# INFORME DE PENTESTING

## 1. Introducción

Este informe documenta la evaluación de seguridad realizada sobre el sistema objetivo, detallando las vulnerabilidades encontradas, las pruebas efectuadas, los métodos de explotación utilizados y las soluciones implementadas para mitigar riesgos.

## 2. Alcance del Pentesting

- Evaluación de seguridad en servicios expuestos (SSH, FTP, HTTP, MySQL).
- Identificación de procesos sospechosos en el sistema.
- Análisis de contraseñas almacenadas en MySQL.
- Revisión de permisos y configuraciones en servicios críticos.
- Implementación de medidas correctivas y preventivas.

---

## 3. Fase 1: Reconocimiento y Recolección de Evidencias

### 3.1. Identificación de Acceso No Autorizado

**Pruebas realizadas:**

- Revisión de logs con journalctl -u ssh.
- Identificación de conexiones sospechosas en /var/log.

**Hallazgos:**

- Conexión no autorizada detectada el **08/10/2024** desde la IP **192.168.0.134**, utilizando el puerto **45623** para SSH.

**Soluciones Aplicadas:**

- Modificación del archivo /etc/ssh/sshd_config:
- PermitRootLogin no
  PasswordAuthentication no

- Reinicio del servicio: sudo systemctl restart sshd
- Configuración de firewall con ufw:
- sudo ufw default deny incoming
- sudo ufw allow OpenSSH
  sudo ufw enable

### 3.2. Identificación de Malware y Rootkits

**Pruebas realizadas:**

- Escaneo con rkhunter en búsqueda de rootkits y malware.
- Análisis de procesos activos con ps aux --sort=-%cpu | head -10.

**Hallazgos:**

- Procesos con alto consumo de CPU y memoria, indicando actividad sospechosa.
- Archivos desconocidos modificados en /var/log.

**Soluciones Aplicadas:**

- Eliminación de procesos sospechosos.
- Modificación de permisos en wp-config.php.
- Cambio de contraseñas de usuarios comprometidos.

### 3.3. Evaluación de Puertos Abiertos

**Pruebas realizadas:**

- Escaneo de red con nmap -sV -p- -O 10.0.2.11.

**Hallazgos:**

- Puertos abiertos identificados:
  - **21/tcp (FTP) - vsftpd 3.0.3**
  - **22/tcp (SSH) - OpenSSH 9.2p1**
  - **80/tcp (HTTP) - Apache 2.4.62**
  - **8834/tcp (SSL/Nessus)**

**Soluciones Aplicadas:**

- Bloqueo de puertos innecesarios con ufw.
- Configuración de reglas de acceso.

---

## 4. Fase 2: Explotación y Corrección de Vulnerabilidades

### 4.1. Vulnerabilidad en Apache (Directory Listing)

**Pruebas realizadas:**

- Análisis con Nikto:

  nikto -h http://10.0.2.11

- Verificación con nmap --script http-vuln* -p 80 10.0.2.11.

**Hallazgos:**

- Configuración insegura en **Apache 2.4.62**, permitiendo el listado de archivos en /uploads.

**Soluciones Aplicadas:**

- Modificación del archivo de configuración:
- <Directory /var/www/html/>
- Options -Indexes
- AllowOverride All
  </Directory>

- Reinicio del servicio: sudo systemctl restart apache2

### 4.2. Contraseñas Débiles en MySQL

**Pruebas realizadas:**

- Análisis de contraseñas con SELECT user, authentication_string FROM mysql.user;

**Hallazgos:**

- Usuarios con credenciales débiles:
  - root → Contraseña: **123456** (hash: *6BB4837EB74329105EE4568DDA7DC67ED2CA2AD9)
  - wordpressuser → Mismo hash que root.
  - user → Contraseña: **password**

**Soluciones Aplicadas:**

- Cambio de contraseñas a valores seguros:
- ALTER USER 'root'@'localhost' IDENTIFIED BY 'S3gur@P4ssw0rd!';
- ALTER USER 'wordpressuser'@'localhost' IDENTIFIED BY 'WpS3gura!2024';
  ALTER USER 'user'@'localhost' IDENTIFIED BY 'Us3r_F0rt!fied';

- Habilitación de validación de contraseñas:
- INSTALL PLUGIN validate_password SONAME 'validate_password.so';
  SET GLOBAL validate_password_policy = STRONG;

---

## 5. Fase 3: Plan de Respuesta a Incidentes y Certificación

### 5.1. Identificación y Contención

- Bloqueo de la IP atacante con ufw.
- Restricción de acceso root en SSH.
- Deshabilitación de Anonymous FTP (anonymous_enable=NO).

### 5.2. Erradicación y Recuperación

- Eliminación de archivos maliciosos.
- Revisión y actualización de configuraciones críticas.
- Monitoreo del sistema con auditd y fail2ban.

### 5.3. Prevención de Futuros Ataques

- Implementación de autenticación de doble factor en SSH.
- Auditorías de seguridad periódicas.
- Aplicación de parches de seguridad de inmediato.

---

## 6. Conclusión y Recomendaciones

- Se eliminaron vulnerabilidades críticas en SSH, Apache y MySQL.
- Se implementaron medidas de seguridad en firewall y autenticación.
- Se recomienda la adopción de prácticas de seguridad continuas:
    - **Monitoreo activo** con herramientas como fail2ban.
    - **Restricción de accesos** mediante listas blancas.
    - **Actualización constante** del sistema y software.

Con la aplicación de estas soluciones, el sistema ha mejorado significativamente su seguridad, reduciendo el riesgo de ataques futuros.