Le contexte BOXTOBED

Source : https://www.reseaucerta.org/labo-bloc3-kali

L'organisation cliente

BOXTOBED est une chaîne d'hôtels fondée en 2019 qui s'appuie sur le concept de logements conteneurs. Les bâtiments de BOXTOBED sont construits par empilement de conteneurs de marchandises mesurant 9 m².

Les chambres sont ainsi proposées à un prix très abordable pour des clients recherchant une solution simple et économique d'hébergement. Fort d'une croissance rapide de son activité, le gérant de BOXTOBED souhaite auditer la sécurité de son infrastructure numérique avant de proposer de nouveaux services à ses clients.

Le prestataire informatique

INFOSUR est une entreprise spécialisée en déploiement de solutions informatiques dans le domaine de la cybersécurité. Elle analyse les besoins de ses clients et propose des solutions pour développer leur sécurité numérique en conformité avec le RGPD via la réalisation de tests d'intrusion (pentest).

> **Pentest :**
>
> Prestation sur mesure de **test de pénétration** visant à tester la sécurité d'une infrastructure numérique

Votre mission

Vous êtes une personne salariée de l'entreprise INFOSUR affectée au service du support informatique. Vous participez à l'étude du projet numérique de BOXTOBED et votre mission consiste à préparer l'intégration de la solution du client BOXTOBED. Cette préparation se fera sur une **maquette de test constituée de machines virtuelles** afin de préparer le projet.

Les besoins exprimés par le gérant de BOXTOBED

- auditer la sécurité du réseau informatique et des applications ;
- assurer la sécurité des données à caractère personnel : les données doivent restent privées (confidentialité) et ne fassent l'objet d'aucune falsification (intégrité).
- disponibilité du réseau pour l'accès Internet et pour la téléphonie à toute heure : prévenir les ruptures d'accès qui pourraient nuire la réputation de BOXTOBED.
- des inquiétudes sur la sécurité du site Web ;
- inquiétudes sur les vulnérabilités possibles des solutions libres téléchargées gratuitement sur internet.

Schéma de la maquette de test

Le schéma de la maquette (proposé par INFOSUR) servant de base de travail à vos missions est le suivant :

Proposition de plan d'adressage IP

Machines	Descriptions	Adresse IP	
Client légitime	Machine linux ou windows avec un navigateur	192.168.50.10/24	192.168.50.254
Hacker	Machine virtuelle Kali Linux	192.168.50.20/24	192.168.50.254
Serveur Mutillidae	Machine virtuelle metasploitable	172.16.10.5/24	172.16.10.254
Firewall	Firewall stormshield sous forme de machine virtuelle	interface 1 : 172.16.10.254 \\interface 2 : 192.168.50.254	Interface 3 : sortie internet via le réseau du lycée

Kali

Kali Linux est une distribution basée sur Debian regroupant l'ensemble des outils nécessaires aux tests de sécurité d'un système d'information, notamment le test d'intrusion.

L'intérêt de Kali Linux est de comporter près de 300 outils déjà installés pour travailler dans le domaine de la cybersécurité.

- Identifiant/mot de passe de connexion : kali / kali.
- Pour avoir un clavier français, lancer la commande : setxkbmap fr depuis une fenêtre shell.

Pour installer la VM Kali :

- lancez **VirtualBox** ;
- **importez** la l'archive **kali-linux-2021.3-virtualbox-i386.ova** en réinitialisant les adresses MAC.
- Modifiez le mode d'accès réseau pour définir le mode d'accès **par pont (Bridged)**.

Metasploitable

Metasploitable (version 2.0.0) est une distribution linux (ubuntu) intentionnellement vulnérable.

Son objectif est d'apprendre à tester les principales vulnérabilités en liaison avec la distribution Kali Linux (https://sourceforge.net/projects/metasploitable).

- Première connexion : msfadmin / msfadmin.
- Pour avoir un clavier en français, il faut saisir la commande loadkeys fr puis valider. C'est sur ce serveur que sera disponible le site mutillidae.

Pour installer la VM **Multidae** :

- **décompressez** l'archive **metasploitable-linux-2.0.0.zip**
- lancez **VirtualBox** ;
- Créez une nouvelle VM en définissant une RAM de 512 MO et en choisissant d'utiliser le disque dur existant **Metasploitable.vmdk** présent dans l'archive avec le mode d'accès **par pont (Bridged)**.