Roadmap Completo IDS - Angelo Conforti

📌Objetivo Principal

Desarrollar un **Sistema de Detección de Intrusiones (IDS)** que sirva como proyecto central para el portafolio profesional, demostrando habilidades en análisis de seguridad, programación, correlación de eventos, y detección de amenazas.

🕰️Etapas y Proyectos Intermedios

Cada mini-proyecto aporta una **pieza funcional** que luego se integrará en el IDS final.

1. Proyecto de Análisis de Logs (Log Analyzer)

- **Descripción:** Crear una aplicación en Python que lea, procese y analice archivos de logs de distintos servicios (Apache, SSH, Windows Event Logs, etc.).
- **Funcionalidades clave:**
- Normalización de logs.
- Identificación de patrones sospechosos (intentos de login fallidos, accesos desde IPs inusuales, etc.).
- Exportación de reportes (CSV/JSON).
- **Relación con el IDS:** Módulo de **recolección y preprocesamiento de datos**.
- **Métrica de éxito:** Detectar al menos 5 tipos de patrones comunes de amenazas en archivos de prueba.

2. Proyecto de Correlación de Eventos

- **Descripción:** Sistema que toma logs de diferentes fuentes y los correlaciona para identificar actividades sospechosas.
- **Funcionalidades clave:**
- Reglas de correlación basadas en tiempo (ejemplo: 5 intentos fallidos en 1 minuto).
- Motor de reglas configurable (YAML/JSON).
- Alertas clasificadas por severidad.
- **Relación con el IDS:** Módulo de **detección basada en reglas**.
- **Métrica de éxito:** Generar alertas con un ratio de falsos positivos < 20% en dataset de prueba.

3. Proyecto de Detección Basada en Anomalías (ML/Estadístico)

- **Descripción:** Aplicar técnicas de Machine Learning o estadística para detectar comportamientos anómalos.
- **Funcionalidades clave:**
- Extracción de features (ej. número de conexiones por IP, hora del acceso, geolocalización).
- Algoritmos simples (Isolation Forest, clustering, etc.).
- Dashboard para visualizar anomalías.
- **Relación con el IDS:** Módulo de **detección avanzada (anomalías)**.
- **Métrica de éxito:** Detectar al menos el 80% de las anomalías inyectadas en datasets controlados.

4. Proyecto de Interfaz de Monitoreo y Alertas (SIEM Lite)

- **Descripción:** Panel web ligero (Flask/Django + frontend básico) para centralizar la visualización de alertas.
- **Funcionalidades clave:**
- Dashboard con logs y alertas en tiempo real.
- Filtros de búsqueda por IP, usuario, severidad.
- Exportación de reportes.
- **Relación con el IDS:** Módulo de **visualización y gestión de incidentes**.
- **Métrica de éxito:** Dashboard usable con latencia de actualización < 2s en dataset simulado.

🕰️Integración Final: IDS

- **Componentes integrados:**
- Recolección y normalización de logs (proyecto 1).
- Correlación de eventos (proyecto 2).
- Detección de anomalías (proyecto 3).
- Visualización y gestión de alertas (proyecto 4).
- **Entregable final:** Un IDS funcional con pipeline de datos end-to-end.
- **Métricas de éxito:**
- Detectar >80% de incidentes simulados.
- Dashboard accesible y entendible para analistas.
- Documentación clara de arquitectura y casos de uso.

📅Cronograma Estimado

- **Mes 1:** Proyecto de Análisis de Logs.
- **Mes 2:** Proyecto de Correlación de Eventos.
- **Mes 3:** Proyecto de Detección Basada en Anomalías.
- **Mes 4:** Proyecto de Interfaz de Monitoreo.
- **Mes 5:** Integración final del IDS + pruebas.

⚙️Reglas y Estandarización

- **Reglas de correlación:** Definidas en YAML con formato estándar.
- **Dataset de prueba:** Logs reales y generados con herramientas como `hping3`, `Hydra`, `Apache logs` simulados.
- **Documentación:** Cada mini-proyecto tendrá README y ejemplos de uso.
- **Tests:** Cada módulo debe tener tests unitarios y funcionales.

🧪Laboratorios y Comandos de Prueba

- **Logs simulados:**
- `ssh -p 22 usuario@ip` con contraseñas incorrectas → prueba de brute force.
- `ab -n 5000 -c 50 http://localhost/` → prueba de DoS.

- **Generación de anomalías:**
- Enviar tráfico irregular con `hping3`.
- **Validación de alertas:**
- Revisar que cada escenario dispare la alerta esperada.

🔗Conclusión

Este roadmap propone un camino progresivo en **5 meses**, con 4 proyectos intermedios que aportan **módulos reutilizables** para el IDS final. Cada fase tiene métricas de éxito, datasets de validación y un entregable claro. El resultado será un IDS **funcional, modular y demostrable** en entrevistas y portafolio profesional.