Actividad principal

Ciberdefensores en red

2.º CFGS ASIR — Seguridad y Alta Disponibilidad

🎯 Enunciado de la actividad

Desarrollar un proyecto cooperativo en el que los equipos del aula simulen un **Centro de Operaciones de Seguridad (SOC)**.

El objetivo será **diseñar, implementar y defender una red corporativa virtualizada** ante ataques simulados, aplicando técnicas reales de ciberseguridad.

🧩 Objetivos técnicos

- Diseñar una infraestructura de red segmentada (DMZ, LAN, servicios internos).
- Implementar medidas de protección (firewall, ACL, autenticación, hardening).
- Monitorizar eventos de seguridad con herramientas SIEM.
- Simular y responder a ciberincidentes reales (MITM, escaneos, malware, etc.).
- Documentar y presentar las soluciones aplicadas.

🔧 Herramientas y entorno

- **VirtualBox o Proxmox** para montar los sistemas.
- **TryHackMe** para entrenamiento y simulación de amenazas.
- Herramientas: Wazuh, UFW/iptables, rsyslog, ClamAV, Suricata, etc.
- Redes y máquinas simuladas: intranet, servidores, estación atacante, SIEM.

🧪 Fases del proyecto

1. **Diseño de la red y asignación de roles**.
2. **Despliegue de servicios y medidas defensivas**.
3. **Simulación de ataque sorpresa** (preparado por el docente).
4. **Análisis del incidente y recuperación**.
5. **Presentación técnica final**: explicación de respuestas, medidas adoptadas y documentación.

📦 Producto final

- Infraestructura funcional documentada.
- Red resistente frente al ataque simulado.
- Dossier técnico por equipo.
- Defensa oral con justificación técnica.