DISEÑO INICIAL DEL PROYECTO PORT MIRRORING

Primer Prototipo

Para el primer prototipo tenemos hecho la siguiente configuración:

- Switch y Port Mirroring configurado.
- Los servicios que van a actuar como IDS y generación de alertas, que son
    - **TheHive**, que es una herramienta para la creación de organizaciones, casos y observables con la ayuda de por ejemplo VirusTotal.
    - **Cortex,** que es un analizador y creador de alertas de datos que le pasa des de TheHive y responder cuando sea necesario.
    - **MISP** es una base de datos de amenazas/ataques donde compara los patrones de otros ataques con los datos que TheHive le pasa
    - **ELK (Filebeat, Elasticsearch y Kibana)** donde con el primero recolectamos la información, el segundo es para el almacenamiento de los datos recolectados y el tercero para la visualización de estos datos
    - **Snort 3.0** es un IDS para la detección de estos ataques y mandarselos a ELK.

Para el prototipo final los requisitos son los siguientes:
- Hacer Cluster
- Implementar Firewall
- Probar funcionalidad del Port Mirroring
- Probar funcionalidad del SIEM