

M6 - P5: Taller Final de Hardening sobre Sistema Vulnerable

Después de aprender sobre hardening, firewalls, segmentación y monitorización, llega el momento de **poner en práctica todos los conocimientos adquiridos**. Esta práctica propone que los alumnos trabajen sobre una **máquina vulnerable**, identifiquen debilidades reales y **apliquen medidas concretas de mitigación**.

Objetivos específicos

- Evaluar la seguridad de un sistema comprometido o mal configurado.
- Aplicar medidas de hardening en capas (sistema, red, servicios).
- Integrar herramientas de auditoría, firewall, monitorización y benchmarks.
- Elaborar un informe técnico profesional, como se hace en una auditoría de seguridad.

Requisitos técnicos

- Máquina virtual vulnerable:
 - Recomendado: **Metasploitable 2**, **DVWA**, **OWASP Broken Web Apps**, **VM de Vulhub** o **una VM personalizada sin hardening**
- Kali Linux (como máquina atacante o de auditoría)
- Conectividad entre las máquinas
- Herramientas: nmap, lynis, ufw, fail2ban, Wazuh, aide, netstat, auditd, iptables, etc.

Parte A: Auditoría inicial del sistema

Paso 1: Escaneo de puertos y servicios (Kali)

Desde Kali Linux:

```
nmap -sV -O -p- <IP de la máquina vulnerable>
```

Documentar:

- Puertos abiertos
- Servicios identificados
- Sistemas operativos o versiones

Objetivo: Obtener una vista general de la superficie de ataque expuesta.

Paso 2: Auditoría con Lynis

En la VM vulnerable:



```
sudo apt update && sudo apt install lynis -y  
sudo lynis audit system
```

Documentar:

- Recomendaciones críticas
- Puntaje de seguridad inicial
- Módulos fallidos o inseguros

Paso 3: Evaluación manual

Ejecutar y documentar los siguientes puntos:

- ¿Qué servicios se están ejecutando innecesariamente?
- ¿Hay cuentas con contraseñas débiles o sin contraseña?
- ¿Se permiten login como root por SSH?
- ¿Existe un firewall activo?
- ¿Hay logs sin protección o rotación?

Resultado esperado: Mapa de vulnerabilidades y debilidades del sistema.

Parte B: Aplicación de medidas de hardening

Cada alumno o grupo debe aplicar al menos **5 medidas técnicas** distintas de hardening.

Ejemplos recomendados:

1. Deshabilitar servicios innecesarios:

```
sudo systemctl disable telnet  
sudo systemctl stop telnet
```

2. Configurar ufw:

```
sudo ufw default deny incoming  
sudo ufw allow 22/tcp  
sudo ufw enable
```

3. Forzar políticas de contraseñas:

Editar /etc/login.defs y /etc/pam.d/common-password

4. Instalar y configurar fail2ban:

```
sudo apt install fail2ban  
sudo systemctl enable fail2ban  
sudo systemctl start fail2ban
```

5. Monitoreo con **audit** o instalación de agente Wazuh
6. Implementar **aide** para integridad:

```
sudo apt install aide
sudo aideinit
sudo cp /var/lib/aide/aide.db.new /var/lib/aide/aide.db
```

Parte C: Reauditoría del sistema

Paso 1: Volver a correr Lynis

```
sudo lynis audit system
```

Comparar puntaje antes y después.

Paso 2: Validar con Nmap

Desde Kali:

```
nmap -sV -O -p- <IP>
```

Documentar:

- Servicios ahora cerrados
- Mejoras visibles en la seguridad del sistema

Objetivo: Verificar y validar que las medidas aplicadas **han reducido la superficie de ataque**.

Parte D: Informe técnico final

El informe debe estar redactado como si fuera para una empresa o cliente real.

Estructura sugerida:

1. **Introducción**
 - Contexto del análisis
 - Objetivos
2. **Resumen de vulnerabilidades**
 - Detalle de hallazgos iniciales
3. **Medidas aplicadas**
 - Qué cambios se realizaron y por qué
4. **Comparación antes/después**
 - Escaneo de puertos
 - Puntaje de Lynis
 - Servicios eliminados
5. **Conclusiones**



GOBIERNO
DE ESPAÑA

MINISTERIO
DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL



UNIÓN EUROPEA
Fondo Social Europeo
El FSE invierte en tu futuro



GENERALITAT
VALENCIANA
Conselleria d'Educació, Cultura,
Universitats i Ocupació



CEFIRE
FORMACIÓ PROFESSIONAL
ENSENYANÇES ARTÍSTIQUES
I ESPORTIVES

FPcv
Formació Professional
Comunitat Valenciana

- Estado final del sistema
- Recomendaciones futuras

Actividades complementarias

- Simular un ataque de fuerza bruta antes/después de implementar fail2ban.
- Configurar reglas de firewall para limitar acceso solo a IPs específicas.
- Mostrar gráficamente el “antes y después” de la infraestructura.

Reflexión final

- ¿Qué fue lo más difícil de endurecer?
- ¿Qué herramientas ayudaron más?
- ¿Cómo puede mantenerse seguro este sistema a largo plazo?

Buenas prácticas

- Tomar **capturas de pantalla** del proceso para incluir en el informe.
- Mantener una bitácora de todos los comandos ejecutados.
- Asegurarse de que el sistema sigue siendo funcional tras el hardening.
- Si se bloquea algo por error, **documentar cómo se revirtió**.