Vulnerability/Penetration Testing Report

For

ABCD Pvt Ltd

By

Maverick Quality Advisory Services

DOCUMENT DETAILS

Document Type	Penetration Testing Report
Project Name	Vulnerability Assessment and Penetration Testing
Document Version	1.0
Testing Date	
Report Date	
Authored by	MQAS
Reviewed by	MQAS

Disclaimer:
This report and any supplements are **HIGHLY CONFIDENTIAL** and may be protected by one or more legal privileges. It is intended solely for the use of the addressee identified in the report. This report is prepared based on the IT environment that prevailed in the approved period of assessment.

This report is not a guarantee or certification that all vulnerabilities have been discovered and reported in the findings. Subsequent reviews may report on previously unidentified findings or on new vulnerabilities. The samples screen shot should not be treated as the final vulnerabilities. Gaps which we have identified can also get replicated in any part of the Infrastructure. Client should ensure that Vulnerability Management Program should be adapted continuously rather than fixing just the issues identified within the areas which MQAS has highlighted.

Table of Contents

1. Introduction

This document summarizes the results of Vulnerability / Penetration tests conducted on the given IP's.

S. NO	IP address	Status
1	A.A.A.A	Reachable
2	B.B.B.B	Not Reachable

2. Scope

The aim of this project was to conduct the following activities

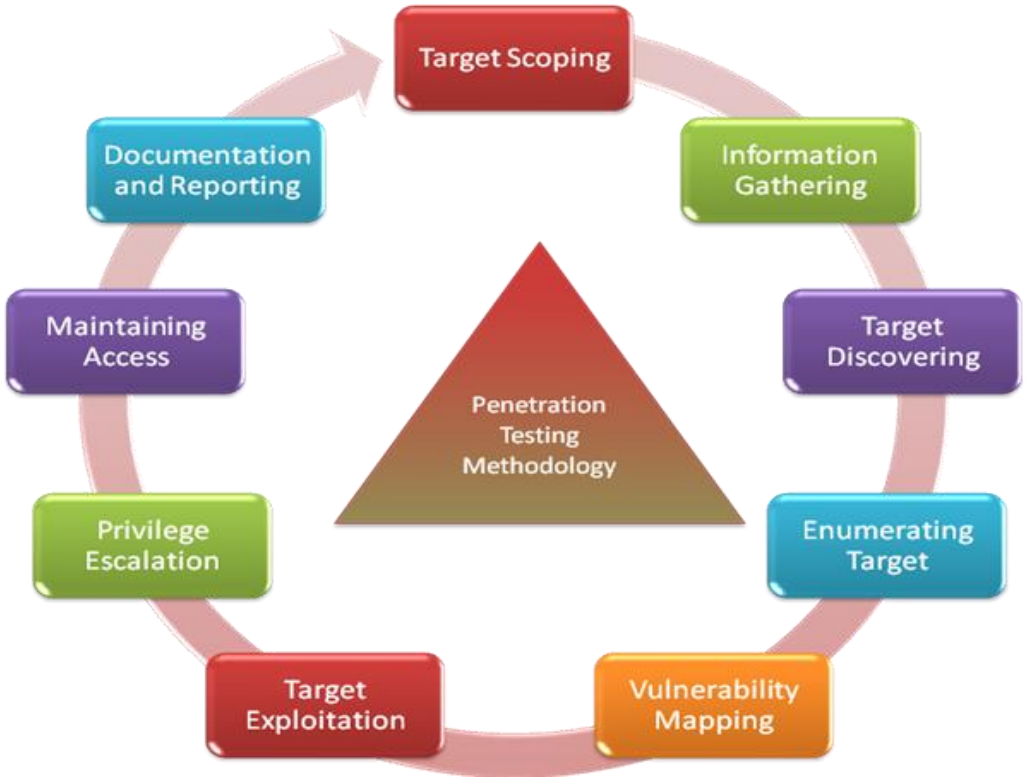
i. Gather Information
ii. Enumerate the network
iii. Establish Vulnerabilities
iv. Reporting details based on the information gathered

Range of IP Addresses / Application

Following range of IP addresses and Application given for Vulnerabilities Testing.

S. NO	IP address
1	A.A.A.A, B.B.B.B,….N.N.N.N

3. VAPT Methodology



3.1 Four Step Approach

3.1.1 Foot Print Analysis (Information Gathering)

The initial step is to gain preliminary understanding of the target machines e.g. Internet connectivity, IP address, packet routing path, operating system types and target network environment. Such information will help to build a target profile and provide useful pointers for subsequent stages.

3.1.2 Vulnerabilities Assessment

The second stage involves “probing” and “scanning” HEXAWARE systems to identify possible symptoms of vulnerabilities. These entails querying the target machines network port for network connection statistics, version number of running network services and verifying the security settings of the servers.

3.1.3 Exploitation Analysis

The third stage attempts to demonstrate any plausible security weaknesses by testing the exploitation of vulnerabilities to a certain extent. Data analysis and data correlation are also conducted here. The purpose of data analysis is to differentiate false alarms from true alarms i.e. the elimination of false positives. All scanning and/or penetration tools present a large amount of scanning results of which some are false alarms. Therefore, true alarms need to be sorted out to eliminate the false alarms. Data correlation is required to synergize raw data collected from various assessment tools into meaningful information concerning the suspected vulnerabilities.

3.1.4 Configuration Analysis

In this stage, different security parameters of the configuration are reviewed and the risk pertaining to that parameter is gauged based on the existing network environment. These security parameters are based on the best practices defined by the vendor and the industry.
Following are the risk levels of the various systems. The Risk level is divided in four categories:

Risk	Description
Critical	Critical vulnerabilities provide attackers with remote root or administrator capabilities. Malicious users have the ability to compromise the entire host. Easy to detect and exploit and result in large asset damage.
High	Exploitation of the vulnerability discovered on the system can directly lead to an attacker to information allowing them to gain privileged access (e.g., administrator or root) to the system. These issues are often difficult to detect and exploit but can result in large asset damage.
Medium	The vulnerability discovered on the system can directly lead to an attacker gaining non-privileged access (e.g., as a standard user) to the system or the vulnerability provides access that can be leveraged within one step to gain administrator-level access. These issues are easy to detect and exploit, but typically result in small asset damage.
Low	The vulnerability discovered on the system provides low-level, but sufficient data to the attacker that may be used to launch a more informed attack against the target environment. In addition, the vulnerability may indirectly lead to an attacker gaining some form of access to the system. These issues can be difficult to detect and exploit and typically result in small asset damage.

4. Summary of Findings

This report is based on following assumption

- On-site/Off-site Blackbox testing.
- No application testing.
- This report is based on tool-based testing and analysis is done with multiple level testing.
- The result of informational is not a part of this report, but can be provided, if required.

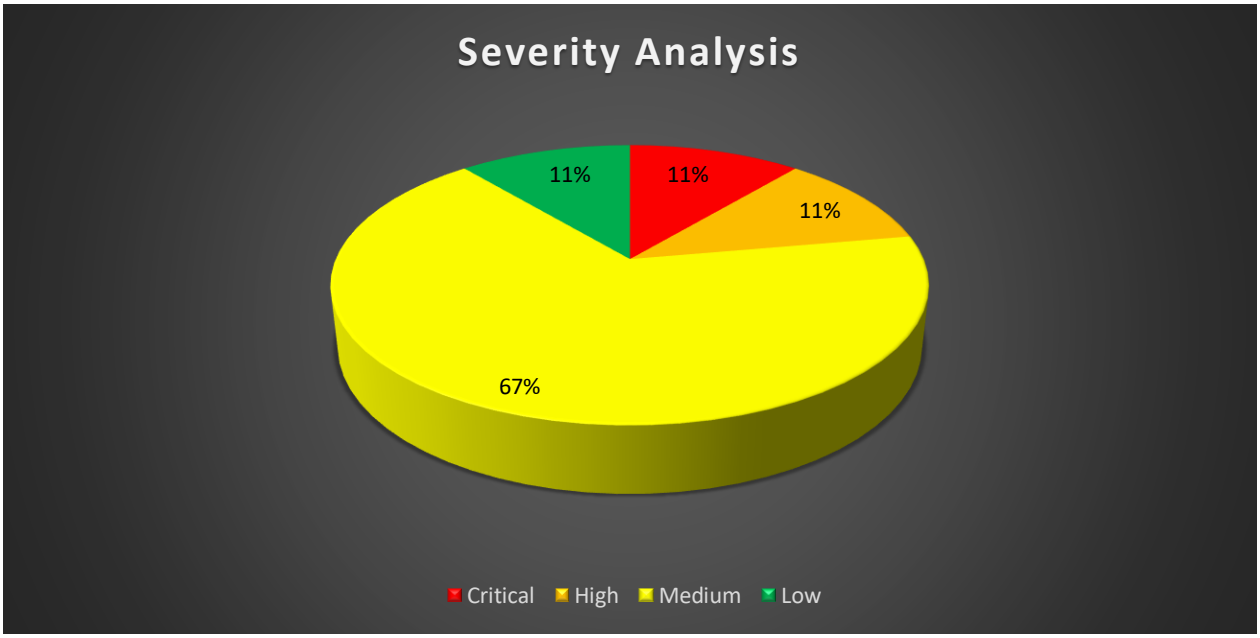
The severities of IPs are summarized in below:

IP Address	Finding	Severity
	Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)	Critical
	SSL Version 2&3 and TLS Version 1.0&1.1 Protocol Detection	High
	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness	Medium
	SMB Signing not Required	Medium
	SSL Certificate Cannot Be Trusted	Medium

	SSL Certificate Signed Using Weak Hashing Algorithm	Medium
	SSL Medium Strength Cipher Suites Supported (SWEET32)	Medium
	SSL RC4 Cipher Suites Supported (Bar Mitzvah)	Medium
	Terminal Services Encryption Level is Medium or Low	Low

IP Address	Service Running	State	IP Address	Service Running	State
	135/msrpc	open		8081/blackice-icecap	open
	445/microsoft-ds	open		49152/unknown	open
	2179/vmrdp	open		49153/unknown	open
	3389/ssl	open		49154/unknown	open
	8081/blackice-icecap	open		49155/unknown	open
	49153/unknown	open		49156/unknown	open
	49154	open		49157/unknown	open
	135/msrpc	open		49158/unknown	open
	445/microsoft-ds	open		http	open
	2179/vmrdp	open		135/msrpc	open
	3389/ssl	open		netbios-ssn	open
	8081/blackice-icecap	open		80/https	open
	49153	open		445/microsoft-ds	open
	49154	open		1433/ms-sql-s	open
	111/rpcbind	open		3389/ms-wbt-server	open
	135/msrpc	open		8081/blackice-icecap	open
	139/netbios-ssn	open		8100/xprint-server	open
	445/microsoft-ds	open		49152/unknown	open
	3389/ssl	open		49154/unknown	open
	6502/netop-rc	open		unknown	open

Row Labels	Count of Vulnerability
Critical	1
High	1
Medium	6
Low	1
Grand Total	**9**



5. Web Server Vulnerabilities

5.1 Vulnerability in Schannel Could Allow Remote Code Execution (2992611) (uncredentialed check)

Affected IP	:	IP
Severity	:	**Critical**
Description	:	The remote Windows host is affected by a remote code execution vulnerability.
Impact	:	The remote Windows host is affected by a remote code execution vulnerability due to improper processing of packets by the Secure Channel (Schannel) security package. An attacker can exploit this issue by sending specially crafted packets to a Windows server.
Recommendation	:	Microsoft has released a set of patches for Windows 2003, Vista, 2008, 7, 2008 R2, 8, 2012, 8.1, and 2012 R2.
Reference	:	

5.2 SSL Version 2 & 3 and TLS Version 1.0 & 1.1 Protocol Detection

Affected IP	:	IP 1	IP2
		IP 3	IP4
Severity	:	**High**	
Description	:	The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: • An insecure padding scheme with CBC ciphers. • Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography.	

Modern implementations of TLS 1.0 mitigate these problems, but newer versions of **TLS like 1.2 and 1.3** are designed against these flaws and should be used whenever possible.

PCI DSS v3.2 requires that TLS 1.0 be disabled entirely by June 30, 2018, except for POS POI terminals (and the SSL/TLS termination points to which they connect) that can be verified as not being susceptible to any known exploits.

The remote service accepts connections encrypted using TLS 1.1. TLS 1.1 lacks support for current and recommended cipher suites. Ciphers that support encryption before MAC computation, and authenticated encryption modes such as GCM cannot be used with TLS 1.1.
As of March 31, 2020, Endpoints that are not enabled for TLS 1.2 and higher will no longer function properly with major web browsers and major vendors. PCI DSS v3.2 still allows TLS 1.1 as of June 30, 2018, but strongly recommends the use of TLS 1.2/1,3.

Impact : The remote service encrypts traffic using a protocol with known weaknesses.

Recommendation : Consult the application's documentation to disable SSL 2.0,3.0 &TLS 1.0 & 1.1. Use TLS 1.2/1.3 (with approved cipher suites) or higher instead.

Reference :

5.3 Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness

Affected IP :

IP 1	IP2

Severity : **Medium**

Description : The remote version of the Remote Desktop Protocol Server (Terminal Service) is vulnerable to a man-in-the-middle (MiTM) attack. The RDP client makes no effort to validate the identity of the server when setting up encryption. An attacker with the ability to intercept traffic from the RDP server can establish encryption with the client and server without being detected. A MiTM attack of this nature would allow the attacker to obtain any sensitive information transmitted, including authentication credentials.

This flaw exists because the RDP server stores a hard-coded RSA private key in the mstlsapi.dll library. Any local user with access to this file (on any Windows system) can retrieve the key and use it for this attack.

Impact : It may be possible to get access to the remote host.

Recommendation :
- Force the use of SSL as a transport layer for this service if supported, or/and
- Select the 'Allow connections only from computers running Remote Desktop with Network Level Authentication' setting if it is available.