Informe de Pentesting

Autor: 4k4m1m3

Análisis de Vulnerabilidades
Comunidad Hacking Ético

Fecha:
2024-03-27

Documento:
CTF RETO1 OCLAT

Versión:
2024-03-27-RV.001-MM

Web:
4k4m1m3.github.io

Teléfono:

Correo:
4k4m1m3@gmail.com

AVISO LEGAL

CONTROL DE DOCUMENTO

NOMBRE DOCUMENTO:	**CTF RETO1 OCLAT**
AUTOR:	**4k4m1m3**
FECHA:	**2024-03-27**
CLIENTE:	**Comunidad Hacking Ético**

DECLARACIÓN DE CONFIDENCIALIDAD

Este informe contiene la información relativa a las posibles brechas de seguridad de Comunidad Hacking Ético y sus sistemas. 4k4m1m3 recomienda que sean tomadas precauciones especiales para proteger la confidencialidad de este documento y de la información contenida en él. Todas las demás copias del informe se han entregado a Comunidad Hacking Ético. La evaluación de la seguridad es un proceso incierto, basado en las experiencias, la información actualmente disponible y las amenazas conocidas. Se debe entender que todos los sistemas de información, por su naturaleza dependen de los seres humanos y son vulnerables en cierto grado.

Este informe podrá recomendar que Comunidad Hacking Ético utilice ciertos productos de software o hardware fabricados o mantenidas por otros proveedores. 4k4m1m3 basa estas recomendaciones a partir de su experiencia previa con las capacidades de estos productos. Sin embargo, 4k4m1m3 no puede y no debe garantizar que un determinado producto funcionará según lo anunciado por el vendedor.

ÍNDICE

(GENERAR INDICE CON WORD)

1. INTRODUCCIÓN

Durante las pruebas se simulan las actividades que realizaría un atacante real, descubriendo las vulnerabilidades, su nivel de riesgo, y generando recomendaciones que permitan al cliente realizar la remediación de estas. En cada sección de este informe se detallan los aspectos importantes de la forma en que un atacante podría utilizar la vulnerabilidad para comprometer y obtener acceso no autorizado a información sensible. Se incluyen además directrices que al ser aplicadas mejoraran los niveles de confidencialidad, integridad y disponibilidad de los sistemas analizados.

1.1. OBJETIVO

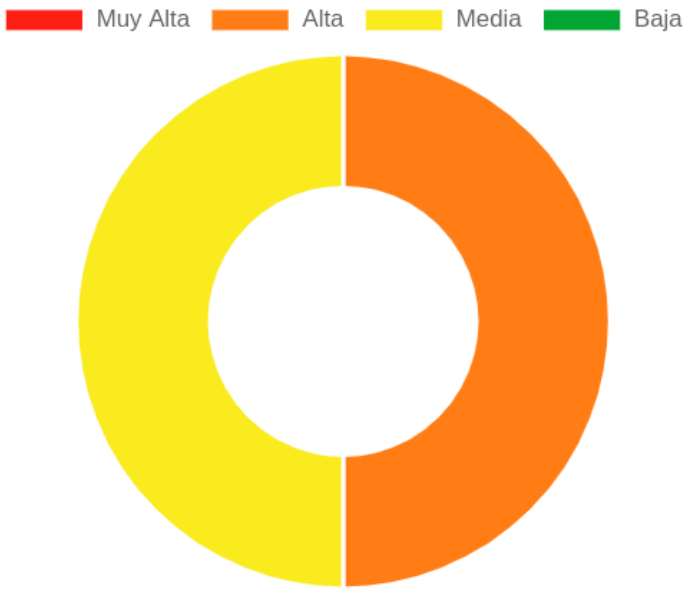
El objetivo de la evaluación de seguridad es detectar las vulnerabilidades de seguridad existentes en los sistemas analizados para posteriormente generar un informe con los hallazgos y recomendaciones que permitan la remediación de estas.

1.2. ALCANCE

La evaluación realizada se ha centrado en los objetivos aprobados en el alcance del contrato, en el cual se establece:

No.	Objetivos
1	Host: 10.6.8.11

2. RESUMEN EJECUTIVO



Vulnerabilidad	Cantidad	Porcentaje
Muy Alta	0	0%
Alta	1	50%
Media	1	50%
Baja	0	0

3. RESULTADO DE LAS PRUEBAS

3.1 DETALLES DE LOS OBJETIVOS

Host: 10.6.8.11

Vulnerabilidad:: Autentificación insegura
Criticidad: Alta

Descripción:
Los mecanismos de autentificación pueden ser facilmente bypaseados.

Recomendación:
Usar políticas de contraseñas robustas, implementar un sistema de autentificación multi-factor.

Vulnerabilidad:: Fuga de información
Criticidad: Media

Descripción:
Expone información confidencial a usuarios no autorizados

Recomendación:
Asegurarse que los mensajes de error y los registros no revelen datos confidenciales

---

4. TABLA DE CRITICIDAD

Host: 10.6.8.11

Nombre	Criticidad
Autentificación insegura	Alta
Fuga de información	Media

5. CONCLUSIONES

El proceso de pentesting reveló la presencia de vulnerabilidades significativas en la configuración de la máquina analizada. La identificación de los puertos 21 y 22 abiertos con los servicios FTP y SSH, respectivamente, junto con las versiones específicas de software (vsftpd 3.0.3 y OpenSSH 7.2p2), plantea preocupaciones de seguridad, ya que estas versiones pueden ser susceptibles a ataques conocidos. Además, la presencia de archivos root.txt y user.txt en el resultado del escaneo del puerto 21 FTP, accesibles mediante una conexión anónima, indica una grave falta de protección de datos sensibles. Esta situación subraya la importancia de implementar medidas de seguridad adecuadas, como la autenticación robusta y la configuración adecuada de los servicios, para mitigar los riesgos de acceso no autorizado y la filtración de información confidencial.