



# **Demo Company Security Assessment Findings Report**

Business Confidential

Date: March 22, 2023  
Project: 897-19  
Version 1.0

# Contents

<b>Confidentiality statement</b>	<b>2</b>
<b>Disclaimer</b>	<b>2</b>
<b>Contact information</b>	<b>2</b>
<b>Assessment overview</b>	<b>3</b>
<b>Assessment components</b>	<b>3</b>
External penetration test . . . . .	3
<b>Finding severity ratings</b>	<b>4</b>
<b>Scope</b>	<b>4</b>
Scope exclusions . . . . .	4
Client allowances . . . . .	4
<b>Executive summary</b>	<b>5</b>
Attack summary . . . . .	5
<b>Security strengths</b>	<b>6</b>
SIEM alerts of vulnerability scans . . . . .	6
<b>Security weaknesses</b>	<b>6</b>
Missing multi-factor authentication . . . . .	6
Weak password policy . . . . .	6
Unrestricted login attempts . . . . .	6
<b>Vulnerabilities by impact</b>	<b>6</b>
<b>External penetration test findings</b>	<b>6</b>
Insufficient Lockout Policy – Outlook Web App (Critical) . . . . .	6
Exploitation proof of concept . . . . .	6
Remediation . . . . .	6

## Confidentiality statement

This document is the exclusive property of Demo Company (DC) and TCM Security (TCMS). This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both DC and TCMS.

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

## 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. TCMS prioritized the assessment to identify the weakest security controls an attacker would exploit. TCMS recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

## Contact information

Name	Title	Contact information
<b>Demo Company</b>		
John Smith	VP, Information Security (CISO)	Office: (555) 555-5555 Email: <a href="mailto:john.smith@demo.com">john.smith@demo.com</a>
Jim Smith	IT Manager	Office: (555) 555-5555 Email: <a href="mailto:jim.smith@demo.com">jim.smith@demo.com</a>
Joe Smith	Network Engineer	Office: (555) 555-5555 Email: <a href="mailto:joe.smith@demo.com">joe.smith@demo.com</a>
<b>TCM Security</b>		
Heath Adams	Lead Penetration Tester	Office: (555) 555-5555 Email: <a href="mailto:hadams@tcm-sec.com">hadams@tcm-sec.com</a>
Bob Adams	Penetration Tester	Office: (555) 555-5555 Email: <a href="mailto:badams@tcm-sec.com">badams@tcm-sec.com</a>
Rob Adams	Account Manager	Office: (555) 555-5555 Email: <a href="mailto:radams@tcm-sec.com">radams@tcm-sec.com</a>

## Assessment overview

From May 20th, 2019 to May 29th, 2019, DC engaged TCMS 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.

## 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 TCMS 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.

## 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
<b>Critical</b>	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.
<b>High</b>	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.
<b>Moderate</b>	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.
<b>Low</b>	0.1 – 3.9	Vulnerabilities are non-exploitable but increase an organisation's attack surface. It is advised to form a plan of action and patch during the next maintenance window.
<b>Informational</b>	N/A	No known vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

## Scope

### Scope exclusions

Per client request, TCMS did not perform any Denial of Service attacks during testing.

### Client allowances

DC did not provide any allowances to assist the testing.

## Executive summary

TCMS evaluated DC's external security posture through an external network penetration test from 20 May 2019 to 29 May 2019. By leveraging a series of attacks, TCMS found critical vulnerabilities that allowed full internal network access to the DC headquarter office. It is highly recommended that DC address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and can be exploited without much effort.

## Attack summary

The following table describes how TCMS gained internal network access, step by step: [INSERT TABLE HERE]

## Security strengths

### SIEM alerts of vulnerability scans

During the assessment, the DC security team alerted TCMS engineers of detected vulnerability scanning against their systems. The team was successfully able to identify the TCMS engineer's attacker IP address within minutes of scanning and was capable of blacklisting TCMS from further scanning actions.

## Security weaknesses

### Missing multi-factor authentication

TCMS leveraged multiple attacks against DC login forms using valid credentials harvested through open-source intelligence. Successful logins included employee e-mail accounts through Outlook Web Access and internal access via Active Directory login on the VPN. The use of multi-factor authentication would have prevented full access and required TCMS to utilize additional attack methods to gain internal network access.

### Weak password policy

TCMS successfully performed password-guessing attacks against DC login forms, providing internal network access. A predictable password format of Summer2018! (season + year + special character) was attempted and successful.

### Unrestricted login attempts

During the assessment, TCMS performed multiple brute-force attacks against login forms found on the external network. For all logins, unlimited attempts were allowed, which permitted a successful login on the Outlook Web Access application.

## Vulnerabilities by impact

The following chart illustrates the vulnerabilities found by impact: [INSERT TABLE HERE]

## External penetration test findings

### Insufficient Lockout Policy – Outlook Web App (Critical)

#### Exploitation proof of concept

TCMS gathered historical breached data found in credentials dumps. The data amounted to 868 total account credentials (Note: A full list of compromised accounts can be found in "Demo Company-867-19 Full Findings.xlsx").

### Remediation

Item 1: VPN and OWA login with valid credentials did not require Multi-Factor Authentication (MFA). TCMS recommends DC implement and enforce MFA across all external-facing login services.

Item 2: OWA permitted unlimited login attempts. TCMS recommends DC restrict logon attempts

against their service.

Item 3: DC permitted a successful login via a password spraying attack, signifying a weak password policy. TCMS recommends the following password policy, per the Center for Internet Security (CIS):

- 14 characters or longer
- Use different passwords for each account accessed
- Do not use words and proper names in passwords, regardless of language

Item 4: OWA permitted user enumeration. TCMS recommends DC synchronize valid and invalid account messages.

Additionally, TCMS recommends that DC:

- Train employees on how to create strong passwords
- Check employee credentials against known breached passwords
- Discourage employees from using work e-mails and usernames as login credentials to other services unless absolutely necessary