Proyecto Final

Presentado por
Santiago Rivero

Introducción

Contexto del proyecto

- Se detectó el compromiso de un servidor crítico de la organización.
- El objetivo del proyecto fue analizar el incidente, corregir las vulnerabilidades, demostrar riesgos adicionales y establecer un plan de respuesta a incidentes.
- El trabajo se dividió en tres fases complementarias:
    a. Reconocimiento y hardening del sistema comprometido
    b. Detección y explotación de una vulnerabilidad adicional
    c. Diseño de un plan de respuesta a incidentes y SGSI (ISO 27001)

Enfoque aplicado

- Análisis técnico
- Explotación controlada
- Mitigación y prevención
- Uso de estándares internacionales (NIST, ISO 27001)

Problemas Detectados

Análisis de Riesgos Críticos

Descripción general de los problemas

Durante el análisis del servidor comprometido se identificaron múltiples debilidades de seguridad que, en conjunto, facilitaron el acceso no autorizado y aumentaron el riesgo de escalación de privilegios. La principal problemática estuvo relacionada con configuraciones inseguras en servicios críticos, uso de credenciales débiles, exposición innecesaria de servicios y falta de controles preventivos y de respuesta ante incidentes.

Principales problemas detectados

- Acceso SSH inseguro mediante autenticación por contraseña y acceso root previo
- Servicios expuestos innecesarios (FTP, MySQL, Apache)
- Usuario de MySQL/MariaDB con contraseña débil
- Métodos HTTP inseguros habilitados
- Exposición de información del servidor
- Acceso directo a directorios sensibles de WordPress (/wp-includes)
- Ausencia de hardening básico del sistema
- Falta de un plan formal de respuesta a incidentes
- Inexistencia de un SGSI alineado con ISO 27001

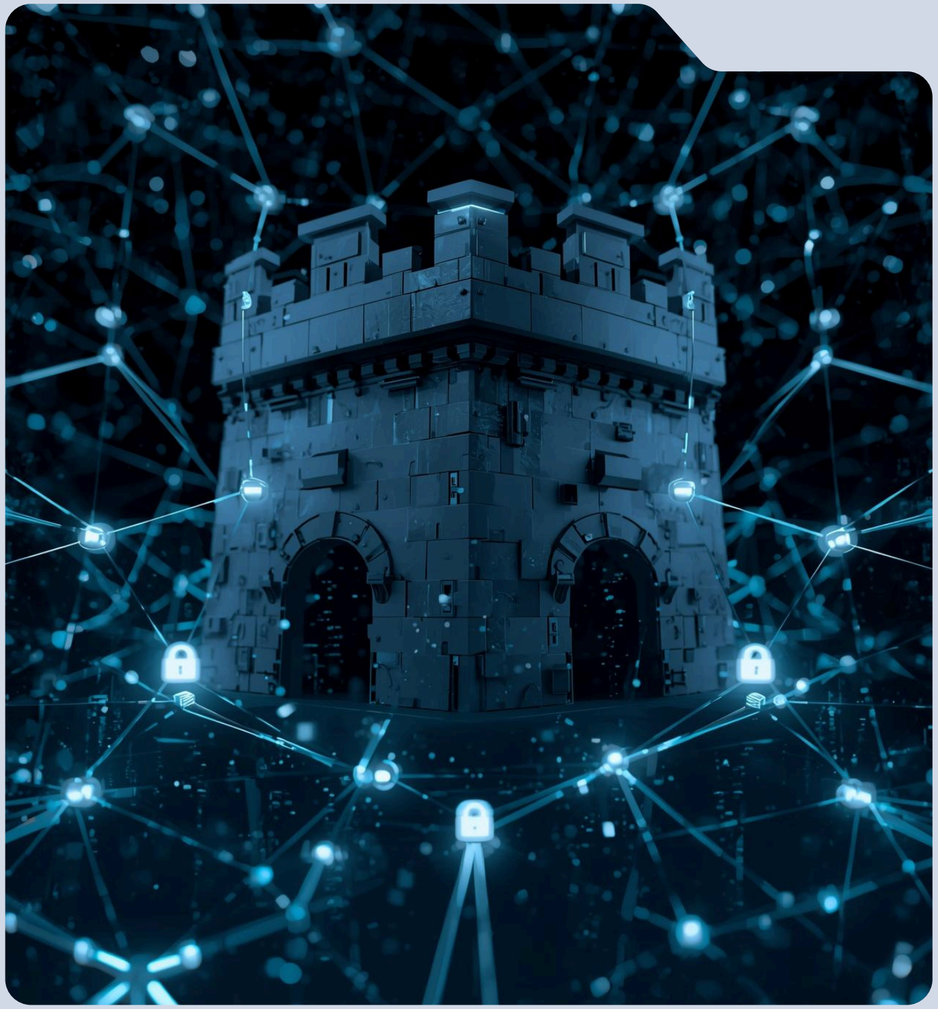
Objetivos

Objetivo general

- Restaurar la seguridad del servidor comprometido y elevar el nivel de madurez de seguridad de la organización.

Objetivos específicos

- Identificar cómo ocurrió el ataque inicial
- Eliminar accesos y configuraciones inseguras
- Detectar y explotar una vulnerabilidad adicional
- Aplicar hardening técnico verificable
- Diseñar un plan de respuesta a incidentes
- Implementar un SGSI conforme a ISO 27001



Soluciones Aplicadas

Descripción general de las soluciones

Tras la identificación de las vulnerabilidades y debilidades del sistema, se aplicaron medidas técnicas orientadas a contener el incidente, eliminar los vectores de ataque y fortalecer la postura de seguridad del servidor. Las soluciones implementadas se enfocaron en reducir la superficie de ataque, corregir configuraciones inseguras y establecer controles preventivos y reactivos que permitan mitigar incidentes similares en el futuro.

Principales soluciones aplicadas

- Hardening del acceso SSH
  - Deshabilitación del acceso root
  - Restricción de usuarios permitidos
  - Refuerzo de métodos de autenticación
- Desactivación de servicios inseguros o innecesarios
  - Deshabilitación del servicio FTP (vsftpd)
- Corrección de credenciales débiles en MySQL/MariaDB
  - Eliminación de usuarios con contraseñas inseguras
  - Restricción de accesos a la base de datos
- Hardening del servidor web (Apache)
  - Deshabilitación del método HTTP TRACE
  - Ocultamiento de información del servidor
  - Bloqueo de listados de directorios
- Implementación de controles preventivos adicionales
  - Configuración de firewall (UFW)
  - Instalación de Fail2Ban para mitigación de ataques por fuerza bruta
- Definición de un Plan de Respuesta a Incidentes y SGSI
  - Basado en NIST SP 800-61 e ISO 27001

Metodología-Fase 1

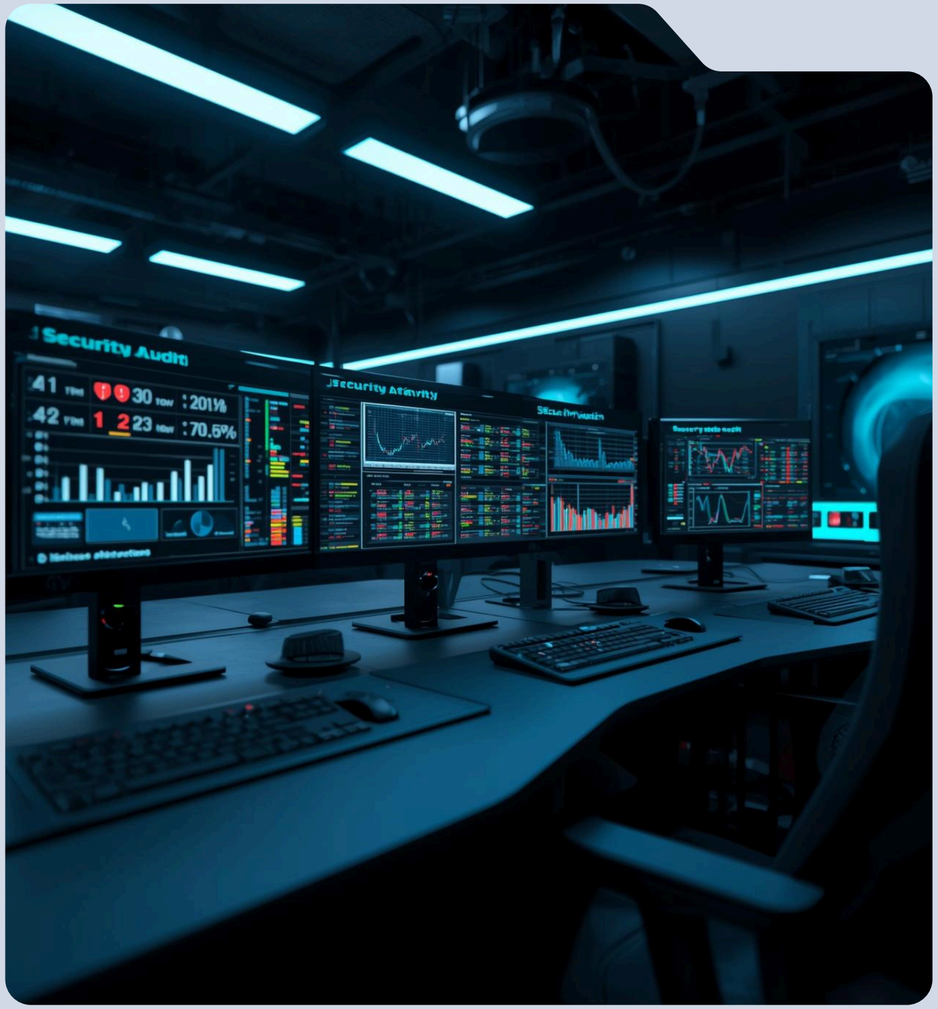
Comandos utilizados (respaldo técnico)

```bash
# Análisis de accesos y eventos
sudo journalctl -u ssh
sudo journalctl | grep Accepted
sudo journalctl | grep useradd

# Revisión de servicios y procesos
ss -tulpn
ps aux

# Revisión de usuarios y privilegios
cat /etc/passwd
getent group sudo
who

# Escaneo de malware y rootkits
sudo chkrootkit
sudo rkhunter --check --sk
```

```bash
# Hardening y contención
systemctl stop vsftpd
systemctl disable vsftpd

nano /etc/ssh/sshd_config
PermitRootLogin no
PasswordAuthentication no
AllowUsers usuario_autorizado

systemctl restart ssh
```

Metodología aplicada

Durante esta fase se realizó un análisis forense del sistema **comprometido** con el objetivo de identificar cómo ocurrió el acceso inicial, qué servicios fueron **afectados** y qué acciones realizó el atacante. Se analizaron **registros** del sistema, usuarios, procesos y servicios activos para determinar el alcance del incidente. Posteriormente, se aplicaron medidas de **hardening y contención**, deshabilitando servicios inseguros, corrigiendo configuraciones vulnerables y **reforzando** controles de acceso.

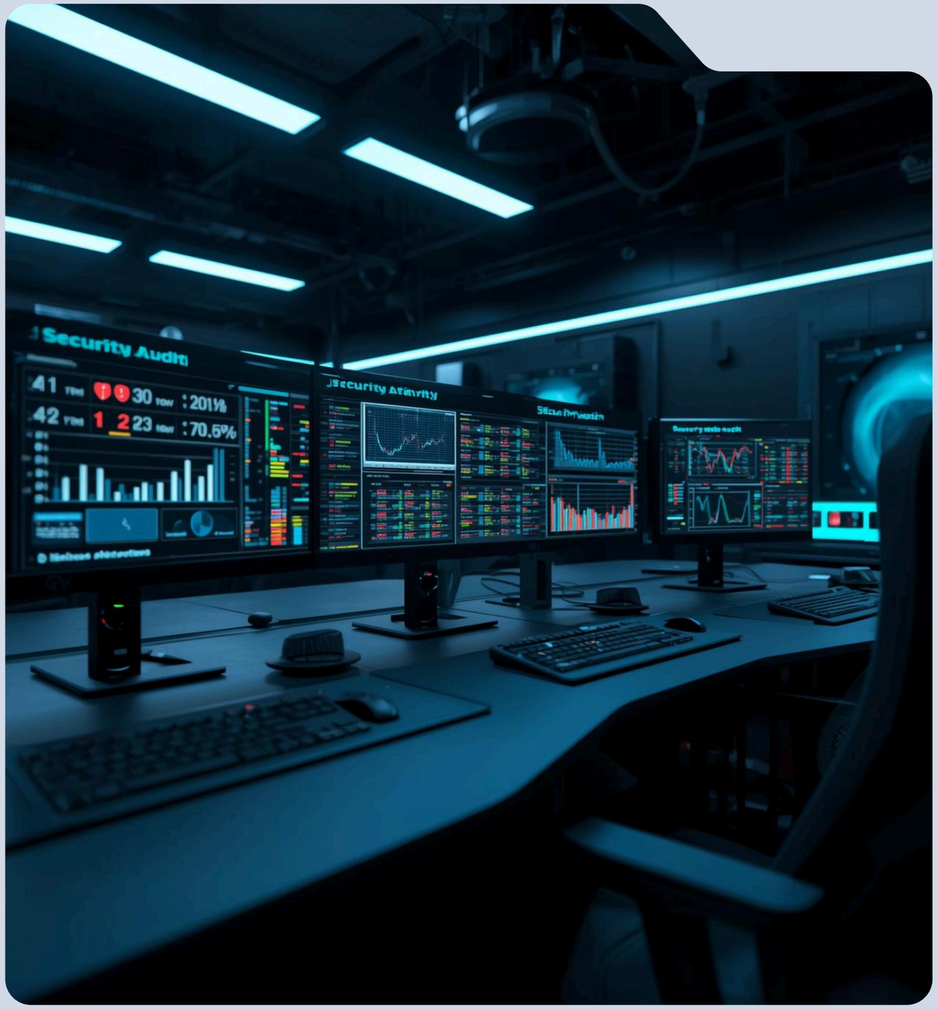


Metodología-Fase 2

Comandos utilizados (respaldo técnico)

```bash
# Reconocimiento externo
nmap -sS -sV -p- 10.0.2.11

# Enumeración del servicio web
nmap --script http-enum,http-headers,http-methods -p 80 10.0.2.11

# Explotación controlada
curl -X TRACE http://10.0.2.11
curl -I http://10.0.2.11
# Acceso a directorios sensibles
http://10.0.2.11/wp-includes

# Corrección de la vulnerabilidad
nano /etc/apache2/conf-enabled/security.conf
TraceEnable Off
ServerTokens Prod
ServerSignature Off

nano /etc/apache2/sites-available/000-default.conf
Options -Indexes

systemctl restart apache2
```

En esta fase se adoptó la perspectiva de un atacante externo, realizando escaneos de puertos y servicios para identificar vulnerabilidades distintas al ataque inicial. Una vez detectada una mala configuración en el servicio web, se llevó a cabo una explotación controlada para demostrar su impacto real.



Metodología-Fase 3

En la fase final se diseñó un Plan de Respuesta a Incidentes basado en la guía NIST SP 800-61, definiendo procedimientos claros para identificar, contener, erradicar y recuperar ante futuros incidentes. Además, se desarrolló un Sistema de Gestión de Seguridad de la Información (SGSI) conforme a la norma ISO/IEC 27001, permitiendo gestionar la seguridad de forma estructurada, preventiva y basada en riesgos, asegurando la mejora continua de la postura de seguridad de la organización.

Marcos y controles aplicados

- NIST SP 800-61 (Respuesta a Incidentes)
- ISO/IEC 27001 (SGSI)
- Análisis de riesgos
- Definición de políticas y controles
- Mejora continua

Explotación

La Fase 2 permitió detectar una vulnerabilidad distinta al ataque inicial, demostrar su impacto mediante explotación controlada y confirmar que la corrección aplicada fue efectiva. Se redujo significativamente la superficie de ataque del servicio web.

Evidencias técnicas (salidas relevantes)

Escaneo de puertos

```bash
nmap -sS -sV -p- 10.0.2.11
```

Resultado

```
22/tcp   open  ssh
80/tcp   open  http
3306/tcp open  mysql
```

Metodos HTTP Habilitados

```bash
nmap --script http-methods -p 80 10.0.2.11
```

Resultado

```
Supported Methods: GET POST OPTIONS TRACE
```

Explotación del metodo TRACE

```bash
curl -X TRACE http://10.0.2.11
```

Resultado

```
HTTP/1.1 200 OK
TRACE / HTTP/1.1
```

Bannrer grabbing

```bash
curl -I http://10.0.2.11
```

Resultado

```
Server: Apache/2.4.x (Ubuntu)
```

Acceso a directorio sensible

```text
http://10.0.2.11/wp-includes
```

Validación tras la corrección

```bash
curl -X TRACE http://10.0.2.11
```

Resultado

```
405 Method Not Allowed
```

```
curl -I http://10.0.2.11
```

Resultado

```
Server: Apache
```

Recomendaciones

Recomendaciones Tecnicas

- Auditorías de seguridad periódicas
- Escaneos automatizados de vulnerabilidades
- Revisión constante de configuraciones
- Uso obligatorio de autenticación por claves

Recomendaciones Organizacionales

- Capacitación continua del personal
- Actualización del SGSI
- Simulacros de respuesta a incidentes
- Integración de seguridad en procesos operativos