

Nouvelle page

1. IDS/IPS et Sécurité Périmétrique

IDS (Système de détection d'intrusions) : Il surveille le trafic réseau et alerte en cas de détection d'activités suspectes, mais il ne prend pas de mesures pour empêcher ces activités.

IPS (Système de prévention des intrusions) : Il va plus loin en bloquant ou en isolant le trafic potentiellement malveillant en temps réel.

Inconvénients:

1. Faux positifs

Détection basé sur la signature ,sur l'anomalie ou bien sur le comportement de l'utilisateur.

1. SNORT
2. ZEEK
3. SURICATA
4. CISCO

2. Gestion des identités et des accès (IAM - Identity and Access Management) :

IAM ensemble de processus et technologies => gérer et sécuriser les identités numériques / accès aux ressources IT d'une organisation.

Objectifs principaux :

- **Authentification** : Vérification de l'identité d'un utilisateur (ex : mots de passe, 2FA).
- **Autorisation** : Définition des permissions d'accès aux ressources après authentification (ex : accès à certaines applications, serveurs ou fichiers en fonction du rôle de l'utilisateur).
- **Provisionnement** : Création, modification et suppression des comptes utilisateurs et des droits d'accès au fur et à mesure que les employés rejoignent, quittent ou changent de poste dans l'entreprise.

- **Audit** : Vérification des logs d'accès pour s'assurer que l'accès aux ressources a été utilisé de manière appropriée

1. Compréhension des outils d'IAM comme **Active Directory**, **LDAP**, ou des solutions de gestion cloud comme **Azure AD**.
2. Différence entre **Single Sign-On (SSO)** et **Multi-Factor Authentication (MFA)**.
3. Processus d'audit d'accès et gestion des privilèges (principes du moindre privilège).

3. Analyse Forensique et Réponse aux Incidents :

- **Analyse Forensique** (en informatique) consiste à **examiner les systèmes informatiques** pour **collecter et analyser des données après un incident** de sécurité, en vue de **comprendre ce qui s'est passé**, comment cela s'est produit et qui est responsable.

- **Objectifs** :

- **Identifier** les causes d'un incident (ex : intrusion, vol de données).
- **Collecter** des preuves pour une éventuelle enquête (logs, fichiers suspects, empreintes d'intrusions).
- **Préparer des rapports détaillant** les vulnérabilités exploitées.

- **Réponse aux incidents** :

- C'est la réaction rapide à un incident de sécurité pour minimiser les impacts sur l'organisation. Elle inclut la détection, la gestion et la récupération après un incident.

- **Phases clés de réponse aux incidents** :

- **Préparation** : Avoir des plans en place, des outils et des équipes prêtes à répondre.
- **Identification** : Détection de l'incident (via monitoring, alertes).
- **Confinement** : Limiter l'impact (isoler les machines compromises, bloquer les ports).
- **Éradication** : Supprimer les causes de l'incident (suppression de malwares, correction de vulnérabilités).
- **Récupération** : Remettre les systèmes en ligne de manière sécurisée.
- **Leçons apprises** : Examiner l'incident pour éviter qu'il ne se reproduise.

Points clés à réviser :

- Outils et techniques d'analyse forensique (ex : analyse de logs, fichiers, images disque).
- Outils de réponse aux incidents comme **SIEM** (Security Information and Event Management).
- Connaissance des bonnes pratiques (ISO 27035, NIST Cybersecurity Framework).