Metasploit

msf >

Préfixe qui signifie que vous interagissez avec Metasploit

search name:Microsoft type:exploit

Trouve la localisation de votre requête. Ici, on cherche les failles liée à Microsoft. **name** est le nom de votre objet et **type** est le type de script que vous cherché.

info auxiliary/admin/http/iis_auth_bypass

Donne les informations du module ou de la platform, où il est utilisé, qui est l'auteur, les vulnérabilité référencées et les restrictions payload

Armitage GUI (Metasploit)

Lancer Armitage dans la rubrique Exploit Tools. Entrée les informations requises et cliqué sur **Connect**. C'est un programme très intuitif, son GUI a trois zones distincts : **Targets**, **Console** et **Modules**.
Targets liste toutes les machines que vous découvrez et celle sur laquelle vous travaillez. Les cibles pirater sont en rouge. Après le piratage d'une cible, faite clique droit dessus et continuer d'explorer avec ce que vous souhaitez comme analyser les dossiers.
Console apporte une vue sur les dossiers. Cliquer dessus, vous pouvez directement naviguer dans les dossiers sans utiliser les commandes de Metasploit.
Modules est la section qui liste le module des vulnérabilités.

Vulnerable Target (Metasploit)

C'est une cible qui peut être une machine ou un appareil avec une faille de sécurité non corrigée. Ce qui en fait un hôte vulnérable. Le site Rapid7 permet de générer des machines virtuelles avec diverses vulnérabilités. **Il est interdit de pénétrer sur n'importe quelle machine sans permission préalable**.
Pour faire vos tests, vous devez télécharger **metaspoitable** qui est une machine virtuelle sous Linux que vous devrez installer sur **VM VirtualBox**. Les logins sont **username: msfadmin** et **pwd: msfadmin**.

Discovery Scans

Première phase de pénétration est de scanner un réseau ou un hôte pour recueillir des informations et créer une vue d'ensemble de la cible.
Discovery Scan est la création d'une liste d'IP dans le réseau cible, les services tournants actuellement sur les machines. Pour faire cela sur Metasploit, nous devons utiliser un outil complémentaire Nmap et ses lignes de commandes importer sur Metasploit. (Voir dans ce même CheatSheet)

Wireshark

Installation de Wireshark sur Linux

sudo apt-get install wireshark | sudo dpkg-reconfigure wireshark-common | sudo adduser $USER wireshark

Capture de paquets de données

Nous pouvons filtrer les paquets capturés sur le trafic réseau. En maintenant la touche majuscule, on peut sélectionner plusieurs interfaces.

Capture -> Start ou Ctrl + E pour faire de même. Arrêter la capture avant l'analyse de ceux-ci.

Analyse de paquets de données

Signification des titres de colonnes

No.

Wireshark (cont)

Numéro du paquet capturé

Time

La durée de temps avant la capture du paquet après activation du mode capture.

Source

Adresse du système émettant le paquet

Destination

Adresse de destination du paquet

Protocole

Type de paquet. Ex : TCP, DNS, DHCPv6 ou ARP

Length

Taille/Longueur du paquet (en octets)

Info

Présente le contenu du paquet en fonction du type de celui-ci

Filtres Wireshark

Filtres de Capture

Ettercap

Aircrack-ng