eCPPTv2 Penetration Testing Report

Demo Corp

By

Elliot Alderson

Versión 1.0

Este documento es confidencial y contiene información sensible.
No debería ser impreso y compartido con terceras entidades.

08 de Marzo del 2024

Table of Contents

1. Confidentiality Statement

This document is the exclusive property of Demo Corp and Elliot Alderson. 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 Elliot Alderson.

Demo Corp may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compilance.

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 evaluations of all security controls. Elliot Alderson prioritized the assessment to identify the weakest security controls an attacker would exploit. Elliot Alderson 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
Demo Corp		
Demo Corp	CISO 2	Office: `(555) 555-5555` Email: `john.smith@demo.com`
Elliot Alderson		
Elliot Alderson	Lead Penetration Tester	Email: `elliot.alderson@proton.me`

4. Assessment Overview

From 08 de Marzo del 2024 to 12 de Marzo del 2024, Demo Corp engaged Elliot Alderson to evaluate the security posture of its infraestrucure compared to current industry best practices that included an internal network penetration test. All testing performed is based on the NIST SP 800-115 Techinical Guide to Information Security TEsting and Assessment, OWASP Testing Guide (v4), and customized testing frameworks.

Phases of penetration testing activities include the following:

1. **Planning:** Customer goals are gathered and rules of engaggment obtained.
2. **Discovery:** Perform scanning and enumeration to identify potential vulnerabilities, weak, areas, and exploits.
3. **Attack** Confirm potential vulnerabilities through explotation and perform additional discovery upon new access.
4. **Reporting:** Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.

5. Assessment Components

5.1. Internal Penetration Test

An internal penetration test emulates the role of an attacker from inside the network. An engineer will scan the network to idenfiy 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 trough lateral movement, compromise domain user and admin accounts, and exfiltrate sensitive data.

6. Finding Severity Raitings

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	9-10	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediateley.
High	7-8	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	4-6	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	1-3	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advice to form a plan of action and patch during the next maintenance window.
Informational	N/A	No vulnerability exists. Additional information is provided regarding itemas noticed during testing, strong controls, and additional documentation.

7. Risk Factors

Risk is measured by two factors **Likelihood** y **Impact**

7.1. Likelihood

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

7.2. Impact

Impact measures the potential vulnerabilities effect on operations, including confidentiality, integrity, and availabiility of client systems and / or data, reputational harm, and financial loss.

8. Scope

Assessment	Details
Internal Penetration Test	10.10.10.0/24, 10.10.10.5

8.1. Scope Exclusions

During the auditing process, and at the request of the client Demo Corp, it is strictly forbidden to carry out any of the following activities:

- Performing tasks that may cause a denial of service (DoS) or affect the availability of the exposed services.
- Deleting files resident on the server once it has been compromised.

8.2. Client Allowances

Demo Corp provided Elliot Alderson with the following concessions:

- Identifying vulnerable ports and services.
- Exploiting the vulnerabilities found.
- Gaining access to the server by exploiting the identified vulnerable services.
- Enumerating potential avenues to escalate privileges in the system once it has been compromised.

9. Executive Summary

Elliot Alderson evaluó la postura de seguridad del examen de **Demo Corp** mediante una prueba de penetración de tipo interna desde **08 de Marzo del 2024** hasta el **12 de Marzo del 2024**. Al aprovechar una serie de ataques, Elliot Alderson encontró vulnerabilidades de nivel crítico que comprometieron el entorno del examen y los objetivos de aprobación. Se recomienda encarecidamente que **Demo Corp** aborde estas vulnerabilidades lo antes posible, ya que son fácilmente detectables a través de reconocimiento básico y son explotables sin mucho esfuerzo.

10. Testing Summary

En esta sección, se deben describir las vulnerabilidades identificads y proporciona información básica sobre el impacto de la explotación.

11. Vulnerability Summary & Report Card

The following table ilustrate the vulnerabilities found by impact and recommended remendations:

11.1. Internal Penetration Testing Findings

0	0	0	0	0
Critical	High	Moderate	Low	Informational

Total of Vulnerabilities	1

Finding	**Severity**	**Recommendation**
Internal Penetration Test		
Vulnerability 001: Insufficient Patch Management - Samba 3.0.20 `Username` map script Command Execution - CVE-2007-2447	**Critical**	Upgrade the Samba to the latest version
Vulnerability 002: Insufficient Hardening - Anonymous permitted	**High**	Disable the anonymous login on ftp
Vulnerability 003: Insufficient Hardening Samba READ/WRITE Permissions allowed	**High**	Disable the READ/WRITE for the tmp folder without getting any password
Vulnerability 004: Insufficient Patch Management - vsftpd 2.3.4 Backdoor Command Execution - CVE-2011-2523	**Moderate**	Disable the READ/WRITE for the tmp folder without getting any password

12. Techinical findings

12.1. Target - 10.10.10.5

12.1.1. Vulnerability 001 - Local File Inclusion

Description:	Breve descripción sobre que concisite la vulnerabilidad explotada.
Severity:	Ej. Critical
Vulnerability ID:	(OSVDB, Bugtraq ID, CVE) Ej. CVE-2017-0144
Risk:	En esta sección, debemos indicar la probabilidad (Likelihood) y el impacto (Impact).
Tools Used:	Listar las herramientas utilizadas al momento de realizar el ataque. Ej. Burpsuite
References:	Enlaces a recursos utilizados para realizar el ataque o que sirvan para complementar la descripción. Enlace a la referencia de Clasificación de la vulnerabilidad: Ej. https://cve.mitre.org/cgi-bin/cvename.cgi?name=cve-2017-0144

Evidence

En esta sección debemos indicar el paso a paso de la explotación, complementando la misma con capturas de imágenes. Como si fuese un mini writeup.

Recommendations En esta sección debemos detallar las recomendaciones/medidas necesarias para resolver/-mitigar la vulnerabilidad.

13. Conclusion

Se han detectado vulnerabilidaes cr´ıticas que pueden suponer un riesgo desde el punto de vista de la seguridad. Han sido encontradas vulnerabilidades las cuales permitieron vulnerar la integridad del servidor, consiguiendo acceso al mismo como el usuario ’apache’. Esto ha sido posible debido a una versi´on vulnerable de PhpMyAdmin existente en uno de los subdominios identificados durante el proceso de reconocimiento bajo el dominio ’votenow.local’. Se recomienda encarecidamente aplicar las contramedidas recomendadas para corregir estas vulnerablidades lo antes posible, dado que de lo contrario se podr´ıa comprometer la seguridad del servidor y poner en riesgo la integridad de todos los datos almacendos en este.

14. Appendices

14.1. Detailed technical information

14.2. Glossary of terms

14.3. References

Last Page