GOVINDIN Devendra
BTS SIO - option SISR
Session 2024-2026

Choix et Déploiement du Serveur Hôte (NIDS)

Dans le cadre du Projet E6 (mise en place d'un système de détection d'intrusions pour l'infrastructure Vénus), la sélection du système d'exploitation de la sonde réseau a été une étape déterminante. La machine hôte devait être capable de recevoir le trafic dupliqué par l'hyperviseur Proxmox, d'exécuter le moteur d'analyse Suricata et de centraliser les journaux de sécurité via la pile ELK.

Note : La documentation technique détaillée de ce déploiement (configuration du Port Mirroring Proxmox, fichiers de configuration Suricata et ELK) est consultable dans les annexes du dossier technique du projet.

I. Pertinence de Kali Linux pour l'analyse défensive (Blue Team)

Kali Linux est principalement connu pour les tests d'intrusion (Red Team). Toutefois, son utilisation dans une optique de défense (Blue Team) pour héberger une sonde NIDS présente de forts avantages opérationnels :

1. **L'outillage d'analyse de trames natif**
   Lorsqu'un NIDS comme Suricata remonte une alerte de sécurité *(ex: détection d'un scan Nmap ou d'une tentative d'exploitation)*, l'administrateur doit s'assurer qu'il ne s'agit pas d'un faux positif. L'avantage d'avoir déployé la sonde sous Kali Linux est la présence native d'outils comme `Wireshark` ou `tcpdump`. Cela permet de lancer instantanément une capture réseau ciblée et d'analyser le contenu brut des paquets suspects, étape indispensable pour confirmer la réalité d'une attaque.

2. **Le système "Rolling Release"**
   Basé sur Debian Testing, Kali Linux fonctionne sur le principe de mises à jour continues *(Rolling Release)*. Dans un contexte de cybersécurité, ce modèle est un atout car il m'a permis de déployer facilement les versions les plus récentes du moteur Suricata et des agents Elastic, sans avoir à compiler les dépendances depuis le code source.

3. **Une gestion optimisée du réseau de bas niveau**
   Pour qu'un NIDS analyse du trafic qui ne lui est pas destiné *(Port Mirroring)*, la carte réseau doit fonctionner en écoute globale *(Mode Promiscuous)*. Le noyau de Kali Linux est nativement conçu pour la manipulation de trames brutes, ce qui garantit une interception fluide du trafic sans brider les performances de l'interface réseau.

II. Durcissement du système (Hardening) et Intégration

L'utilisation d'une distribution orientée sécurité offensive nécessite quelques adaptations. Afin de transformer cette machine en une véritable appliance de sécurité furtive, j'ai appliqué plusieurs mesures de durcissement :

- Séparation des environnements : La machine virtuelle hébergeant la sonde est strictement dédiée à l'écoute et à la détection. Les simulations d'attaques nécessaires pour tester les règles Suricata proviennent d'une autre machine virtuelle totalement isolée du réseau d'analyse.
- Furtivité réseau (Stealth Mode) : Il est impératif que la sonde n'interagisse pas avec le réseau de production. À l'aide de l'outil `nmcli` (NetworkManager), j'ai désactivé l'IPv4 et IPv6 sur les quatre interfaces dédiées à la capture de trames. Ainsi, la sonde analyse silencieusement les VLANs mais reste injoignable et invulnérable aux attaques directes.
- Sécurisation des journaux : La base de données Elasticsearch et le tableau de bord Kibana sont hébergés localement sur la sonde. Pour restreindre l'accès aux alertes, l'interface web Kibana n'écoute que sur l'adresse IP associée au VLAN d'administration (VLAN 99).

III. Piste d'amélioration et Veille technologique : Kali Purple

Ce projet m'a permis d'assimiler l'installation et l'interconnexion manuelle d'une chaîne de sécurité complète (interfaces réseau, moteur Suricata, agents Filebeat et pile Elasticsearch). Cependant, dans le cadre de ma veille technologique, j'ai identifié une solution plus aboutie pour l'apprentissage et le déploiement de scénarios de défense : Kali Purple.

Éditée par Offensive Security, cette distribution récente a été pensée pour faciliter le concept de Purple Teaming *(la collaboration active entre les équipes offensives et défensives)*. Alors que la version standard de Kali Linux est historiquement axée sur l'arsenal d'attaque (Red Team), Kali Purple fusionne les deux mondes en intégrant simultanément les outils de la Red Team et ceux de la Blue Team.