IUT DE VILLETANEUSE

SAE401-CYB

SÉCURISER UN SYSTÈME D'INFORMATION

Réaliser par Rafael MAIA, Andon PENDICHEV et Jason LAMVU

SAE401-CYB

SOMMAIRE

SNORT

Snort est un IDS open source qui surveille le trafic réseau et détecte les activités suspectes.

Durant le TP, nous avons configuré des règles de détection et validé leur efficacité avec des tests d'attaque simulés.

KEEPASS

KeePass est un gestionnaire de mots de passe sécurisé qui stocke les identifiants dans un coffre-fort chiffré.

Dans un contexte TPRM, il permet de mieux protéger les accès critiques, à condition d'utiliser un mot de passe maître robuste, de limiter le partage et de vérifier les sauvegardes.

PFSENSE

pfSense est un pare-feu et routeur open source utilisé pour filtrer les flux et segmenter le réseau.

Dans nos travaux, il s'inscrit dans une logique de cloisonnement avec VLANs et contrôle des accès, ce qui permet de réduire la surface d'attaque et de mieux protéger les ressources sensibles.

ROOT - ME

L'un des challenge Root-Me réalisé portait sur une injection de commande dans un contexte SOC Web.

À partir de l'analyse des logs Apache et ModSecurity, nous avons identifié une activité malveillante, compris la méthode d'attaque et observé les impacts possibles, comme l'exécution de commandes à distance ou le déploiement d'un web-shell.

CONCLUSION

SAE401-CYB

DES QUESTIONS

ANDON PENDICHEV RAFAEL MAIA JASON LAMVU