

Desarrollo del tema

A cada equipo se le asignará una plataforma.
Cada equipo deberá entregar

- **Un documento en formato APA**
 - **Una Presentación para exposición del tema**
 - **Una práctica demostrable.**
-

Apartado 1: Descripción técnica de la plataforma

Cada equipo debe explicar:

- ¿Qué es la plataforma?
 - ¿Cómo funciona?
 - ¿Qué tecnologías utiliza?
 - ¿Por qué es un objetivo importante en ciberseguridad?
 - ¿Qué roles puede tener en un ataque real? (ej. punto de entrada, persistencia, robo de datos, etc.)
-

Apartado 2: Principales vulnerabilidades

Los alumnos deben investigar y presentar:

- Vulnerabilidades típicas
 - Debilidades de configuración
 - Errores humanos frecuentes
 - Casos reales (brechas o ataques conocidos)
 - Riesgos para la empresa y para los usuarios
-

Apartado 3: Herramientas de hackeo ético aplicables

Cada plataforma tiene herramientas específicas.

Los alumnos deben describir:

- Nombre de la herramienta
- ¿Para qué sirve?
- ¿En qué fase del pentesting se usa?
- Capturas de pantalla reales
- Comandos básicos o procedimientos

Apartado 4: Laboratorio práctico

Cada equipo debe ejecutar **un laboratorio seguro**, demostrable en video.

El laboratorio debe incluir:

- Preparación del entorno
- Herramientas utilizadas
- Comandos ejecutados
- Resultados obtenidos
- Evidencias (pantallas, reportes, trazas, logs)
- Conclusiones

Apartado 5: Recomendaciones de seguridad (Hardening)

En este punto deben proponer:

- Soluciones
- Buenas prácticas
- Configuraciones seguras
- Políticas recomendadas
- Medidas preventivas y correctivas