TROJENT

Demo Corp

Security Assessment Report

DATE: August 25, 2025
PROJECT: Demo Corp-2025
VERSION: 1.0

TABLE OF CONTENTS

Legal 1
Statement of confidentiality 1.1
Non-disclosure agreement 1.2
Permission to test 1.3
Disclaimer 1.4

Contacts 2

Assessment overview & Mythodology 3

Executive summary 4
Scoping and time limitations 4.1
Internal testing summary 4.2
Key strengths and weaknesses 4.3
Scope 5
Rules of engagements 5.1
Client allowances 5.2

Severity ratings 6

Vulnerability summary & Report card 7
Internal testing findings 7.1

Technical findings 8
Finding IPT-01: Insufficient Encryption- Deprecated Encryption Standard (Low)
Finding IPT-02: Insufficient Hardening - Insecure HTTP Response (Low)
Finding IPT-03: Misconfigured Access and Permissions - FTP Anonymous (Low)

LEGAL

Statement of Confidentiality

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

Non-Disclosure Agreement

A legally binding contract that establishes a confidential relationship between the client and the security tester. It ensures that sensitive information shared during the engagement or discovered during testing—such as critical system vulnerabilities—remains private and is not disclosed to unauthorized third parties.

Permission to test

The explicit, written authorization granted by a system owner to a security tester to perform simulated attacks on their digital infrastructure.

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

Contacts

Name	Title	Contact Information
DemoCorp		
John Doe	Cybersecurity Manager	j.doe@democorp.com
Trojent		
Abdulrahman Saud	Red Team Lead	a.saud@trojent.com

ASSESSMENT OVERVIEW

From February 22nd, 2021 to March 5th, 2021, Demo Corp engaged TROJENT 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.

EXECUTIVE SUMMARY

Overview

TROJENT 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 & 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, TROJENT performed vulnerability scanning against all IPs provided by Demo Corp to evaluate the overall patching health of the network. It 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, TROJENT 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.

TROJENT also 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 tester 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 tester was also able to dump local account hashes on each machine accessed and 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, TROJENT 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.

INTERNAL TESTING SUMMARY

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 & 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

SCOPE

Assessment	Details
Internal Penetration Test	IP Range: 10.192.x.x/24

Rules of Engagement

Per client request, TROJENT did not perform any of the following attacks during testing:
1. Denial of Service (DoS)
2. Phishing/Social Engineering
3. Bruteforcing
4. Resource altering

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

Client Allowances

Demo Corp provided TROJENT the following allowances:
1. Internal access to network and port allowances

SEVERITY RATINGS

How Its Calculated

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

Name	CVSS 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.

VULNERABILITY SUMMARY & REPORT CARD

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

Internal Penetration Testing Findings

13	5	6	0	1
Critical	High	Moderate	Low	Informational

Finding	Severity	Recommendation
Internal Penetration Test		
IPT-001: Insufficient LLMNR Configuration	Critical	Disable multicast name resolution via GPO.
IPT-002: Security Misconfiguration – Local Admin Password Reuse	Critical	Utilize unique local admin passwords and limit local admin users via least privilege.
IPT-003: Security Misconfiguration – Wdigest	Critical	Disable WDigest via GPO.
IPT-017: Default Credentials on Web Services	High	Change default credentials or disable unused accounts.
IPT-018: Insufficient Hardening – Listable Directories	High	Restrict access and conduct web app assessment.
IPT-019: Unauthenticated SMB Share Access	Moderate	Disable SMB share or require authentication.
IPT-020: Insufficient Patch Management – SMBv1	Moderate	Upgrade to SMBv3 and apply latest patching.
IPT-021: IPMI Hash Disclosure	Moderate	Disable IPMI over LAN if it is not needed.
IPT-022: Insufficient SNMP Community String Complexity	Moderate	Disabled SNMP if not required.
IPT-023: Insufficient Data in Transit Encryption - Telnet	Moderate	Migrate to TLS protected protocols.
IPT-024: Insufficient Terminal Services Configuration	Moderate	Enable Network Level Authentication (NLA) on the remote RDP server.
IPT-025: Steps to Domain Admin	Informational	Review action and remediation steps.

TECHNICAL FINDINGS

Finding IPT-008: Insufficient Patch Management – Software (Critical)

Description	Demo Corp permitted various deprecated software in their network. This includes: • Apache version < 2.4.46 • Apache Tomcat version < 7.0.100, 8.5.51, 9.0.31 • Cisoco AireOS version 8.5.151.10 • CodeMeter version 3.05 (5.21.1478.500) • Dropbear SSH Server version 2015.68 • Dell iDRAC7 version 2.63.60.62.01 • Dell iDRAC8 version 2.63.60.61.06 • Dell iDRAC9 version 3.36.36.36.21 • ESXi version 5.5 • ESXi version 6.5 build 15256549 • Flexera FlexNet Publisher version 11.16.0 • IIS version 7.5 • ISC BIND version 9.6.2-P2 • Microsoft DNS Server version 6.1.7601.24261 • Microsoft SQL Server version 11.0.6594.0 • Netatalk OpenSession version < 3.1.12 • PHP version < 7.3.11 • Rockwell Automation RSLinx Classic Above lists all critical and high-rated deprecated software, the majority of which permit serious vulnerabilities, such as remote code execution. For a full patching list, please review the provided Nessus scan documentation.
Risk	Likelihood: High – An attacker can discover these vulnerabilities with basic tools. Impact: Very High – If exploited, an attacker could possibly gain full remote code execution on or deny service to a system.
Tools	Nessus
References	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Remediation

Update to the latest software version. For a full list of vulnerable systems, versions, and patching requirements, please see the below document.

TECHNICAL FINDINGS

Finding IPT-010: Insufficient Patching – MS08-067 - ECLIPSEDWING/NETAPI (Critical)

Description	Demo Corp permitted an unpatched system on the internal network that is vulnerable to MS08-067. TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk	Likelihood: High – Considered one of the most exploited vulnerabilities in Microsoft Windows as it ships natively with Windows XP. Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
Systems	10.x.x.x
Tools	Nessus, Nmap
References	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence

```
└─# nmap -p445 10.[redacted] --script smb-vuln-ms08-067
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 20:33 EST
Nmap scan report for [redacted] (10.[redacted])
Host is up (0.014s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds

Host script results:
| smb-vuln-ms08-067:
|   VULNERABLE:
|   Microsoft Windows system vulnerable to remote code execution (MS08-067)
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2008-4250
|           The Server service in Microsoft Windows 2000 SP4, XP SP2 and SP3, Server 2003 SP1 and SP2,
|           Vista Gold and SP1, Server 2008, and 7 Pre-Beta allows remote attackers to execute arbitrary
|           code via a crafted RPC request that triggers the overflow during path canonicalization.
|
|     Disclosure date: 2008-10-23
|     References:
|       https://technet.microsoft.com/en-us/library/security/ms08-067.aspx
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-4250

Nmap done: 1 IP address (1 host up) scanned in 10.55 seconds
```

Figure 10: Unpatched MS08-067

Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching MS08-067 can be found here: https://docs.microsoft.com/en-us/security-updates/SecurityBulletins/2008/ms08-067

TECHNICAL FINDINGS

Finding IPT-011: Insufficient Patching – MS12-020 – Remote Desktop RCE (Critical)

Description	Demo Corp permitted an unpatched system on the internal network that is vulnerable to MS12-020. TCM Security confirmed that the vulnerability likely exists but did not attempt the exploit to prevent any denial of service.
Risk	Likelihood: High – The vulnerability is easily discoverable and exploitable with open-source tools. Impact: Very High – If exploited, an attacker gains code execution as the system user. An adversary will require additional techniques to obtain domain administrator access.
Systems	10.x.x.x
Tools	Nessus, Nmap
References	NIST SP800-53 r4 MA-6 – Timely Maintenance NIST SP800-53 r4 SI-2 – Flaw Remediation

Evidence

```
┌──(root㉿kali)-[~]
└─# nmap -p3389 10.[redacted] --script rdp-vuln-ms12-020
Starting Nmap 7.91 ( https://nmap.org ) at 2021-03-03 20:35 EST
Nmap scan report for [redacted] (10.[redacted])
Host is up (0.014s latency).

PORT     STATE SERVICE
3389/tcp open  ms-wbt-server
| rdp-vuln-ms12-020:
|   VULNERABLE:
|   MS12-020 Remote Desktop Protocol Denial Of Service Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0152
|     Risk factor: Medium  CVSSv2: 4.3 (MEDIUM) (AV:N/AC:M/Au:N/C:N/I:N/A:P)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to cause a denial of service.
|
|     Disclosure date: 2012-03-13
|     References:
|       http://technet.microsoft.com/en-us/security/bulletin/ms12-020
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0152
|
|   MS12-020 Remote Desktop Protocol Remote Code Execution Vulnerability
|     State: VULNERABLE
|     IDs:  CVE:CVE-2012-0002
|     Risk factor: High  CVSSv2: 9.3 (HIGH) (AV:N/AC:M/Au:N/C:C/I:C/A:C)
|           Remote Desktop Protocol vulnerability that could allow remote attackers to execute arbitrary code on the targeted system.
|
|     Disclosure date: 2012-03-13
|     References:
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0002
|_      http://technet.microsoft.com/en-us/security/bulletin/ms12-020
```

Figure 11: Unpatched MS12-020

Remediation

Apply the appropriate Microsoft patches to remediate the issue. More information on patching MS12-020 can be found here: https://docs.microsoft.com/en-us/security-updates/securitybulletins/2012/ms12-020

END OF REPORT

This concludes our penetration testing report for Demo corp, if further scan information is needed, it will be provided as raw data for the client.

THANK YOU