TP 5
Mise en œuvre d'un Botnet!!!

Définition :

Un Botnet est un ensemble de machines connectées à Internet qui, à l'insu de leurs propriétaires, ont été configurés de manière à envoyer des spams ou du trafic à des cibles reliés à Internet. Ces machines infectées, appelés « zombies » ou « bots », servent les intérêts de l'auteur du spam ou du trafic.

Information : Ce bot sera mis en place pour réaliser des tests de pénétration et pour des fins éducatives.

Objectif du TP :

L'objectif de ce TP sera la mise en œuvre du botmaster Hybrid_V1.0 (interface décrite par la figure 1) pour lancer des attaques.

Figure 1. Plateforme du botnet Hybrid1.0

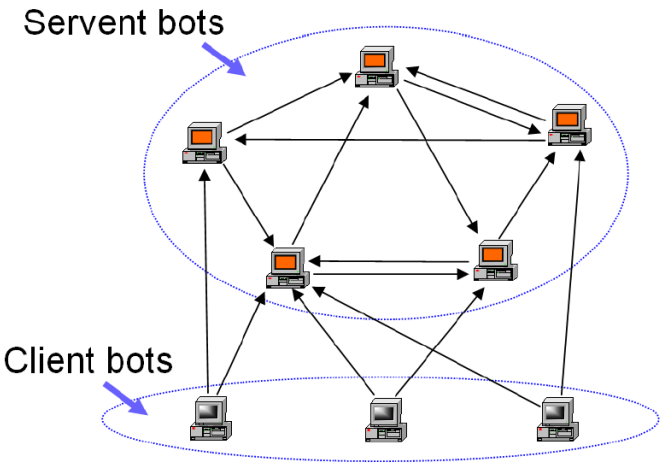

Figure 2. Architecture d'un botnet centralisé

Travail à réaliser :

Le travail dans ce TP consiste à installer le BotMaster, générer des malwares pour créer des bots, lancer des attaques et enfin analyser le trafic.

Tout d'abord lancer la machine virtuelle Ubuntu en mode pont et lancer la commande *service networking restart* et vérifier si la VM a bien récupéré une adresse IP.

Si cela ne fonctionne pas, exécutez:

$ sudo dhclient eth1

Si vous utilisez la machine virtuelle fournie par l'enseignant, commencez à partir de l'étape 3

1. **Installation du serveur LAMP**

   a) Installation du serveur Apache: *sudo apt-get install apache2*
   Testez le bon fonctionnement sur un navigateur web:
   http://localhost
   b) Installation de Mysql: *sudo apt-get install mysql-server php5-mysql*
   Pendant l'installation un mot de passe root pour Mysql vous sera demandé
   c) Installation de PHP: *sudo apt-get install php5 libapache2-mod-php5 php5-mcrypt*
   d) Installation de PhpMyAdmin: *sudo apt-get install phpmyadmin apache2-utils*
   Il vous sera demandé alors : de choisir votre serveur web. Sélectionnez Apache2. Si vous voulez obtenir une configuration de base de phpMyAdmin (dbconfig-common). Acceptez d'entrer votre mot de passe root MySQL de spécifier un mot de passe root pour vous connecter à phpMyAdmin.
   e) Rendez-vous dans les configurations d'Apache : */etc/apache2/apache2.conf*
   f) Ajoutez-y à la fin : *include /etc/phpmyadmin/apache.conf*
   g) Et redémarrez apache : *sudo service apache2 restart*
   h) Testez le bon fonctionnement sur un navigateur web: *http://localhost/phpmyadmin*

2. **Installation du BotMaster**

Préparation :

- Extraire l'archive *Hybrid.zip* *(à télécharger du site pédagogique)*
- Créez une base de données pour le botnet (vous pouvez utiliser PhpMyAdmin ou en ligne de commande)
- Modifiez les fichiers Index.php et getcmd.php : changez l'adresse IP de votre BotMaster ainsi que le mot de passe root pour Mysql
- Modifiez le fichiez install.php : changez « TYPE » par « ENGINE »

Installation :

- Déplacez le dossier Web dans votre serveur web : */var/www*

Si vous utilisez la VM fournie par l'enseignant, commencez à partir d'ici (mdp : toor):

- Via un navigateur web faites : *http://localhost/web*
- Remplissez les données et faites *install*
  - Mysql Database host : *localhost*
  - Mysql Database user : *root*
  - Mysql Database : *toor*
  - Mysql Database : *hybrid*
- un username et Password vous sera demandé : faite 1 1 (pour les deux)

3. **Génération du malware (Bot)**
   - Allez sur l'anglet Hybrid generation
   - Directory to place bot : */opt/*
   - Mettez l'adresse IP de votre BotMaster
   - Autostart file: */root/autostart.txt*
   - Generate new HybridBot
   - Enregistrez le nouveau bot.zip et changez-lui d'extension en bot.pl

4. **Compilation du bot**

- Téléchargez Perl2exe
- Convertir le script perl en exécutable : *./perl2exe bot.pl*
- Copiez le bot dans la machine cible
- Exécutez le bot sur la machine cible : *./bot*

5. **Générez des attaques**

- Sur le BotMaster allez dans l'onglet Statistics and Control Panel : l'onglet Help vous explique les détails de chaque attaque
- Exécuter les attaques de type flooding
- Pour chaque attaque (flooding) remplissez les arguments comme décrit :

Exemple pour l'attaque TCP SYN : IP_Cible Port [0 ou 1] Nb_Paquets

- Exécuter l'attaque Reverse Shell :
- La réalisation de cette attaque, nécessite l'utilisation du serveur NetCat pour écouter sur un port définit : nc -l 6666 (vous pouvez utiliser n'importe quel port)

- Ouvrez un sniffeur de paquets (ex : Wireshark) et analysez les paquets pour chaque attaque.
- Quand il n y a pas d'attaque en cours, il éxiste toujours des paquets échangés entre le BotMaster et le Bot. A quoi correspondent ces paquets ?

6. Analyse du malware

- Ouvrez *bot.pl*
- Essayer d'expliquer comment fonctionne la fonction SYNStorm
- Que fait la ligne my $rand_source = join ''.'', map int rand 256, 1..4 ;
- Modifier le malware pour qu'il envoie des paquets toutes les 2 secondes
- Vérifier avec un sniffeur (Wireshark).

7. Détection

- Que pourrait être la signature de ce malware ?
- Quelle méthode de détection conviendrait elle le mieux pour le détecter ?
- Si on devait ajouter une règle au détecteur, à quoi ressemblerait-elle ?