

SISTEMA DE DETECCIÓN DE INTRUSOS

Pablo Veen

Índice

Sumario

Introducción.....	3
2. Análisis de la problemática.....	3
2.1 Riesgo de Pérdida de Datos y Continuidad del Negocio.....	3
2.2 Vulnerabilidad y Conectividad.....	3
2.3 Vulnerabilidad en Seguridad Física.....	3
3. Objetivos Específicos.....	3
6. Herramientas y elementos a utilizar.....	4
4: Alcance y límites.....	4
5: Fases o etapas del proyecto.....	4
7: Fechas propuestas.....	5
8. Resultados de aprendizaje cubiertos.....	5
Desarrollo de la práctica.....	6

Introducción

La seguridad informática es un pilar fundamental en cualquier infraestructura tecnológica. Este proyecto propone la implantación de un sistema de detección de intrusos (SDI) en una red local simulada, con el objetivo de identificar, registrar y responder ante posibles amenazas en tiempo real.



2. Análisis de la problemática

2.1 Riesgo de Pérdida de Datos y Continuidad del Negocio

La falta de monitorización activa puede derivar en pérdidas de información crítica y afectar la disponibilidad de servicios.

2.2 Vulnerabilidad y Conectividad

Las redes locales están expuestas a ataques internos y externos. La ausencia de segmentación y protocolos seguros incrementa el riesgo.

2.3 Vulnerabilidad en Seguridad Física

El acceso no controlado a dispositivos y servidores puede comprometer la integridad del sistema.

3. Objetivos Específicos

Implementar un SDI como Snort o Suricata en un entorno virtualizado.

Monitorizar tráfico de red y generar alertas ante patrones sospechosos.

Automatizar respuestas ante incidentes mediante scripting.

Documentar el proceso de instalación, configuración y validación.

Evaluar el rendimiento y fiabilidad del sistema implantado

6. Herramientas y elementos a utilizar

6.1 Infraestructura de Hardware

- PC con soporte para virtualización
- Switch simulado (software)
- Router virtualizado

6.2 Herramientas de monitorización y simulación

- VirtualBox / VMware
- Kali Linux (para pruebas de intrusión)
- Ubuntu Server (SDI)
- Snort / Suricata
- Wireshark
- Nagios / Zabbix (monitorización)
- Bash / Python (automatización)

4: Alcance y límites

El proyecto se desarrollará en un entorno virtualizado, lo que permite simular una red local sin necesidad de infraestructura física costosa. Se utilizarán herramientas libres y de código abierto así que el coste de este proyecto solamente será el desgaste de las propias máquinas y mi tiempo.

5: Fases o etapas del proyecto

Fase	Descripción	Duración
Fase 1	Definición de arquitectura y criterios de seguridad	1 semana
Fase 2	Instalación de sistemas y despliegue del SDI	2 semanas
Fase 3	Configuración, scripting y monitorización	3.5 semanas
Fase 4	Validación, pruebas de intrusión y entrega final	2.5 semanas

7: Fechas propuestas

Inicio: 1 diciembre 2025

Desarrollo: 1 – 20 diciembre 2025

Documentación: 20 – 22 diciembre

Finalización: 22 diciembre 2025

8. Resultados de aprendizaje cubiertos

Este proyecto cubre los siguientes módulos y RA:

- Implantación de sistemas operativos: RA1, RA2, RA3, RA6
- Fundamentos de hardware: RA2, RA3
- Gestión de bases de datos: RA1, RA2, RA3, RA4, RA5
- Planificación y administración de redes: RA1, RA5
- Seguridad y alta disponibilidad: RA1, RA3, RA6
- Administración de sistemas operativos: RA2, RA3, RA7
- Implantación de aplicaciones web: RA2, RA3
- Lenguajes de marcas y sistemas de gestión de información: RA2
- Servicios en red e internet: RA3, RA5
- Itinerario para la empleabilidad I y II: RA1, RA5



Desarrollo de la práctica

Mi idea es desarrollar un proyecto cuyo objetivo principal es implementar una solución de seguridad que permita identificar y responder ante amenazas en tiempo real dentro de una red simulada.

Para llevarlo a cabo, he dividido el proyecto en **cuatro fases**:

1. **Definición de la arquitectura y criterio preventivo:**

En esta etapa diseño la red virtual, elijo el programa y defino qué tipo de ataques voy a simular. También establezco los criterios de seguridad que guiarán el resto del trabajo.

2. **Montaje y despliegue:**

Aquí instalo los sistemas operativos en máquinas virtuales, configuro la red local simulada y despliego el sistema en el servidor. Me aseguro de que todo esté correctamente conectado y funcional.

3. **Configuración avanzada y lógica proactiva:**

En esta fase configuro el programa para que detecte patrones de tráfico sospechoso, automatizo respuestas mediante scripts en Bash o Python, y utilizo herramientas como Wireshark y Zabbix para monitorizar el sistema.

4. **Validación de la fiabilidad y entrega final:**

Realizo pruebas de intrusión usando Kali Linux, verifico que el SDI responde correctamente, documento todo el proceso y evalúo el rendimiento del sistema.

Durante el desarrollo, utilizo herramientas como VMware, Ubuntu Server, Snort/Suricata, Wireshark, Nagios, y Kali Linux, además de lenguajes de scripting para automatizar tareas. También creo una pequeña interfaz web para visualizar alertas, lo que me permite aplicar conocimientos de HTML y CSS.

Este proyecto me permite cubrir una gran cantidad de resultados de aprendizaje, incluyendo la instalación y configuración de sistemas operativos, la gestión de redes, la administración de bases de datos, la automatización de tareas, la seguridad informática, y la documentación técnica. Además, tiene un enfoque práctico y realista que me prepara para enfrentar situaciones similares en el mundo profesional.