[SYBRID LOGO]

[DRAFT] Penetration Testing Report

Prepared by: Sybrid (Pvt.) Ltd.

Prepared for: XYZ, Ltd.

V1.0 February | 10 | 2021

[XYZ] – Company's LOGO

Sybrid (Pvt.) Ltd.

Email: --- **Web: www.sybrid.com**

Table of Contents

[SYBRID LOGO]

Document Control

Issue Control			
Document Reference	n/a	**Project Number**	n/a
Issue	v1.0	**Date**	10 February 2021
Classification	Confidential	**Author**	
Document Title			
Approved by			
Released by			

Owner Details	
Name	
Office/Region	
Contact Number	
E-mail	

Revision History			
Issue	**Date**	**Author**	**Comments**
1.0	10 February 2021	Ahmed Ajmal	n/a

[SYBRID LOGO]

Executive Summary

Test Scope

Results

Environment Tested	Testing Results
Internal Network	Status [**Critical**, **Low**, **High**]
Wireless Network	Status [**Critical**, **Low**, **High**]
Web Application	Status [**Critical**, **Low**, **High**]
Mobile Application	Status [**Critical**, **Low**, **High**]
Social Engineering Exercises	Status [**Critical**, **Low**, **High**]

Procedure

Recommendations

Testing Approach

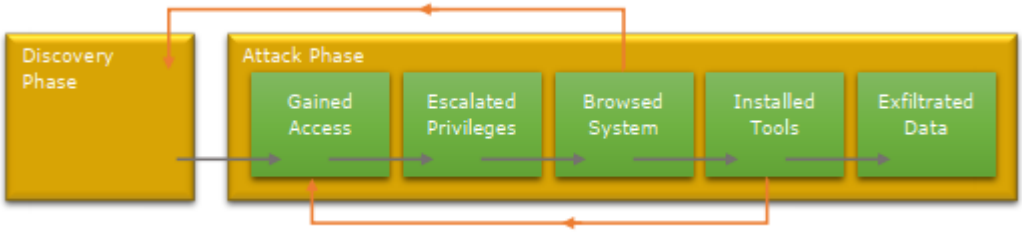
Overview

[Explanation of 4-Phases as per below figure]

1.
2.
3.
4.

Four-Stage
Penetration Testing Methodology

[Explanation of Discovery phase step-by-step]



Discovery & Reconnaissance

Validation & Exploitation

[SYBRID LOGO]

Internal Network Findings

Scope

Target IP Addresses
192.x.x.x
100.x.x.x
172.x.x.x

Network Penetration Testing Results

Result Classification	
Vulnerabilities Found	Status [**YES**, **NO**]
Exploited – Denial of Service (DoS)	Status [**YES**, **NO**]
Exploited – Elevation of Privileges (EoP)	Status [**YES**, **NO**]
Exploited – Remote Code Execution (RCE)	Status [**YES**, **NO**]
Exploit Persistent Achieved	Status [**YES**, **NO**]
Sensitive Data Exfiltrated	Status [**YES**, **NO**]
Overall Risk	Status [**High**, **Low**]

Services by Host and by Port

IP Addresses	TCP/UDP	Port	Service	Version
192.x.x.x	Tcp	22	ssh	OpenSSH 7.x (protocol 2.x)

Vulnerability Summary Table

#	Vulnerability Summary	Risk Level	Recommendations
1	[name & security control issue]	Status [**Critical**, **High**, **Medium**, **Low**]	[solutions]

Details

1. [Vulnerability 1 Name]	
Risk	Status [**Critical**, **High**, **Medium**, **Low**]
Location	**192.x.x.x: Port**
Description	

Observations

[Process]

[Images]

Impact

CVSS Score	Scale [1-10]
Confidentiality	
Integrity	
Availability	
Access Complexity	
Recommendations	
References	