Fortify Tech
Security Assessment Findings Report

Business Confidential

Date: May 8th, 2024
Project: DC-001
Version 1.0

Table of Contents

Confidentiality Statement

This document is the exclusive property of Demo Corp 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 Demo Corp and TCMS.

Demo Corp 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

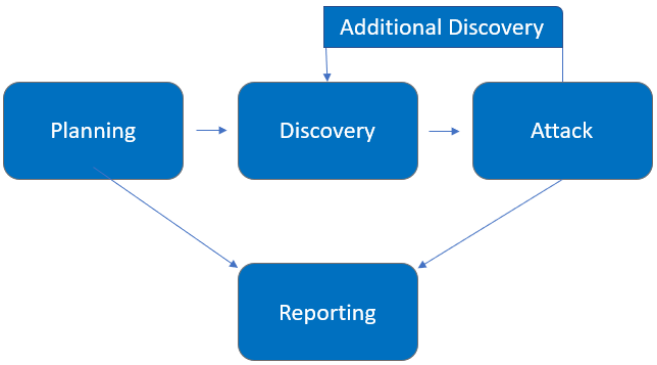
Name	Title	Contact Information
Mohammad Arkananta Radithya Taratugang	5027221003	Email: Aarkaradithya47@gmail.com
TCM Security		
Heath Adams	Lead Penetration Tester	Email: heath@tcm-sec.com

Assessment Overview

From February 22nd, 2021 to March 5th, 2021, Demo Corp engaged TCMS to evaluate the security posture of its infrastructure compared to current industry best practices that included an internal network 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

Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to identify potential host vulnerabilities and perform common and advanced internal network attacks, such as: LLMNR/NBT-NS poisoning and other man- in-the-middle attacks, token impersonation, kerberoasting, pass-the-hash, golden ticket, and more. The engineer will seek to gain access to hosts through lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

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.

Risk Factors

Risk is measured by two factors: Likelihood and Impact:

Likelihood

Likelihood measures the potential of a vulnerability being exploited. Ratings are given based on the difficulty of the attack, the available tools, attacker skill level, and client environment.

Impact

Impact measures the potential vulnerability's effect on operations, including confidentiality, integrity, and availability of client systems and/or data, reputational harm, and financial loss.

Scope

Assessment	Details
Internal Penetration Test	10.15.42.36

Scope Exclusions

Per client request, TCMS did not perform any of the following attacks during testing:

- Denial of Service (DoS)
- Phishing/Social Engineering

All other attacks not specified above were permitted by Demo Corp.

Client Allowances

Demo Corp provided TCMS the following allowances:

- Internal access to network via dropbox and port allowances

Executive Summary

TCMS evaluated Demo Corp's internal security posture through penetration testing from February 22nd, 2021 to March 5th, 2021. The following sections provide a high-level overview of vulnerabilities discovered, successful and unsuccessful attempts, and strengths and weaknesses.

Scoping and Time Limitations

Scoping during the engagement did not permit denial of service or social engineering across all testing components.

Time limitations were in place for testing. Internal network penetration testing was permitted for ten (10) business days.

Testing Summary

The network assessment evaluated Demo Corp's internal network security posture. From an internal perspective, the TCMS team performed vulnerability scanning against all IPs provided by Demo Corp to evaluate the overall patching health of the network. The team also performed common Active Directory based attacks, such as Link-Local Multicast Name Resolution (LLMNR) Poisoning, SMB relaying, IPv6 man-in-the-middle relaying, and Kerberoasting. Beyond vulnerability scanning and Active Directory attacks, the TCMS evaluated other potential risks, such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

The TCMS team discovered that LLMNR was enabled in the network (Finding IPT-001), which permitted the interception of user hashes via LLMNR poisoning. These hashes were taken offline and cracked via dictionary attacks, which signals a weak password policy (Finding IPT-005). Utilizing the cracked passwords, the TCMS team gained access to several machines within the network, which indicates overly permissive user accounts.

With machine access, and the use of older operating systems in the network (Finding IPT-009), the team was able to leverage WDigest (Finding IPT-003) to recover cleartext credentials to accounts. The team was also able to dump local account hashes on each machine accessed. The TCMS team discovered that the local account hashes were being re-used across devices (Finding IPT-002), which lead to additional machine access through pass-the-hash attacks.

Ultimately, the TCMS team was able to leverage accounts captured through WDigest and hash dumps to move laterally throughout the network until landing on a machine that had a Domain Administrator credential in cleartext via WDigest. The testing team was able to use this credential to log into the domain controller and compromise the entire domain. For a full walkthrough of the path to Domain Admin, please see Finding IPT-025.

In addition to the compromise listed above, the TCMS team found that users could be impersonated through delegation attacks (Finding IPT-004), SMB relay attacks were possible due to SMB signing being disabled (Finding IPT-007), and IPv6 traffic was not restricted, which could lead to LDAPS relaying and domain compromise (Finding IPT-006).

The remainder of critical findings relate to patch management as devices with critical out-of-date software (Finding IPT-008), operating systems (Finding IPT-009), and Microsoft RCE vulnerabilities (Findings IPT-010, IPT-011, IPT-012, IPT-013), were found to be present within the network.

The remainder of the findings were high, moderate, low, or informational. For further information on findings, please review the Technical Findings section.

Tester Notes and Recommendations

Testing results of the Demo Corp network are indicative of an organization undergoing its first penetration test, which is the case here. Many of the findings discovered are vulnerabilities within Active Directory that come enabled by default, such as LLMNR, IPv6, and Kerberoasting.

During testing, two constants stood out: a weak password policy and weak patching. The weak password policy led to the initial compromise of accounts and is usually one of the first footholds an attacker attempts to use in a network. The presence of a weak password policy is backed up by the evidence of our testing team cracking over 2,200 user account passwords, including a majority of the Domain Administrator accounts, through basic dictionary attacks.

We recommended that Demo Corp re-evaluates their current password policy and considers a policy of 15 characters or more for their regular user accounts and 30 characters or more for their Domain Administrator accounts. We also recommend that Demo Corp explore password blacklisting and will be supplying a list of cracked user passwords for the team to evaluate. Finally, a Privilege Access Management solution should be considered.

Weak patching and dated operating systems led to the compromise of dozens of machines within the network. We believe the number of compromised machines would have been significantly larger, however the TCMS and Demo Corp teams agreed it was not necessary to attempt to exploit any remote code execution (RCE) based vulnerabilities, such as MS17-010 (Finding IPT-012), as the domain controller had already been compromised and the teams did not want to risk any denial of service through failed attacks.

We recommend that the Demo Corp team review the patching recommendations made in the Technical Findings section of the report along with reviewing the provided Nessus scans for a full overview of items to be patched. We also recommend that Demo Corp improve their patch management policies and procedures to help prevent potential attacks within their network.

On a positive note, our testing team triggered several alerts during the engagement. The Demo Corp Security Operations team discovered our vulnerability scanning and was alerted when we attempted to use noisy attacks on a compromised machine. While not all attacks were discovered during testing, these alerts are a positive start. Additional guidance on alerting and detection has been provided for findings, when necessary, in the Technical Findings section.

Overall, the Demo Corp network performed as expected for a first-time penetration test. We recommend that the Demo Corp team thoroughly review the recommendations made in this report, patch the findings, and re-test annually to improve their overall internal security posture.

Key Strengths and Weaknesses

The following identifies the key strengths identified during the assessment:

1. Observed some scanning of common enumeration tools (Nessus)
2. Mimikatz detected on some machines
3. Service accounts were not running as domain administrators
4. Demo Corp local administrator account password was unique to each device

The following identifies the key weaknesses identified during the assessment:

1. Password policy found to be insufficient
2. Critically out-of-date operating systems and weak patching exist within the network
3. Passwords were observed in cleartext due to WDigest
4. LLMNR is enabled within the network
5. SMB signing is disabled on all non-server devices in the work
6. IPv6 is improperly managed within the network
7. User accounts can be impersonated through token delegation
8. Local admin accounts had password re-use and were overly permissive
9. Default credentials were discovered on critical infrastructure, such as iDRACs
10. Unauthenticated share access was permitted
11. User accounts were found to be running as service accounts
12. Service accounts utilized weak passwords
13. Domain administrator utilized weak passwords

Vulnerability Summary & Report Card

The following tables illustrate the vulnerabilities found by impact and recommended remediations:

Internal Penetration Test Findings

Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
Absence of Anti-SCRF Tokens	Moderate	
Content Security Policy (CSP) Header Not Set	High	
Missing Anti-clickjacking Header	Moderate	
Cookie No HttpOnly Flag	Low	
Cookie without SameSite Attribute	Low	
Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)	Low	
Server Leaks Version Information via "Server" HTTP Response Header Field	Low	
X-Content-Type-Options Header Missing	Low	
Information Disclosure - Suspicious Comments	Informational	
Modern Web Application	Informational	.
Session Management Response Identified	Informational	
User Controllable HTML Element Attribute (Potential XSS)	Informational	
Vulnerable to Terrapin	Moderate	

Technical Findings

Internal Penetration Test Findings

Absence of Anti-SCRF Tokens

Description:	No Anti-CSRF tokens were found in a HTML submission form. A cross-site request forgery is an attack that involves forcing a victim to send an HTTP request to a target destination without their knowledge or intent in order to perform an action as the victim.
Risk:	Moderate
System:	Web applications that rely on session cookies for authentication.
Tools Used:	OWASP
References:	https://cwe.mitre.org/data/definitions/352.html

Content Security Policy (CSP) Header Not Set

Description:	The product does not use or incorrectly uses a protection mechanism that provides sufficient defense against directed attacks against the product. This weakness covers three distinct situations. A "missing" protection mechanism occurs when the application does not define any mechanism against a certain class of attack. An "insufficient" protection mechanism might provide some defenses - for example, against the most common attacks - but it does not protect against everything that is intended. Finally, an "ignored" mechanism occurs when a mechanism is available and in active use within the product, but the developer has not applied it in some code path.
Risk:	High
System:	All
Tools Used:	OWASP
References:	https://developer.mozilla.org/en-US/docs/Web/Security/CSP/Introducing_Content_Security_Policy https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Shee

	t.html http://www.w3.org/TR/CSP/ http://w3c.github.io/webappsec/specs/content-security-policy/csp-specification.dev.html http://www.html5rocks.com/en/tutorials/security/content-security-policy/ http://caniuse.com/#feat=contentsecuritypolicy http://content-security-policy.com/

Missing Anti-clickjacking Header

Description:	The response does not include either Content-Security-Policy with 'frame-ancestors' directive or X-Frame-Options to protect against 'ClickJacking' attacks.
Risk:	Moderate
System:	- 10.15.42.7 - 10.15.42.36:8888
Tools Used:	OWASP
References:	https://cwe.mitre.org/data/definitions/1021.html

Cookie No HttpOnly Flag

Description:	A cookie has been set without the HttpOnly flag, which means that the cookie can be accessed by JavaScript. If a malicious script can be run on this page then the cookie will be accessible and can be transmitted to another site. If this is a session cookie then session hijacking may be possible
Risk:	Low
System:	- 10.15.42.7
Tools Used:	OWASP
References:	https://cwe.mitre.org/data/definitions/1004.html

Cookie without SameSite Attribute

Description:	A cookie has been set without the SameSite attribute, which means that the cookiecan be sent as a result of a 'cross-site' request. The SameSite attribute is an effectivecounter measure to cross-site request forgery, cross-site script inclusion, and timing attacks.
Risk:	Low
System:	- 10.15.42.7
Tools Used:	OWASP

References:	https://cwe.mitre.org/data/definitions/1275.html

Server Leaks Information via "X-Powered-By" HTTP Response Header Field(s)

Description:	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Risk:	Low
System:	- 10.15.42.7
Tools Used:	OWASP
References:	https://cwe.mitre.org/data/definitions/200.html

Server Leaks Information via "Server" HTTP Response Header Field(s)

Description:	The web/application server is leaking information via one or more "X-Powered-By" HTTP response headers. Access to such information may facilitate attackers identifying other frameworks/components your web application is reliant upon and the vulnerabilities such components may be subject to.
Risk:	Low
System:	- 10.15.42.7
Tools Used:	OWASP
References:	https://cwe.mitre.org/data/definitions/200.html