
**Nombre del estudiante:** Jamiel Santana.

**Nombre del profesor:** Gean Sosa.

**Materia:** Fundamentos de seguridad.

**Institución:** ITLA.

# Implementar Security Onion

- Instalar **Security Onion** como servidor standalone.
- Configurar IDS.
- Realizar demostración de **Sguil.**
- Configurar **Suricata.**
- Configurar **Kibana** para la visualización de los logs de **Suricata.**
- Detallar el funcionamiento de **CyberChef.**
- Realizar demostración de **NetworkMiner.**

## ¿Qué es Security Onion?

Es una distribución Linux que está orientada a la detección de amenazas, monitorización de seguridad y gestión de los logs. Una de las características más destacadas de Security Onion, es que cuenta con múltiples herramientas incluidas por defecto, por lo que no tendremos que instalar nada ni complicarnos demasiado la vida para su puesta en marcha. Por ejemplo, puedes acceder a Elasticsearch, Snort, Zeek, Wazuh, Cyberchef y NetworkMiner entre otras herramientas. Por otro lado, es muy sencilla de implementar, porque cuenta con un asistente