Atelier 1 : Premiers Pas

Dans cet atelier, vous allez installer Kali et Metasploitable2 sur votre ordinateur, et faire une brève visite des systèmes en prévision des prochains travaux plus approfondis.

Partie 1 – Configuration de l'infrastructure

Suivez les instructions de la fiche de l'atelier 0 « **configuration de la machine virtuelle** » pour télécharger et installer Kali et Metasploitable2 en tant que machines virtuelles. Faites une capture d'écran comme preuve de travail.

Remarque : n'utilisez pas d'appareil photo numérique pour prendre une photo de votre écran. La qualité du résultat varie de marginale au mieux à embarrassante au pire. Utilisez la fonction de capture d'écran de Windows ou de Mac pour accomplir cette tâche.

Livrables :

- Mettre sur le rapport une seule capture d'écran montrant :
  0. La VM Kali en cours d'exécution, connectée, et sur le bureau prête à être utilisée.
  1. La VM Metasploitable2 en cours d'exécution et à l'invite de commande, prête à être utilisée.
  2. Le gestionnaire de tâches de Windows ou le moniteur d'activité de Mac ou encore la liste des processus sous tout autre OS Unix montrant l'utilisation des ressources du système avec les deux VM et votre OS hôte fonctionnant simultanément. Plus précisément, assurez-vous que l'utilisation de la mémoire (RAM) est affichée.
  3. Un éditeur de texte ouvert dans Kali avec votre nom et la date du jour clairement écrits à l'intérieur.

Partie 2 – Analyse du réseau

Tout d'abord, à partir du terminal de votre VM Metasploitable2 en cours d'exécution, trouvez son adresse IP.

Référence : Exemples de commandes Linux IP

Ensuite, à partir du terminal de votre VM Kali, utilisez `nmap` pour rechercher les services réseau ouverts dans la VM Metasploitable2. Ciblez l'adresse IP que vous avez trouvée précédemment, et scannez tous les ports (0-65535).

Référence : Exemples de lignes de commande Nmap

Comme vous avez scanné la VM Metasploitable2, presque tous les services actifs listés ont une vulnérabilité de sécurité sous une forme ou une autre. Choisissons-en un – NFS, le système de fichiers réseau, pour l'examiner de plus près.

Livrables :

- Quelle commande avez-vous utilisée pour trouver l'adresse IP de votre VM Metasploitable2 ?
- Quelle commande avez-vous utilisée pour l'analyse nmap ? La commande doit cibler une adresse IP spécifique et analyser les ports 0-65535.
- D'après les résultats de votre analyse nmap, sur quel port TCP le service nfs écoute-t-il ?

Partie 3 – NFS

Le système de fichiers réseau (NFS) de la VM Metasploitable2 présente une faiblesse importante.

Tout d'abord, à partir du terminal de la VM Kali, utilisez la commande `showmount` pour trouver la **liste d'exportation** de la VM Metasploitable2. La liste d'exportation est l'ensemble des répertoires qui sont rendus accessibles via NFS, et les adresses IP/sous-réseaux qui sont autorisés à y accéder.

Référence : man showmount
Référence : man exports

Livrables :

- Quelle est la liste d'exportation pour la VM Metasploitable2 ? Et surtout, que signifie cette liste d'exportation ? Expliquez avec vos **propres mots**.

Deuxièmement, abusons maintenant de notre accès NFS.

Sur votre VM Kali, accomplissez les tâches suivantes :

1. Générez une nouvelle clé SSH à l'aide de la commande ssh-keygen. Acceptez l'emplacement par défaut de la clé afin que SSH puisse trouver le fichier à l'avenir (`~/.ssh/id_rsa`). Laissez la phrase de passe vide afin qu'il n'y ait pas de confusion sur le fait que vous ayez un accès sans mot de passe ou non.

Référence : ssh-keygen

2. Montez le disque NFS de Metasploitable2 en utilisant la commande mount, afin de pouvoir accéder aux fichiers distants dans Kali. Pour ce faire, vous devrez d'abord créer un répertoire vide dans Kali comme point de montage où les fichiers réseau apparaîtront. Je suggère un emplacement comme /tmp/metasploitable. Afin de monter un disque réseau, vous devez être root, donc utilisez sudo dans votre commande.

Référence : Comment monter un partage NFS sous Linux

3. En utilisant le disque NFS monté, ajoutez votre clé publique SSH (le fichier se terminant par .pub, comme indiqué dans la sortie de ssh-keygen) à la fin du fichier existant `root->.ssh->authorized_keys` dans la VM Metasploitable2. Cela vous donnera un accès SSH sans mot de passe à ce système, car votre client SSH utilisera automatiquement votre clé pour s'authentifier. **Remarque** : vous devez être root dans la VM Kali pour éditer ce fichier en tant que root dans la VM Metasploitable2. NFS transmet simplement votre numéro d'identification d'utilisateur (0, pour root) à travers le réseau.

Référence : man cat

Remarque : Cette commande est légèrement délicate à réaliser avec sudo si vous voulez utiliser la redirection de sortie ! (ce que je suggère). Une astuce courante consiste à écrire votre commande comme ceci :

`sudo sh -c 'COMMANDE >> Fichier_de_sortie'`

4. Démontrez que vous avez accompli cette tâche en effectuant la séquence suivante, et en prenant une capture d'écran de la séquence complète **a – d** :
   a. Depuis votre VM Kali, montrez votre nom d'hôte : hostname (devrait être kali ou tout autre nom d'hôte que vous avez choisi lors de l'installation de la VM Kali)
   b. SSH depuis la VM Kali vers la VM Metasploitable2 en tant qu'utilisateur root. La commande doit être ssh root@xx.xx.xx.xx, où xx.xx.xx.xx est l'adresse IP de la VM

Metasploitable2 que vous avez identifiée précédemment. Si vous avez correctement ajouté votre clé publique au fichier `authorized_keys` précédemment, lorsque vous essayez de vous connecter en SSH au système et que vous présentez automatiquement votre clé privée, vous devriez obtenir un accès immédiat, sans mot de passe.

c. A l'invite, montrez à nouveau votre nom d'hôte : `hostname` (devrait être `metasploitable`)

d. Quittez SSH via `exit` pour revenir à Kali.

Correction de bug : Kali est une distribution Linux de dernière génération, et Metasploitable2 est très ancien. La version actuelle de Kali ne prend en charge que les algorithmes de hachage de certificats SSH les plus récents et les plus sûrs, mais l'ancien système Metasploitable2 ne prend en charge que des algorithmes que Kali (et les clients OpenSSH récents) ont dépréciés ! Pour plus d'informations, voir cet article. Pour résoudre ce problème, exécutez la commande suivante pour éditer votre fichier de configuration SSH afin de forcer SSH à supporter les anciens algorithmes de hachage :

```
echo -e "Host *\nPubkeyAcceptedKeyTypes=+ssh-rsa\nHostKeyAlgorithms=+ssh-rsa" >> ~/.ssh/config
```

Livrables :

- Soumettez une capture d'écran démontrant que vous avez réussi à insérer votre clé privée dans la VM Metasploitable2 et que vous pouvez maintenant vous connecter sans mot de passe à ce système en tant qu'utilisateur root.