**Shoppers Stop Limited PCI DSS**

**Internal Segmentation Penetration Test Report**

Version 1.1

August 03, 2022

Statement of Confidentiality

This Confidential Information is being provided to **Shoppers Stop Limited PCI DSS** 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](#_Toc110441538)

[1.1 Introduction 4](#_Toc110441539)

[1.2 Result 4](#_Toc110441540)

[1.3 Steps for Remediation 4](#_Toc110441541)

[2 Approach, Methodology, Scope & Timing 5](#_Toc110441542)

[2.1 Approach 5](#_Toc110441543)

[2.2 Methodology Description 5](#_Toc110441544)

[2.3 Scope 7](#_Toc110441545)

[2.4 Project Team 8](#_Toc110441546)

[2.5 Penetration Timeline 8](#_Toc110441547)

[3 Details of Work Performed 9](#_Toc110441548)

[3.1 Reconnaissance and Documentation Review 9](#_Toc110441549)

[3.2 Port Scanning 10](#_Toc110441550)

[3.3 Observations 11](#_Toc110441551)

[3.4 Exploitation 11](#_Toc110441552)

# Executive Summary

## Introduction

**ControlCase** was engaged by **Shoppers Stop Limited PCI DSS** 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 **June 16, 2022** and included multiple phases of testing, analysis and documentation. Segmentation test has been conducted from **Shoppers Stop Limited PCI DSS’s** internal network in order to replicate the scenario where attacker is having access of out-of-scope network.

## Result

ControlCase assessor observed that no systems of CDE segments are accessible from out-of-scope systems located in the **Shoppers Stop Limited PCI DSS’s** network. As a result, ControlCase concludes that **Shoppers Stop Limited PCI DSS** has **PASSED** the Internal Segmentation Penetration Test.

## Steps for Remediation

Since adequate network segmentation was observed as per PCI DSS 11.3.4, there are no remediation required. However, as a best practice and business as usual, consider following:

* Rule-set review shall be done to verify the rules against the business requirements.
* All unused rules shall be removed and all ACLs shall be configured in a way that they do not allow access to PCI zone (CDE) from Non-PCI zone/Out-of-Scope zone and vice versa.
* All changes in 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** assessors 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 **Shoppers Stop Limited PCI DSS’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 **Shoppers Stop Limited PCI DSS’s** internal network. Nessus is a security-scanning tool that checks for over 85361 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

**Shoppers Stop Limited PCI DSS** provided thirty-two (32) internal network segments to be reviewed by **ControlCase**. The network segments which were provided are shown below:

**Network Segments:**

|  |  |  |  |
| --- | --- | --- | --- |
| * 10.9.55.0/28 | * 172.16.228.0/24 | * 10.35.0.0/22 | * 10.9.59.0/27 |
| * 10.9.56.0/28 | * 172.16.250.0/24 | * 10.36.0.0/22 | * 172.16.232.0/21 |
| * 10.9.57.0/29 | * 172.16.251.0/24 | * 10.37.0.0/24 | * 172.16.247.0/27 |
| * 172.16.252.0/24 | * 192.168.18.0/25 | * 10.38.0.0/22 | * 172.16.248.0/27 |
| * 172.16.0.0/24 | * 192.168.100.0/25 | * 10.39.0.0/28 | * 172.16.253.0/24 |
| * 172.16.2.0/23 | * 192.168.105.0/28 | * 10.43.0.0/22 | * 192.168.19.0/25 |
| * 172.16.224.0/25 | * 192.168.107.0/28 | * 10.9.50.0/24 | * 192.168.20.0/28 |
| * 172.16.226.0/23 | * 10.1.1.0/24 | * 10.9.58.0/27 | * 223.31.76.0/28 |

Above scope was determined by **Shoppers Stop Limited PCI DSS** where it was observed that scope included following systems from **PCI Scope** (CDE and Non-CDE In Scope):

|  |  |  |  |
| --- | --- | --- | --- |
| * 10.9.55.0/28 | * 172.16.0.0/24 | * 172.16.228.0/24 | * 192.168.100.0/25 |
| * 10.9.56.0/28 | * 172.16.2.0/23 | * 172.16.250.0/24 | * 192.168.105.0/28 |
| * 10.9.57.0/29 | * 172.16.224.0/25 | * 172.16.251.0/24 | * 192.168.107.0/28 |
| * 172.16.252.0/24 | * 172.16.226.0/23 | * 192.168.18.0/25 |  |

As per the discussion with **Shoppers Stop Limited PCI DSS,** above VLANs were segregated and considered to be in PCI Scope which should be isolated from corporate network and any other network, therefore this scope was determined for segmentation penetration test. It has been noted that from the above VLANs following are the VLANs which are involved in **processing/transmission/storing of card data**:

|  |  |  |  |
| --- | --- | --- | --- |
| * 10.9.55.0/28 | * 10.9.56.0/28 | * 10.9.57.0/29 | * 172.16.252.0/24 |

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

|  |  |  |  |
| --- | --- | --- | --- |
| * 10.1.1.0/24 | * 10.9.59.0/27 | * 10.37.0.0/24 | * 172.16.247.0/27 |
| * 172.16.253.0/24 |  |  |  |

Attack perspective of the engagement was defined as internal user sitting in the corporate network and what he can see/exploit in the CDE. Type of testing was defined as Network Layer Penetration Test. There were no constraints (time, bandwidth limitations, etc.) put on testing. Testers performed manual as well as automated testing.

## Project Team

The engagement involved contributions from the following team members:

|  |  |
| --- | --- |
| ControlCase Team | **Shoppers Stop Limited PCI DSS Team** |
| Vishal Patil |  |
| Swapnil Kothawade |  |

## Penetration Timeline

The following table outlines key milestones during the penetration test:

| Penetration Timeline | |
| --- | --- |
| Date | Milestone |
| June 16, 2022 | Start Date |
| June 29, 2022 | Submission of Report for First Round of Testing |
| August 03, 2022 | Final Deliverable |

# Details of Work Performed

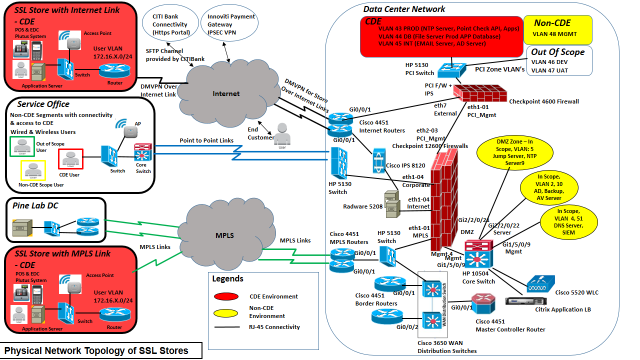
## Reconnaissance and Documentation Review

ControlCase assessor performed reconnaissance using various techniques for gathering information about the company and target scope.

The 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:



## 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 open 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.

Ports on which the connection attempts were made are shown below. The table consists of host IP addresses, protocol types, port numbers and the probable services. It is recommended to remove any unnecessary ports/services as identified below.

Following table shows the Port Scan Results. All other TCP/UDP ports which are not listed here were observed to be in state as FILTERED:

|  |  |  |  |
| --- | --- | --- | --- |
| Source Network (Out-of-Scope) | Destination Network (In scope-CDE) | Open Ports/Services | Shoppers Stop Limited PCI DSS Justification |
| 172.16.247.0/27 | 172.16.252.1 | TCP / 22 / SSH / OPEN | Since this Interface is Gateway, SSH is allowed |
| UDP / 161 / SNMP / OPEN | Since this Interface is Gateway, SNMP is allowed |
| 172.16.253.0/24 | 172.16.252.1 | UDP / 161 / SNMP / OPEN | Since this Interface is Gateway, SNMP is allowed |
| 10.1.1.0/24 | 10.9.55.0/28  10.9.56.0/28  10.9.57.0/29  172.16.252.0/24 | NO OPEN PORTS OBSERVED | Not Applicable |
| 10.9.59.0/27 |
| 10.37.0.0/24 |

## Observations

While performing the assessment, **ControlCase** assessor observed that some of the open as well as closed ports/services that were discovered within targeted PCI zone were filtered. For remaining open/closed ports, **ControlCase** has accepted the justification provided by **Shoppers Stop Limited PCI DSS.**

## Exploitation

During the discovery phase, assessor was not able to identify any observations/vulnerabilities associated with the segmentation between PCI scope and Non-PCI scope, therefore this phase couldn’t be carried out.