Gabin BECU
Elmedin SULTANOVIC

Livrable 1 – Documentation de l'architecture réseau

Dans le cadre de la SAE supervision de la sécurité, nous avons déployée une architecture réseau complète.
Elle permet de centraliser les logs, détecter les intrusions via un IDS/IPS, héberger un service web et simuler des scénarios d'attaque à l'aide d'une machine dédiée.

Solutions choisies

Pour répondre aux exigences du projet, nous avons choisi les solutions suivantes : un SIEM basé sur l'ELK Stack.
Une machine IDS/IPS reposant sur OPNsense.
Un poste de travail Linux jouant le rôle de machine cliente.
Un serveur Web et une base de données MySQL regroupés avec WordPress sur une seule machine afin de simplifier le déploiement.
Une machine attaquante Kali Linux pour effectuer les tests d'intrusion.
L'ensemble des équipements est interconnecté via un switch constituant la plateforme matérielle principale.

Éléments de architecture

Machine	Rôle	Adresse IP
Serveur Web + Base de Données	WordPress + MySQL	192.168.1.1
SIEM (ELK Stack)	Collecte & analyse de logs	192.168.1.10
OPNsense (Suricata)	IDS/IPS	192.168.1.50
PC Client Linux	Poste utilisateur	192.168.1.20
Machine Attaquante Kali	Scans & attaques	192.168.1.150

Gabin BECU
Elmedin SULTANOVIC

Schéma de l'Architecture Réseau