Metasploit - Enumeration

L'**énumération** désigne le processus de collecte d'informations sur une cible dans le but d'identifier des faiblesses exploitables. Cela implique d'examiner en détail un système, un réseau ou un service pour en tirer des données qui pourraient être utilisées pour mener une attaque ou une exploitation. L'énumération est donc une phase préalable à l'exploitation des vulnérabilités, permettant de mieux connaître la cible et de maximiser les chances de réussite d'une attaque.

La commande **db_nmap** dans Metasploit est une version intégrée de l'outil **Nmap** utilisé pour effectuer des analyses réseau tout en stockant automatiquement les résultats dans la base de données de Metasploit. Cela permet de centraliser les informations obtenues à partir de l'analyse Nmap directement dans Metasploit, facilitant ainsi l'exploitation et le suivi des découvertes.

1) Exécutez msfconsole et vérifiez que la connexion à la base de données Metasploit est active. `msf6 > db_status`

2) Une commande qui permet le scan d'une machine est la suivante : `msf6 > db_nmap -sS -sV -O -PN -p- @_IP`, recherchez et expliquez chaque partie de la commande.

3) Testez la commande précédente sur vos machines connectées.

4) Afficher les machines et les services trouvés : `msf6 > hosts` `msf6 > services`

5) En vous servant de l'aide de la commande **services** `msf6 > services -help` :

- Rechercher le service FTP.
- Rechercher les services actifs sur les ports 21 et 22.
- Rechercher des services par nom, numéro de port et état.

6) En vous servant de l'aide de la commande **hosts,** afficher les machines par nom et adresse.

7) Il existe plusieurs autres modules qui peuvent être utilisés pour scanner les ports. Recherchez des modules auxiliaires qui peuvent scanner des ports : `msf6 > search portscan type:auxiliary`

8) Utilisez le module `auxiliary/scanner/portscan/syn` pour scanner vos machines.

9) Le **service SMB** permet le partage de ressources sur des réseaux locaux avec des PC sous Windows.

- Quels sont les ports utilisés par le service SMB ?

- Effectuez une recherche de ces ports dans la base Metasploit.

- Trouvez les modules auxiliaires pour le service SMB.

- Utilisez le module approprié pour déterminer la version de SMB installée sur vos machines.

- Microsoft a publié un bulletin de sécurité très critique (MS17-010) concernant une faille de sécurité du service SMB. Il existe un module Metasploit permettant de vérifier si une machine est vulnérable ou non à cette faille. Trouvez le module correspondant, puis scannez vos machines.

- Le module **auxiliary/scanner/smb/smb_login** permet de trouver le mot de passe d'un utilisateur SMB par force brut. Afficher les options du module.

- CeWL (Custom Word List Generator) est une application Ruby qui explore une URL donnée jusqu'à une profondeur spécifiée, puis renvoie une liste de mots pouvant ensuite être utilisée pour craquer les mots de passe. Dans un autre terminal créer un dictionnaire de mots de passe à l'aide de la commande **cewl** :

```
$ cewl -d 5 -m 7 -w /home/kali/Desktop/mon_fichier_passwd.txt   https://github.com/rapid7/metasploitable3
```

Remarque : la génération des mots de passes prend un certain temps. Arrêtez le processus après quelques secondes.

- Expliquez chaque paramètre de la commande.

- Utilisez le fichier généré pour tenter de trouver le mot de passe de l'utilisateur **vagrant** à l'aide du module précédant.

- L'utilisateur victime est aussi configuré dans le serveur de la machine 10.0.0.7

- À l'aide de l'outil **Crunch**, générer une liste de mots de passe pour pirater le serveur (Supposez que le mot de passe est composé de **six** caractères et contient les caractères **c r s t 3**).

- Utilisez le fichier généré pour tenter trouver le mot de passe de l'utilisateur **victim** à l'aide du module précédant. Cette partie est juste un test pour l'utilisation de Crunch, vous ne devriez pas trouver le mot de passe.

10) Listez les versions MySQL et FTP installées sur les serveurs.

- Il existe sur Internet des fichiers listant les noms d'utilisateur et les mots de passe par défaut pour différents services. Ci-dessous, un fichier pour le service FTP :

https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/ftp-betterdefaultpasslist.txt

Essayez de trouver les noms d'utilisateur et les mots de passe du service FTP des serveurs par Brut Force. (**Remarque** : vous devez remplacer les « : » par de espaces dans le fichier avant de l'utiliser)

11) En suivant la même démarche énumérez les services HTTP installés sur les serveurs.

- On s'intéresse au service Apache 2.2.8. Utiliser le module **auxiliary/scanner/http/crawler** pour trouver l'arborescence de ces serveurs.

12) énumérer les services smtp installés
- connectez-vous via telnet au por snmp trouvé
- utiliser la commande **vrfy** pour vérifier les noms d'utilisateurs suivant : admin, root, metasploit, sys.
- Trouvez la version du service smtp
- Utilisez le module smtp_enum pour trouver tous les utilisateurs.