BTS SERVICES INFORMATIQUES AUX ORGANISATIONS **SESSION 2025**

ANNEXE 9-1-A : Fiche descriptive de réalisation professionnelle (recto)

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

DESCRIPTION D'UNE RÉALISATION PROFESSIONNELLE	**N° réalisation : 2**
Nom, prénom : Flory Ewan	**N° candidat :**
Épreuve ponctuelle ☐ **Contrôle en cours de formation** ☒	**Date :** 20 / 03 /2025

Organisation support de la réalisation professionnelle

CyberSecure Training Center est une organisation spécialisée dans la formation à la cybersécurité, offrant des environnements d'entraînement simulés pour les professionnels et étudiants souhaitant améliorer leurs compétences en défense et attaque informatique. L'organisation met à disposition une infrastructure de virtualisation pour les exercices Red Team / Blue Team, permettant une immersion réaliste dans la gestion des menaces cyber

Intitulé de la réalisation professionnelle

Entraînement Blue Team vs Red Team : Détection et réponse aux attaques sur une infrastructure virtualisée

Période de réalisation : Mars 2025..... **Lieu :** UTEC Avon.....
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)

Ressources fournies :

- **Matérielles :**
  - **Serveur physique pour l'hébergement de Proxmox**
  - **Machines virtuelles Kali Linux, Metasploitable et Suricata**
- **Logicielles :**
  - **Proxmox VE**
  - **Kali Linux avec Metasploit, Nmap**
  - **Metasploitable (machine volontairement vulnérable)**
  - **Ubuntu Server avec Suricata configuré en mode IDS/IPS**
- **Documentaires :**
  - **Documentation officielle de Suricata**
  - **Guides de prise en main Metasploit et Nmap**
  - **Tutoriels de déploiement sur Proxmox**

Résultats attendus :

- **Détection d'un scan réseau : Suricata génère une alerte lorsqu'un scan Nmap est détecté.**
- **Identification et blocage d'une attaque : Suricata intercepte et bloque une tentative d'exploitation de vulnérabilité via Metasploit.**
- **Analyse des logs : Les journaux d'activités sont exploités pour examiner les attaques et vérifier la réactivité du système IDS/IPS.**
- **Validation de l'efficacité de Suricata : Amélioration des règles de détection en fonction des tests effectués.**

Description des ressources documentaires, matérielles et logicielles utilisées[2]

Ressources matérielles

- **Serveur physique** : Hébergeant l'hyperviseur Proxmox, permettant la gestion et l'exécution des machines virtuelles.
- **Ordinateur personnel** : Utilisé pour l'administration de l'infrastructure via l'interface web de Proxmox.
- **Commutateur réseau (si applicable)** : Assure la communication entre les équipements physiques et le serveur d'hébergement.

Ressources logicielles

- **Proxmox VE** : Hyperviseur permettant la virtualisation des machines et la gestion centralisée de l'environnement de test.
- **Kali Linux** : Distribution spécialisée en tests d'intrusion, intégrant Metasploit, Nmap et d'autres outils de pentesting.
- **Metasploitable** : Machine volontairement vulnérable utilisée comme cible pour les attaques et tests de cybersécurité.
- **Suricata** : Système de détection et de prévention des intrusions (IDS/IPS) installé sur Ubuntu Server pour analyser le trafic réseau.
- **Wireshark (en option)** : Outil d'analyse réseau permettant de capturer et d'analyser le trafic pour observer les interactions entre les machines.

Ressources documentaires

- **Documentation officielle de Suricata** : Guide de configuration et d'optimisation des règles IDS/IPS.
- **Guides de Metasploit et Nmap** : Tutoriels pour exécuter des attaques simulées et comprendre leur impact sur un réseau.
- **Manuels Proxmox** : Aide à la gestion des VM et aux configurations réseau nécessaires pour l'environnement de test.
- **Rapports et articles sur la cybersécurité** : Références académiques et professionnelles sur les bonnes pratiques en matière de détection et de prévention des intrusions.

Modalités d'accès aux productions[3] et à leur documentation[4]

Les dossiers sont accessibles à l'adresse : https://ewan-flr.com/E6.html

[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.

[3] 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.

[4] 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.

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

Déploiement de l'infrastructure

L'ensemble du projet repose sur la mise en place d'une infrastructure de test sous **Proxmox**, permettant de simuler des attaques et d'analyser leur impact en environnement contrôlé.

Étapes de mise en place :

1. **Installation et configuration de Proxmox VE** sur un serveur physique.
2. **Création des machines virtuelles** :
   - **Kali Linux (Red Team)** avec Metasploit, Nmap et d'autres outils de pentesting.
   - **Metasploitable (Cible vulnérable)** utilisée pour tester différentes attaques.
   - **Suricata (Blue Team)** installé sur Ubuntu Server pour surveiller le trafic.
3. **Configuration du réseau virtuel** sur Proxmox :
   - Les trois machines sont connectées au même sous-réseau virtuel.
   - Suricata est configuré pour écouter l'ensemble du trafic réseau.
4. **Installation et configuration de Suricata** :
   - Définition de règles personnalisées pour détecter des attaques spécifiques.
   - Mise en place d'un mode **IDS** (détection) et **IPS** (prévention).

Productions réalisées

Infrastructure de virtualisation fonctionnelle avec les 3 VM sous Proxmox.
Configuration réseau entre Kali, Metasploitable et Suricata.
Déploiement et test des règles Suricata pour détecter les attaques.
Rapport d'analyse des tests avec les logs et résultats des attaques détectées.
Captures d'écran et schémas expliquant les interactions entre les machines.