Ewan FLORY

Mise en place d'un environnement d'entraînement Blue Team vs Red Team

Rapport situation professionnelle de l'épreuve E6 du BTS SIO (SISR)

Table des Matières

Contexte

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. Face à la demande croissante de formations pratiques en cybersécurité, l'organisation souhaite mettre à disposition une infrastructure de virtualisation permettant des exercices Red Team / Blue Team réalistes.

L'infrastructure actuelle du centre de formation ne dispose pas d'un environnement isolé et sécurisé pour pratiquer des attaques et défenses informatiques sans risque pour les systèmes de production. Les apprenants ont besoin d'un environnement où ils

peuvent réaliser des attaques offensives et mettre en place des mesures défensives dans un cadre contrôlé.

Le responsable technique du CyberSecure Training Center a donc décidé de mettre en place une plateforme virtualisée permettant la simulation d'attaques et la détection d'intrusions, afin de former les étudiants aux techniques modernes de cybersécurité.

Présentation de l'entreprise CyberSecure Training Center

CyberSecure Training Center est un organisme de formation spécialisé dans la cybersécurité, proposant des formations théoriques et pratiques à destination des professionnels de l'IT et des étudiants. Présent sur le marché depuis plusieurs années, le centre s'est rapidement imposé comme une référence dans le domaine de la formation en sécurité informatique.

L'entreprise dispose d'une équipe d'experts certifiés dans différents domaines de la cybersécurité, capables d'accompagner les apprenants dans leur montée en compétences, de la sensibilisation basique aux techniques avancées d'attaque et de défense.

CyberSecure Training Center propose plusieurs types de formations :

- Formations certifiantes (CEH, CISSP, Security+)
- Ateliers pratiques sur la sécurité offensive et défensive
- Sessions d'entraînement Red Team / Blue Team
- Formations sur mesure pour les entreprises

Ewan FLORY, faisant partie de l'équipe pédagogique du centre, est chargé de mettre en place l'infrastructure virtualisée qui servira de support aux exercices pratiques.

Objectif

L'objectif principal de cette réalisation professionnelle est de concevoir et déployer un environnement d'entraînement virtualisé permettant la simulation d'attaques informatiques et leur détection par des systèmes de sécurité. Cette infrastructure doit répondre aux besoins pédagogiques du centre en matière de formation pratique à la cybersécurité.

Pour cela, nous devrons :

➢ **Analyser les besoins pédagogiques** : Comprendre les exigences spécifiques des formations Red Team / Blue Team en termes de scénarios d'attaque, de détection et de réponse aux intrusions.

➢ **Concevoir une infrastructure virtualisée adaptée** : Proposer une solution technique basée sur la virtualisation, permettant de simuler des réseaux isolés où peuvent se dérouler des attaques sans risque pour les systèmes de production.

➢ **Déployer des outils offensifs et défensifs** : Intégrer des outils d'attaque (Red Team) et des systèmes de détection (Blue Team) dans l'environnement virtualisé pour permettre la pratique des deux aspects de la cybersécurité.

➢ **Tester et valider le bon fonctionnement** : S'assurer que les attaques peuvent être réalisées et détectées conformément aux objectifs pédagogiques.

Cette infrastructure devra être à la fois performante, sécurisée et adaptée à un usage pédagogique, tout en étant facilement déployable et maintenable.

Solution proposée

Après analyse des besoins du CyberSecure Training Center, la solution proposée consiste à créer un environnement de virtualisation complet basé sur les éléments suivants :

➢ **Mise en place d'un hyperviseur Proxmox VE** : Installation et configuration de Proxmox sur un serveur physique pour gérer les machines virtuelles de l'environnement d'entraînement.

➢ **Déploiement d'une machine virtuelle Kali Linux (Red Team)** : Configuration d'une VM Kali Linux intégrant des outils d'attaque comme Metasploit et Nmap pour la réalisation des exercices offensifs.

➢ **Installation d'une machine virtuelle Metasploitable (Cible)** : Déploiement d'une VM volontairement vulnérable servant de cible pour les exercices d'attaque.

➢ **Configuration d'une machine virtuelle Suricata (Blue Team)** : Mise en place d'un système de détection et de prévention d'intrusion (IDS/IPS) sur Ubuntu Server pour la détection des attaques.

➢ **Configuration d'un réseau virtuel isolé** : Création d'un sous-réseau virtuel où les trois machines peuvent communiquer entre elles sans compromettre le reste du réseau.

Cette solution permet de créer un environnement complet de formation pratique à la cybersécurité, avec des outils réels utilisés dans l'industrie, tout en garantissant l'isolation des activités potentiellement dangereuses.

Ressources nécessaires et coût financier

La mise en place d'un environnement d'entraînement Blue Team vs Red Team nécessite plusieurs ressources matérielles, logicielles et humaines.

Les ressources sont les suivantes :

➢ **Matérielles** :

- Un serveur physique pour l'hébergement de l'hyperviseur Proxmox
- Ressources minimales recommandées : 2 CPU Cores, 8 Go de RAM, 50 Go d'espace disque
- Un ordinateur administrateur pour gérer l'infrastructure via l'interface web de Proxmox
- Réseau local avec accès internet pour le téléchargement des images et logiciels

➢ **Logicielles** :

- Proxmox VE (open source)
- Image ISO de Kali Linux
- Image disque de Metasploitable 2
- Image ISO d'Ubuntu Server pour Suricata
- Outils de virtualisation et de cybersécurité (Metasploit, Nmap, Wireshark)

➢ **Humaines** :

- Temps de configuration et de déploiement de l'infrastructure
- Formation des formateurs à l'utilisation de l'environnement

Les coûts financiers sont les suivants :

➢ **Matériel** :

- Serveur dédié : entre 1500€ et 3000€ selon les performances requises
- Coûts de maintenance et d'électricité

➢ **Logiciels** :

- Proxmox VE : gratuit (open source)
- Kali Linux : gratuit (open source)
- Metasploitable : gratuit (open source)
- Ubuntu Server : gratuit (open source)
- Suricata : gratuit (open source)

➢ **Main d'œuvre** :

- Installation et configuration : environ 3 jours de travail d'un administrateur système (environ 1500€)
- Documentation et formation : 1 jour (environ 500€)

Solutions alternatives et concurrentes

Pour la mise en place d'un environnement d'entraînement à la cybersécurité, plusieurs solutions alternatives à notre proposition existent sur le marché.

Tableau comparatif des solutions d'environnement d'entraînement à la cybersécurité :

Caractéristiques / Solutions	**Solution proposée (Proxmox + Kali + Metasploitable + Suricata)**	**VMware vSphere + Security Onion**	**AWS Cyber Range**
Année de réalisation	2025	2020	2018
Description	Solution basée sur des outils open source pour créer un environnement d'entraînement isolé.	Solution basée sur l'hyperviseur VMware avec une distribution dédiée à la détection d'intrusion.	Environnement cloud public permettant de simuler des attaques et défenses à grande échelle.
Simple d'utilisation	★★★	★★	★★★★
Prix	Gratuit (hors matériel)	Payant (licences VMware)	Payant (facturation à l'usage)
Flexibilité	★★★★	★★★	★★
Performance	★★★	★★★★	★★★★
Isolation	★★★★	★★★	★★

Caractéristiques de la solution

Proxmox VE

Proxmox Virtual Environment (VE) est une plateforme de virtualisation open source qui intègre un hyperviseur KVM et des conteneurs LXC. C'est la base de notre infrastructure d'entraînement.

Les principales fonctionnalités : ➢ Gestion centralisée des machines virtuelles via une interface web ➢ Support de multiples formats de stockage (local, NFS, iSCSI) ➢ Haute disponibilité et clustering ➢ Gestion avancée des réseaux virtuels ➢ Snapshots et backups ➢ Monitoring intégré ➢ Interface web intuitive pour la gestion des VM

Kali Linux

Kali Linux est une distribution Linux spécialisée dans les tests de pénétration et l'audit de sécurité. Elle sera utilisée comme machine d'attaque (Red Team) dans notre infrastructure.

Les principales fonctionnalités : ➢ Plus de 600 outils préinstallés pour les tests de pénétration ➢ Framework Metasploit pour l'exploitation de vulnérabilités ➢ Outils de reconnaissance comme Nmap ➢ Applications d'analyse de trafic réseau ➢ Outils de craquage de mots de passe ➢ Environnement de développement pour les scripts personnalisés d'attaque ➢ Interface graphique intuitive pour les débutants

Metasploitable

Metasploitable est une machine virtuelle Linux délibérément vulnérable, conçue pour les tests de pénétration et la formation à la sécurité. Elle servira de cible pour les exercices d'attaque.

Les principales fonctionnalités : ➢ Multiples services vulnérables préinstallés ➢ Versions obsolètes et non patchées de logiciels courants ➢ Configurations par défaut et faibles ➢ Vulnérabilités documentées et exploitables ➢ Conception spécifique pour l'apprentissage des techniques d'exploitation ➢ Environnement contrôlé pour tester les attaques sans risque légal

Suricata

Suricata est un moteur de détection d'intrusion open source capable de fonctionner en mode IDS (détection) et IPS (prévention). Il sera utilisé comme outil de défense (Blue Team) dans notre infrastructure.

Les principales fonctionnalités : ➢ Détection de signatures d'attaques connues ➢ Analyse du trafic réseau en temps réel ➢ Support des protocoles réseaux modernes ➢ Journalisation complète des événements ➢ Possibilité de créer des règles personnalisées ➢ Mode passif (IDS) ou actif (IPS) ➢ Performances optimisées pour le traitement de grands volumes de données

Les contraintes

La mise en place d'un environnement d'entraînement Blue Team vs Red Team présente plusieurs contraintes techniques et organisationnelles :

- **Ressources matérielles** : Le serveur doit disposer de ressources suffisantes pour faire fonctionner plusieurs VM simultanément sans dégradation des performances.
- **Isolation réseau** : L'environnement doit être parfaitement isolé du réseau de production pour éviter toute compromission accidentelle des systèmes réels.
- **Gestion des mises à jour** : L'environnement doit maintenir certaines vulnérabilités intentionnellement pour les besoins pédagogiques, tout en garantissant que ces failles ne puissent pas être exploitées en dehors de l'environnement contrôlé.
- **Compétences techniques requises** : La mise en place et la maintenance de l'infrastructure nécessitent des compétences avancées en virtualisation et en cybersécurité.
- **Adaptation pédagogique** : Les scénarios d'attaque et de défense doivent être conçus pour être à la fois réalistes et adaptés au niveau des apprenants.

Plan d'adressage IP

Équipements	**Adresses IP**
Proxmox (Interface physique)	10.0.0.1/24
Réseau virtuel interne	192.168.1.0/24
Kali Linux (Red Team)	192.168.1.10/24
Metasploitable (Cible)	192.168.1.77/24
Suricata (Blue Team)	192.168.1.100/24

Mise en œuvre de la situation professionnelle

La mise en œuvre de l'environnement d'entraînement Blue Team vs Red Team se déroule en plusieurs étapes :

➢ **Installation et configuration de Proxmox VE** :

- Installation de Proxmox VE sur le serveur physique
- Configuration de l'interface réseau et de l'accès administrateur
- Configuration du stockage pour les machines virtuelles

➢ **Création et configuration des machines virtuelles** :

- Téléchargement des images ISO nécessaires

- Création de la VM Kali Linux avec allocation de 2 Go de RAM et 2 CPU cores
- Configuration de la VM Metasploitable à partir de l'image disque
- Création de la VM Ubuntu Server pour Suricata avec 2 Go de RAM et 2 CPU cores

➢ **Configuration de Suricata** :

- Installation de Suricata sur la VM Ubuntu Server
- Configuration de l'interface réseau en mode promiscuous
- Adaptation du fichier de configuration pour surveiller le trafic réseau
- Activation du service Suricata en mode IDS/IPS

➢ **Configuration du réseau virtuel** :

- Création d'un réseau virtuel isolé dans Proxmox
- Attribution des adresses IP statiques aux machines virtuelles
- Vérification de la connectivité entre les VM

➢ **Tests de fonctionnement** :

- Exécution d'un scan Nmap depuis Kali Linux vers Metasploitable
- Vérification de la détection de l'attaque dans les logs de Suricata
- Test d'une exploitation via Metasploit et vérification de sa détection
- Ajustement des règles de détection si nécessaire

Problèmes rencontrés

Lors de la mise en œuvre de cet environnement d'entraînement, plusieurs défis techniques ont dû être relevés :

1. **Problème d'importation de l'image Metasploitable** : Lors de la configuration de Metasploitable dans Proxmox, nous avons rencontré des difficultés pour importer l'image disque. Le format VMDK n'était pas directement compatible. Nous avons résolu ce problème en convertissant l'image au format qcow2 compatible avec Proxmox.
2. **Configuration de l'interface réseau de Suricata** : Initialement, Suricata ne détectait pas le trafic réseau car l'interface configurée dans le fichier de configuration ne correspondait pas à l'interface réelle du système. Après vérification avec la commande ip a, nous avons modifié le fichier /etc/suricata/suricata.yaml pour utiliser l'interface correcte (ens18).

3. **Visibilité des logs** : Les logs de Suricata n'étaient pas facilement accessibles en temps réel. Pour améliorer la visualisation, nous avons installé l'outil Frontail qui permet de suivre les logs en direct via un navigateur web.

Résultat

Une fois toutes ces étapes réalisées avec succès, l'environnement d'entraînement Blue Team vs Red Team est pleinement fonctionnel et permet de réaliser des exercices pratiques de cybersécurité dans un cadre contrôlé et sécurisé.

Les formateurs et apprenants peuvent désormais :

- Réaliser des scans de vulnérabilités avec Nmap et observer leur détection par Suricata
- Exploiter des vulnérabilités connues sur Metasploitable via Metasploit
- Analyser les logs de détection pour comprendre les indicateurs d'une attaque
- Configurer des règles personnalisées dans Suricata pour améliorer la détection
- Pratiquer la réponse à incident en analysant les alertes générées

Cette infrastructure virtualisée offre ainsi un environnement d'apprentissage pratique et réaliste, permettant aux apprenants de développer leurs compétences en attaque et défense informatique, essentielles pour les métiers de la cybersécurité.