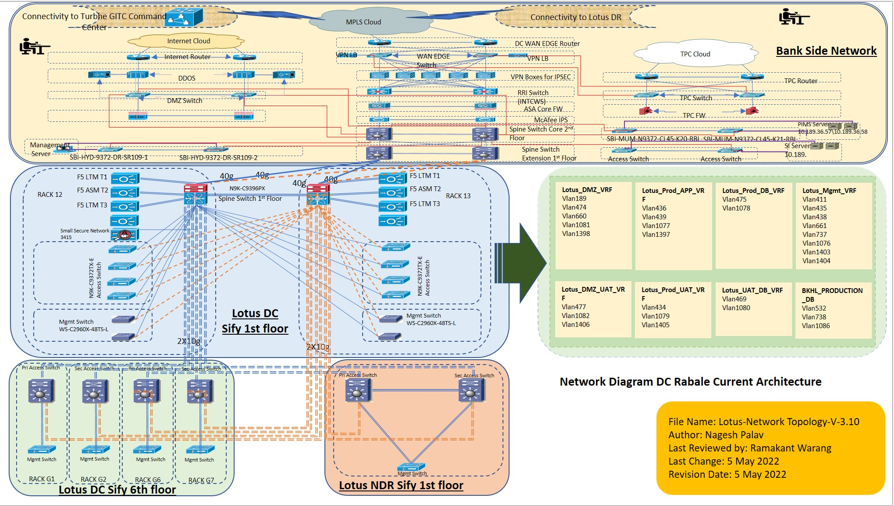
# Details of Work Performed

## Reconnaissance and Documentation Review

ControlCase assessor performed reconnaissance using various techniques for gathering information about the company and target scope where assessor observed that **t**he segregation is done based upon the network using firewalls with multi-layer protection. Each segment is separated with a firewall and access controls. The network is divided into multi VLANs as per the business requirements. The inter-VLAN traffic is further controlled by mapping these VLANs on the Firewall and creating access control lists to secure the traffic between the systems located within.

Assessor observed that documentation for network segmentation is in place which explains the segregation of network and systems based on their criticality. Each new implementation is done with management approval by following change management procedure.

Below is the network diagram which shows the LAN segregation and provided to the ControlCase while performing the assessment:



## Rule-Set Review

**State Bank of India (YONO)** is having number of network segments considered to be isolated from the CDE therefore a representative subset is used for testing to reduce the number of segmentation checks that need to be performed. However to ensure that all the all the subsets of CDE are isolated properly from out-of-scope network, assessor reviewed the firewall rule-sets/access controls which are in place.

To ensure comprehensiveness and identify gaps on security devices, ControlCase assessor followed types of checks mentioned but not limited to:

* Each rule is still required
* Only traffic that is authorized per policy is permitted, and all other traffic is denied by default,
* Rules enforce least privilege access, such as specifying only required IP addresses and ports,
* More specific rules are triggered before general rules,
* There are no unnecessary open ports that could be closed to tighten the perimeter security,
* The ruleset does not allow traffic to bypass other security defenses.

## Port Scanning

Port Scans attempts to connect to ports corresponding to services on the assessed hosts. By scanning ports which are available on the hosts, the engineers test potential weaknesses that can be further exploited.

Any ports that are found visible on the hosts should be verified if they are supposed to be opened there. Unexpected, opened ports should be closed. The firewall should also be checked if the listening ports on the hosts should expose to the Internet or to the internal networks. It is recommended to remove any unnecessary services and implement firewall rules to prevent exposure of any legitimate services that are not meant for the internal network.

It is recommended to remove any unnecessary ports/services as identified in port scanning results.

|  |  |  |
| --- | --- | --- |
| **Source Network (Out-of-Scope)** | **Destination Network (In-Scope-CDE)** | |
| 10.30.28.254 | | 10.176.195.0/24 |
| 10.176.194.0/24 |
| 10.189.194.0 /24 |
| 10.191.177.0/24 |
| 10.30.28.0/24 |
| 10.191.177.0/24 |
| 10.189.194.0/24 |
| 10.30.25.27 | | 10.176.195.0/24 |
| 10.176.194.0/24 |
| 10.189.194.0 /24 |
| 10.191.177.0/24 |
| 10.30.28.0/24 |
| 10.191.177.0/24 |
| 10.189.194.0/24 |

## Observations

**ControlCase** assessor verified and confirmed that the justification and mitigation timeline provided by SBI YONO is appropriate and acceptable.

## Exploitation

During the discovery phase, assessor was not able to identify any vulnerabilities associated with the subnets which are in CDE scope and accessible from Out-of-Scope VLANs, therefore this phase couldn’t be carried out.