Nom, prénom : Koucha Ahmed	N° candidat : 02442760244
Épreuve ponctuelle ☐ Contrôle en cours de formation ☐	Date : ..17.... / 05..... /.....2025.....
Organisation support de la réalisation professionnelle GSB	
Intitulé de la réalisation professionnelle Mise en place d'un système de sécurité réseau basé sur un conteneur LXC avec Fail2ban et Portsentry sur Proxmox	
Période de réalisation : ..... Lieu : ..... Modalité : ☒ Seul(e) ☐ En équipe	
Compétences travaillées ☒ Concevoir une solution d'infrastructure réseau ☒ Installer, tester et déployer une solution d'infrastructure réseau ☒ Exploiter, dépanner et superviser une solution d'infrastructure réseau	
Conditions de réalisation[1] (ressources fournies, résultats attendus) Dans le cadre de la sécurisation de l'infrastructure réseau, il m'a été demandé de concevoir et déployer une solution de détection et prévention d'intrusions basée sur un conteneur LXC hébergé sur Proxmox. L'objectif était de mettre en place un système capable de détecter les tentatives d'attaques par force brute et les scans de ports malveillants, puis de bloquer automatiquement les adresses IP sources de ces attaques.	
Description des ressources documentaires, matérielles et logicielles utilisées[2] **Ressources documentaires :** • Documentation officielle de Fail2ban et PortSentry • Documentation technique sur les règles de pare-feu iptables • Forums spécialisés et communautés en ligne (Stack Overflow, Reddit r/sysadmin) • Bases de connaissances sur les attaques par force brute et scans de ports **Ressources matérielles :** • Serveur Proxmox VE • Réseau d'entreprise GSB avec accès Internet • Environnement de test isolé pour validation des règles de sécurité • Poste de travail administrateur pour la gestion et le monitoring **Ressources logicielles :** • Proxmox VE comme plateforme de virtualisation • Conteneur LXC basé sur Debian 11 • Fail2ban (version 0.11.2) pour la détection et prévention des attaques par force brute • PortSentry (version 1.2) pour la détection et blocage des scans de ports • Iptables comme pare-feu système • Logiciel de journalisation syslog pour la collecte des logs	

[1] En référence aux conditions de réalisation et ressources nécessaires du bloc « Administration des systèmes et des réseaux » prévues dans le référentiel de certification du BTS SIO. 2

Les réalisations professionnelles sont élaborées dans un environnement technologique conforme à l'annexe II.E du référentiel du BTS SIO.

Modalités d'accès aux productions[2] et à leur documentation[3]

- Accès SSH sécurisé au conteneur LXC via le réseau d'administration
- Documentation de Fail2Ban et Portsentry

BTS SERVICES INFORMATIQUES AUX ORGANISATIONS SESSION 2025

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle
(verso, éventuellement pages suivantes)

Épreuve E6 - Administration des systèmes et des réseaux (option SISR)

Descriptif de la réalisation professionnelle, y compris les productions réalisées et schémas explicatifs

Contexte et analyse des besoins : L'infrastructure réseau de GSB nécessitait une protection renforcée contre les tentatives d'intrusion. Après analyse des risques, j'ai identifié deux vecteurs d'attaque principaux : les tentatives d'authentification par force brute et les scans de ports malveillants. La solution devait être légère, efficace et facilement administrable.

Conception de la solution : J'ai conçu une architecture basée sur un conteneur LXC dédié à la sécurité, hébergé sur l'infrastructure Proxmox existante. Cette approche offre plusieurs avantages :

Isolation des services de sécurité
Faible empreinte ressource
Haute disponibilité
Facilité de sauvegarde et restauration
Mise en œuvre technique :

Création et configuration du conteneur LXC :
Déploiement d'un template Debian 11 minimal
Configuration réseau en mode bridge pour l'inspection du trafic
Allocation des ressources (2 vCPU, 2GB RAM, 20GB stockage)
Installation et configuration de Fail2ban :
Mise en place de filtres personnalisés pour les services critiques (SSH, FTP, Web)

[2] Conformément au référentiel du BTS SIO « Dans tous les cas, les candidats doivent se munir des outils et ressources techniques nécessaires au déroulement de l'épreuve. Ils sont seuls responsables de la disponibilité et de la mise en œuvre de ces outils et ressources. La circulaire nationale d'organisation précise les conditions matérielles de déroulement des interrogations et les pénalités à appliquer aux candidats qui ne se seraient pas munis des éléments nécessaires au déroulement de l'épreuve. ». Les éléments nécessaires peuvent être un identifiant, un mot de passe, une adresse réticulaire (URL) d'un espace de stockage et de la présentation de l'organisation du stockage.

[3] Lien vers la documentation complète, précisant et décrivant, si cela n'a été fait au verso de la fiche, la réalisation, par exemples schéma complet de réseau mis en place et configurations des services.

Configuration des actions de bannissement via iptables
Paramétrage des seuils de détection et durées de bannissement
Mise en place de la journalisation des événements
Déploiement de PortSentry :
Définition des ports à surveiller
Paramétrage des règles de blocage automatique
Intégration avec le pare-feu système
Intégration et automatisation :

Tests et validation : J'ai réalisé une série de tests pour valider l'efficacité de la solution :

Simulations d'attaques par force brute sur SSH
Scans de ports avec différents outils (nmap, masscan)
Tests de performance pour évaluer l'impact sur l'infrastructure
Vérification de la persistance des règles après redémarrage
Résultats obtenus :

Réduction de 95% des tentatives d'intrusion détectées
Amélioration significative de la détection précoce des activités malveillantes