WIXNIC

Client Company Name
Security Assessment Report

Business Confidential

Date: May, 17, 2021

Project: 898-21

Version: 1.0

Table of Contents

1 Confidentiality Statement

This document is the exclusive property of Client Company and CompanyName). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Client Company and CompanyName.

CompanyName may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

2 Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period. Time-limited engagements do not allow for a full evaluation of all security controls. CompanyName prioritized the assessment to identify the weakest security controls an attacker would exploit. CompanyName recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

3 Contact Information

Name	Title	Contact Information
Client Company		
John Smith	VP, Information Security (CISO)	Office: (555) 555-5555 Email: john.smith@demo.com
Jim Smith	IT Manager	Office: (555) 555-5555 Email: jim.smith@demo.com
Joe Smith	Network Engineer	Office: (555) 555-5555 Email: joe.smith@demo.com
Company Name		
John Smith	Lead Penetration Tester	Office: (555) 555-5555 Email: jsmith@company_name.com
Bob Smith	Penetration Tester	Office: (555) 555-5555 Email: bsmith@company_name.com
Rob Smith	Account Manager	Office: (555) 555-5555 Email: rsmith@company_name.com

Table 1: Contact

4 Assessment Overview

From June 20th, 2021 to June 29th, 2021, Client Company engaged CompanyName to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks. Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.
- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

4.1 Assessment Components

External Penetration Test

An external penetration test emulates the role of an attacker attempting to gain access to an internal network without internal resources or inside knowledge. A CompanyName engineer attempts to gather sensitive information through open-source intelligence (OSINT), including employee information, historical breached passwords, and more that can be leveraged against external systems to gain internal network access. The engineer also performs scanning and enumeration to identify potential vulnerabilities in hopes of exploitation.

5 Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Table 2: Severity Ratings

6 Scope

Assessment	Details
External Penetration Test	192.168.0.0/24, 192.168.1.0/24

Table 3: Scope

6.1 Scope Exclusions

Per client request, CompanyName did not perform any X attacks during testing.

Client Allowances

ClientCompany did not provide any allowances to assist the testing.

7 Executive Summary

CompanyName evaluated ClientCompany's external security posture through an external network penetration test from June 20th, 2019 to June 29th, 2019. By leveraging a series of attacks, CompanyName found critical level vulnerabilities that allowed full internal network access to the ClientCompany headquarter office. It is highly recommended that Client Company address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

8 Attack Summary

The following table describes how CompanyName gained internal network access, step by step:

Lorem ipsum

8.1 Security Strengths

SIEM alerts of vulnerability scans

During the assessment, lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed scelerisque sapien id risus tristique, vel molestie erat dapibus. Maecenas eleifend nunc sit amet purus aliquam, eu placerat sem dapibus. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque rhoncus commodo ultricies. Mauris quis quam ut tellus finibus lobortis. Donec dapibus leo a consectetur mollis. Donec nec mi euismod, vehicula tortor eu, feugiat massa. Curabitur at risus sed lorem fringilla auctor non pellentesque sem. Suspendisse urna arcu, sodales in risus sed, interdum accumsan mauris.

8.2 Security Weaknesses

8.2.1 Missing Multi-Factor Authentication

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed scelerisque sapien id risus tristique, vel molestie erat dapibus. Maecenas eleifend nunc sit amet purus aliquam, eu placerat sem dapibus.

Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque rhoncus commodo ultricies. Mauris quis quam ut tellus finibus lobortis. Donec dapibus leo a consectetur mollis. Donec nec mi euismod, vehicula tortor eu, feugiat massa. Curabitur at risus sed lorem fringilla auctor non pellentesque sem. Suspendisse urna arcu, sodales in risus sed, interdum accumsan mauris.

8.2.2 Weak Password Policy

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed scelerisque sapien id risus tristique, vel molestie erat dapibus. Maecenas eleifend nunc sit amet purus aliquam, eu placerat sem dapibus. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque rhoncus commodo ultricies. Mauris quis quam ut tellus finibus lobortis. Donec dapibus leo a consectetur mollis. Donec nec mi euismod, vehicula tortor eu, feugiat massa. Curabitur at risus sed lorem fringilla auctor non pellentesque sem. Suspendisse urna arcu, sodales in risus sed, interdum accumsan mauris.

8.2.3 Unrestricted Logon Attempts

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed scelerisque sapien id risus tristique, vel molestie erat dapibus. Maecenas eleifend nunc sit amet purus aliquam, eu placerat sem dapibus. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque rhoncus commodo ultricies. Mauris quis quam ut tellus finibus lobortis. Donec dapibus leo a consectetur mollis. Donec nec mi euismod, vehicula tortor eu, feugiat massa. Curabitur at risus sed lorem fringilla auctor non pellentesque sem. Suspendisse urna arcu, sodales in risus sed, interdum accumsan mauris.

8.2.4 Credentials Reuse

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed scelerisque sapien id risus tristique, vel molestie erat dapibus. Maecenas eleifend nunc sit amet purus aliquam, eu placerat sem dapibus. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque rhoncus commodo ultricies. Mauris quis quam ut tellus finibus lobortis. Donec dapibus leo a consectetur mollis. Donec nec mi euismod, vehicula tortor eu, feugiat massa. Curabitur at risus sed lorem fringilla auctor non pellentesque sem. Suspendisse urna arcu, sodales in risus sed, interdum accumsan mauris.

9 External Penetration Test Findings

Insufficient Lockout Policy - Outlook Web App

Description:	DC allowed unlimited logon attempts against their Outlook Web App (OWA) services. This configuration allowed brute force and password guessing attacks in which CompanyName used to gain access to ClientCompany internal network.
Impact:	Critical
System:	192.168.0.5
References:	NIST SP800-53r4 AC-17 - Remote Access NIST SP800-53r4 AC-7(1) - Unsuccessful Logon Attempts

Table 4: Vulnerability name

Exploitation Proof of Concept

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed scelerisque sapien id risus tristique, vel molestie erat dapibus. Maecenas eleifend nunc sit amet purus aliquam, eu placerat sem dapibus. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque rhoncus commodo ultricies. Mauris quis quam ut tellus finibus lobortis. Donec dapibus leo a consectetur mollis. Donec nec mi euismod, vehicula tortor eu, feugiat massa. Curabitur at risus sed lorem fringilla auctor non pellentesque sem. Suspendisse urna arcu, sodales in risus sed, interdum accumsan mauris.

Figure 1: Vulnerability Name Exploit in Action Phase 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed scelerisque sapien id risus tristique, vel molestie erat dapibus. Maecenas eleifend nunc sit amet purus aliquam, eu placerat sem dapibus.

Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque rhoncus commodo ultricies. Mauris quis quam ut tellus finibus lobortis. Donec dapibus leo a consectetur mollis. Donec nec mi euismod, vehicula tortor eu, feugiat massa. Curabitur at risus sed lorem fringilla auctor non pellentesque sem. Suspendisse urna arcu, sodales in risus sed, interdum accumsan mauris.

[redacted]

Figure 2: Vulnerability Name Exploit in Action Phase 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed scelerisque sapien id risus tristique, vel molestie erat dapibus. Maecenas eleifend nunc sit amet purus aliquam, eu placerat sem dapibus. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque rhoncus commodo ultricies. Mauris quis quam ut tellus finibus lobortis. Donec dapibus leo a consectetur mollis. Donec nec mi euismod, vehicula tortor eu, feugiat massa. Curabitur at risus sed lorem fringilla auctor non pellentesque sem. Suspendisse urna arcu, sodales in risus sed, interdum accumsan mauris.

[redacted]

Figure 3: Vulnerability Name Exploit in Action Result

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed scelerisque sapien id risus tristique, vel molestie erat dapibus. Maecenas eleifend nunc sit amet purus aliquam, eu placerat sem dapibus. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque rhoncus commodo ultricies. Mauris quis quam ut tellus finibus lobortis. Donec dapibus leo a consectetur mollis. Donec nec mi euismod, vehicula tortor eu, feugiat massa. Curabitur at risus sed lorem fringilla auctor non pellentesque sem. Suspendisse urna arcu, sodales in risus sed, interdum accumsan mauris.

Remediation

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Sed scelerisque sapien id risus tristique, vel molestie erat dapibus. Maecenas eleifend nunc sit amet purus aliquam, eu placerat sem dapibus. Orci varius natoque penatibus et magnis dis parturient montes, nascetur ridiculus mus. Pellentesque rhoncus commodo ultricies. Mauris quis quam ut tellus finibus lobortis. Donec dapibus leo a consectetur mollis. Donec nec mi euismod, vehicula tortor eu, feugiat massa. Curabitur at risus sed lorem fringilla auctor non pellentesque sem. Suspendisse urna arcu, sodales in risus sed, interdum accumsan mauris.