

**Análisis de Vulnerabilidades**

* Fecha: 4 de julio de 2023
* Cliente: Iberdrola
* Consultora de Ciberseguridad: The Bridge - Accelerator
* Control de Cambios:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Versión** | **Documento** | **Fecha** | **Cambios** | **Autor** | **revisor** | **visto bueno** |
| 1.1 | Informe de resultados | 03/07/2024 | Informe inicial | Victor Martínez | Ángel  Cardiel | Javier Tomás |

Índice de Contenidos

1. Introducción
2. Alcance
3. Vulnerabilidades Encontradas
4. Anexos

1. Introducción

Este informe técnico presenta un análisis exhaustivo de las vulnerabilidades identificadas en los hosts: Metasploitable y Windowsplotaible. Para llevar a cabo este análisis, se emplearon herramientas avanzadas de ciberseguridad, incluyendo Nessus para la detección de vulnerabilidades y Nmap para el reconocimiento de puertos y servicios. El objetivo de este informe es proporcionar una evaluación detallada de las debilidades de seguridad encontradas, así como los riesgos potenciales que estas vulnerabilidades representan para la integridad, confidencialidad y disponibilidad de los sistemas de la organización.

2. Alcance

El análisis abarcó la identificación de vulnerabilidades que podrían ser explotadas por atacantes para comprometer la seguridad de los sistemas, representando un riesgo significativo para la organización y afectando la integridad, confidencialidad y disponibilidad de los datos.

3. Vulnerabilidades Encontradas

A continuación, se detallan las vulnerabilidades identificadas, su criticidad y las soluciones recomendadas:

Vulnerabilidad Descripción Criticidad Solución Recomendada

CVE-2021-12345 Vulnerabilidad que permite la ejecución remota de código debido a una falla en la validación de entradas. Crítica Aplicar el parche de seguridad disponible

CVE-2021-67890 Vulnerabilidad que permite el escalamiento de privilegios debido a una configuración incorrecta de permisos. Alta Configurar políticas de acceso restrictivas

CVE-2021-54321 Vulnerabilidad que expone información sensible debido a una falta de cifrado en la transmisión de datos. Media Implementar cifrado de datos sensibles

(HACER TABLA CON LOS CVE Y RECOMENDACIONMES)

Anexos

Niveles de Criticidad de las Vulnerabilidades:

Crítica: Vulnerabilidad que puede ser explotada fácilmente y tiene un impacto severo en la seguridad del sistema.

Alta: Vulnerabilidad que puede ser explotada con cierto esfuerzo y tiene un impacto significativo.

Media: Vulnerabilidad que requiere condiciones específicas para ser explotada y tiene un impacto moderado.

Metodologías Utilizadas:

CVE (Common Vulnerabilities and Exposures)

CVSS (Common Vulnerability Scoring System)

Herramientas Empleadas:

Nessus: Utilizado para la detección de vulnerabilidades.

nmap: Utilizado para el reconocimiento de puertos y servicios.