PROYECTO FIN DE MASTER: Spain-cs-pt-2

4Geeks

ALUMNO: Luciano Matias Zuccardi

PROFESORES: Jorge Garcia - Raul Moncada

INTRODUCCION

Este informe se centra en restaurar y proteger un servidor critico en 4Geeks Academy, donde se identificaron áreas de riesgo que podrían comprometer la confidencialidad e integridad de la información. A partir de estos hallazgos, se proponen medidas de mitigación y un plan de recuperación y continuidad para minimizar el impacto de posibles incidentes de seguridad y garantizar la disponibilidad de los servicios.

MAQUINA

Maquina vulnerada: Debian GNU/Linux 12

Maquina Atacante: Kali Linux

RESUMEN DE VULNERABILIDADES

Se identificaron las siguientes vulnerabilidades:

- Mala configuracion en **HTTP** (puerto 80)
- Contraseñas predeterminadas en **FTP** (puerto 21)
- Claves de acceso debiles en **SSH** (puerto 22)
- Mala configuración en el archivo **“wp-config.php”.**
- Mysql con credenciales débiles
- puertos y servicios innecesarios abiertos.

4Geeks

Resumen del analisis de riesgo

La combinación de probabilidad e impacto determina el **nivel de riesgo**. Este nivel indica la prioridad para tomar medidas de seguridad.

Activo	Probabilidad	Impacto	Nivel de Riesgo
HTTP	**Muy Alta**	**Muy Alto**	**Muy Alto**
SSH	**Media**	**Muy alto**	**Muy alto**
FTP	**Alta**	**Alto**	**Alto**
wp-config.php (WordPress)	**Media**	**Alto**	**Alto**

Resumen del Plan de Recuperacion

Vulnerabilidad	Acciones de Recuperación	Configuración correcta
HTTP (Configuracion)	Configuración y actualizacion en los servicios	HTTPS: certificaciones SSL/TLS
SSH (Clave Débil)	Usar claves seguras en SSH y deshabilitar acceso con contraseña.	Deshabilitar Contraseña: PasswordAuthentication **“no”** en carpeta /etc/ssh/sshd_config.
FTP (Usuario Predeterminado)	Desactivar la cuenta o cambiar nombre y contraseña.	Cambio de credenciales predeterminadas.
WP-Config.PHP: Permisos Excesivos	Modificar Permisos con chmod 640 o 440.	1. Acceder: Vía SSH. 2. modificar el Archivo **wp-config.php.** 3. Cambiar Permisos: **chmod 640 wp-config.php (o 440).**

Conclusión

Es muy importante implementar medidas correctivas para cada hallazgo, un plan de recuperación y continuidad, junto con prácticas de monitoreo y respaldo que aseguren la confidencialidad, integridad y disponibilidad de los servicios ante estos incidentes de seguridad.

Para ello es fundamental lograr un plan de mejora continua, implementando soluciones como:

- **Firewalls** y **SIEM**: para el control y monitorización del trafico
- **DLP** (Data loss Prevention): para la protección de datos y cumplimientos normativos
- Auditorias de Seguridad
- Capacitación constante a los empleados
- **SGSI** (Sistema de Gestión de Seguridad de la Información): Para la protección de datos y garantizar la continuidad del negocio.