TP2– Attaque interne (3h)

Vous avez été embauché pour pentester l'architechture de l'entreprise SecurityMake qui se présente comme le spécialiste de la sécurité en France.

Pour cela, vous allez réaliser des tests d'intrusion sur le réseau, applicatif, et infrastructure informatique. Vous prendrez soin d'effacer vos traces :

Chaîne de frappe d'une cyber attaque

Etape 1 : Reconnaissance Exploration de l'environnement
Etape 2:Déploiement des armes : Détermination de l'identifiant de connexion à l'administration et du mot de passe
Etape 3 Livraison : Elevation de privilège
Etape 4 Exploitation :Connexion à la machine hôte
Etape 5 Installation : localisation des donées
Etape 6 Commande et contrôle : Extraction des données
Etape 7 Action : Destruction des données et du site effacer vos traces

Durée de l'attaque 3H

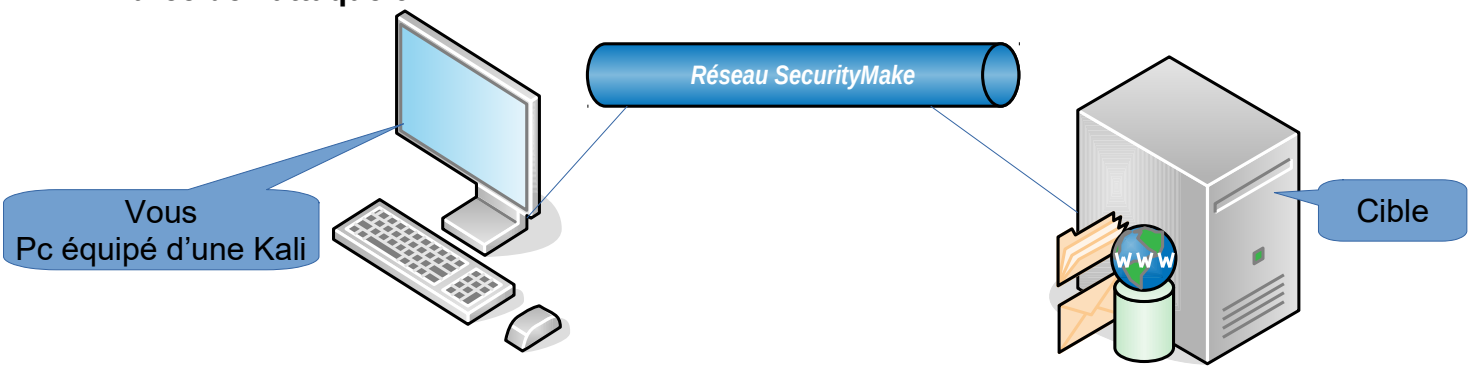


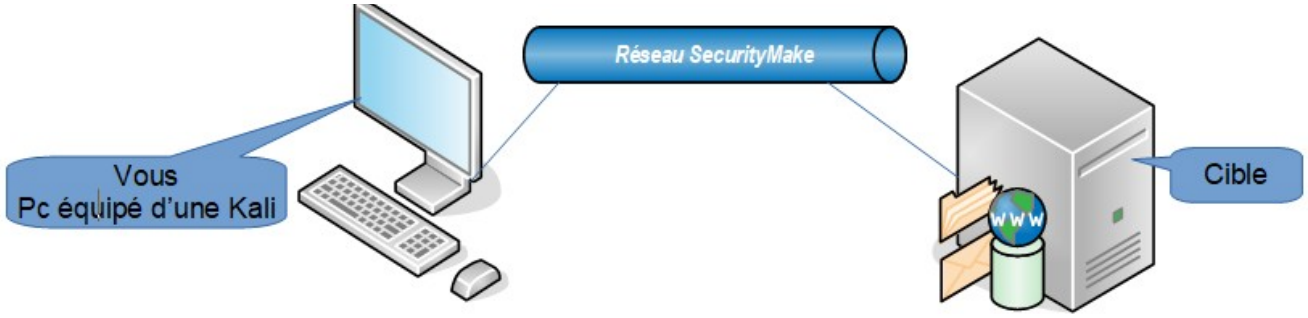
Schéma de topologie

Outils nécessaires :

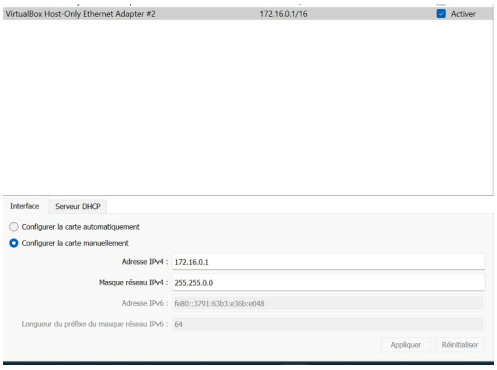
- Une Kali Linux.ova et Cible.ova

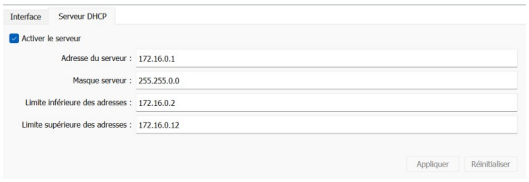
Importer l'infrastructure dans virtual box

Réalisez ce réseau :



montage Réseau privé hôte Activé

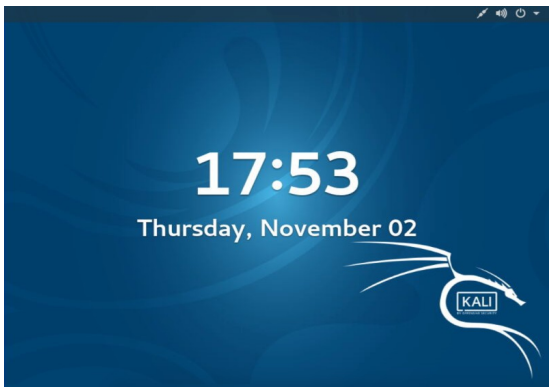




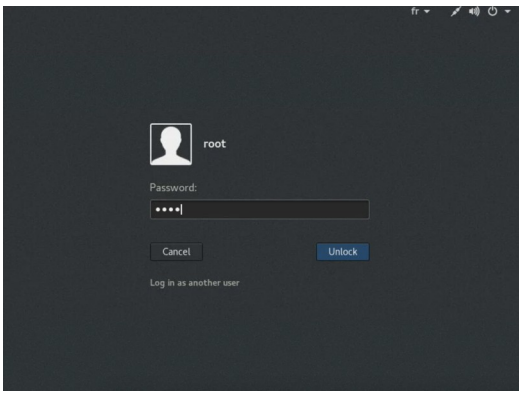
Étape 1:

Préparation et connexion à la machine virtuelle Linux Kali

Connectez vous à la kali :



Rentrez alors le mot de passe du compte administrateur : `kali`



Vous devriez alors obtenir l'accès à la machine virtuelle Kali, comme décrit :

Étape 1: Découverte de l'environnement

⇨ Identifiez les paramètres de la deuxième interface réseau (*eth1*) de la machine virtuelle Kali

⇨ Découvrez les machines actives dans votre sous-réseau ainsi que la machine cible.

Note : la machine cible peut être identifiée aisément ici, 172.16.0.22.

⇨ Scannez les services actifs sur la machine cible

Étape 2: Exploration de votre environnement

⇨ En fonction des résultats de l'étape précédente, explorez la ressource que vous avez découvert et ses contenus.

Étape 3: Détermination de l'identifiant de connexion à l'administration

⇨ Déterminez le nom d'utilisateur pour vous connecter à l'administration du site

Étape 4: Détermination du mot de passe de connexion à l'administration

⇨ Déterminez le mot de passe pour vous connecter à l'administration du site

Étape 5: Trouvez un moyen pour escalader votre compte en tant qu'administrateur

⇨ Trouvez un moyen pour faire de votre utilisateur un administrateur du site

Étape 6: Connexion à la machine hôte

⇨ Connectez-vous à la machine hôte à l'aide des informations découvertes

Étape 7: Localisation de données

⇨ Essayez de déterminer comment les données clientes sont stockées et comment vous connecter à celles-ci

Étape 8: Extraction des données (bonus)

⇨ Accédez à la base sans réinitialiser le mot de passe administrateur

⇨ Explorez la base de données et ses données

⇨ Exportez la base de données vers un fichier local

⇨ Exportez le fichier d'export de base vers un hôte extérieur

Étape 9: Destruction des données clients et du site

⇨ Trouvez une façon de détruire les données de bases de données utilisées pour les clients et le site Internet

Étape 10: Vérification des résultats

⇨ Vérifiez avec l'instructeur en charge de l'évènement que vous avez bien récupéré toutes les informations de la base de données

Étape 11: Effacez vos traces

⇨ Trouvez une façon de détruire l'historique des commandes tapées pendant votre session