Attaque d'un serveur
Prise d'empreinte

[Floux]

L'attaque d'un serveur à «l'aveuglette» à toute ses chances de rater. La prise d'empreinte (ou pentest pour les intimes ;)) permet au pirate de mieux connaître sa victime et ainsi de préparer au mieux son attaque, en se renseignant sur les failles potentielles du serveur par exemple. Pour cela, une poignée d'outils, un peu d'imagination et Internet feront l'affaire...

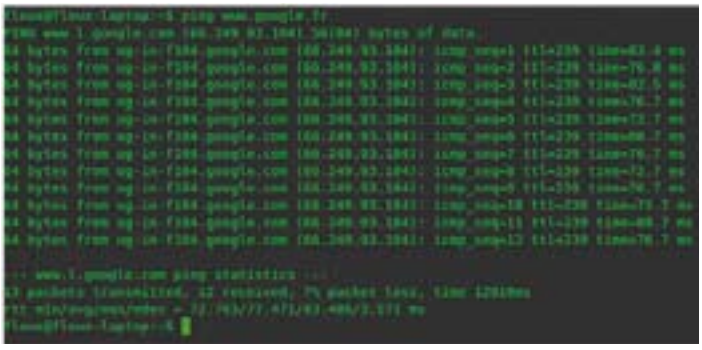
Les bases

Tout d'abord, un petit rappel sur les IPs.

Nos ordinateurs utilisent l' «Internet Protocole», d'où IP, pour communiquer entre eux. Pour cela, une adresse IP leur est attribuée et celle-ci sert ensuite de «numéro de téléphone» pour le poste. Lorsque vous rentrer une URL (http://www.google.fr par exemple) vous allez contacter un serveur DNS qui va vous renvoyer l'IP d'un des serveurs de Google afin de pouvoir s'y connecter.

L'IP change normalement à chaque connexion à moins que vous n'en ayez une fixe. Elle est composé de 4 octets (allant de 0 à 255) et s'écrit sous cette forme x.x.x.x (ex: 192.168.0.1).

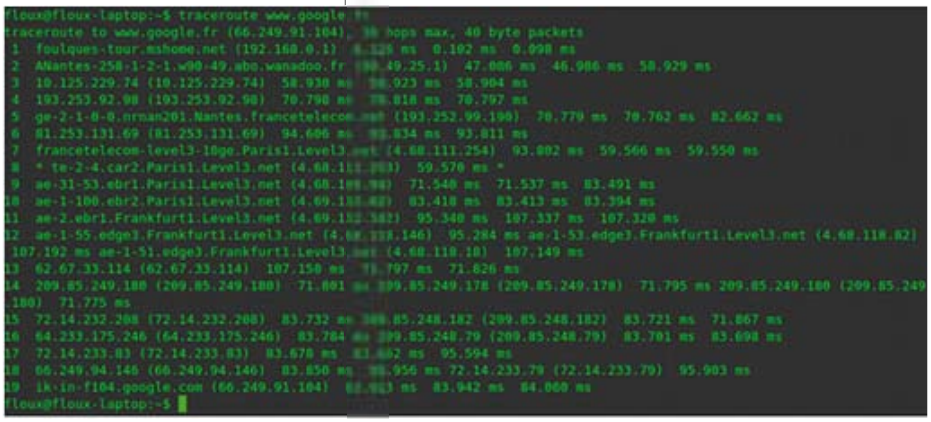
C'est bien beau d'avoir l'URL d'un site, mais si on veut maintenant commencer notre prise d'empreinte, il sera plus pratique d'avoir l'IP du serveur, sachant que certains outils n'accepte pas l'URL en argument. Pour cela nous pouvons utiliser la commande «ping».
Celle-ci enverra des requêtes au serveur pour vérifier qu'il est bien joignable. Le résultat de cette commande nous donnera l'adresse IP du serveur et entre autre le temps de réponse de celui-ci.



Une petite «astuce» qui peu s'avérer très utile pour tout ceux qui utilisent un système basé sur Unix (Linux, Mac OS, FreeBSD...), n'oubliez pas que vous disposez de la commande «man»qui vous permettra d'afficher le manuel de la commande passée en argument et donc de pouvoir ainsi découvrir des options plus ou moins utiles selon l'utilisation que vous en ferez.
Cela offrira un plus grand panel de commande avec toute les explications qui vont avec, par rapport à un «-h ou --help». RTFM quoi! =)
Une dernière chose, vous cherchez des informations sur un logiciel, une faille ou je ne sais quoi encore, rappelez-vous que Google est votre ami est que grâce à lui vous pourrez trouver bien plus que ce que vous cherchez (faut-il savoir chercher...).
Toutes vos questions ont de grandes chances d'avoir déjà été posées un grand nombre de fois sur des forums, alors demandez l'aide de votre ami Google qui devrait vous trouvez ça en moins de 2s ;-)

Trace ta route !

Lorsque notre ordinateur communique avec un serveur distant, la liaison n'est pas direct. Nos paquets passent par plusieurs noeuds (serveurs, routeurs...), il est donc intéressent de voir la route empruntée par la communication.
L'utilisation des commandes «traceroute» et «tracert», respectivement pour Linux et Windows, permettent de réaliser cette tâche. A noter qu'il se peut que «traceroute»ne soit pas installé par défaut sous certaines distribution, un «apt-get install traceroute» permettra de l'installer sous les distributions basées sur Debian. Cette commande peut notamment être intéressante pour comprendre la structure d'un réseau local. Si le hacker réussit à pénétrer dans le réseau interne de l'entreprise, il peut ainsi avoir une «vue»de celui-ci.



Lister les machines d'une entreprise

Nous avons vue que le rôle d'un serveur DNS était de nous donner l'IP d'un serveur à partir d'une URL. Si il est mal configuré, un service peu nous lister l'ensemble des machines du réseau interne de l'entreprise. Ceci est très utile pour un hacker, donc extrêmement dangereux pour l'entreprise.

Cela est donc réalisable par la commande «nslookup»(normalement présente par défaut sous Windows et Linux), et «dig» sous Linux seulement. Il faut savoir que la commande «nslookup» n'est plus mise-à-jour sous Linux, il est donc préférable d'utiliser «dig», par contre, pas de problème avec la première sous Windows.

```
> floux@floux-laptop:~$ nslookup
> google.fr
Server:         192.168.0.1
Address:        192.168.0.1#53

Non-authoritative answer:
Name:   google.fr
Address: 72.14.221.104
Name:   google.fr
Address: 66.249.93.104
Name:   google.fr
Address: 216.239.59.104
>
```

```
; <<>> DiG 9.4.2 <<>> google.fr
;; global options:  printcmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51349
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.fr.                     IN      A

;; ANSWER SECTION:
google.fr.              1444    IN      A       66.249.93.104
google.fr.              1444    IN      A       216.239.59.104
google.fr.              1444    IN      A       72.14.221.104

;; Query time: 72 msec
;; SERVER: 192.168.0.1#53(192.168.0.1)
;; WHEN: Sat May 10 17:57:45 2008
;; MSG SIZE  rcvd: 75

floux@floux-laptop:~$
```

Pour notre recherche un peu plus loin, on peut tenter de faire un transfert de zone. Si cela réussi, le serveur DNS nous renverra la liste des serveurs associé au domaine.

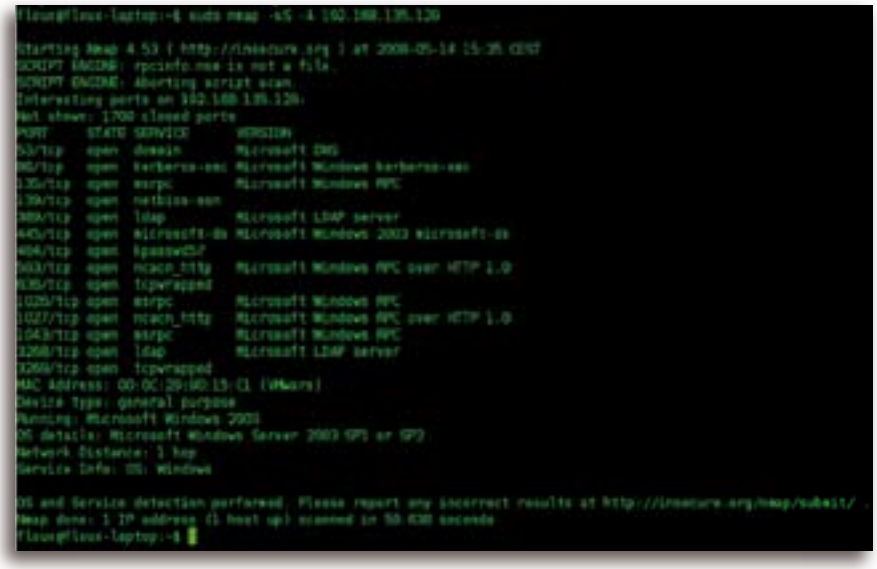
```
floux@floux-laptop:~$ dig axfr [redacted].com @[redacted].net

; <<>> DiG 9.4.2 <<>> axfr [redacted].com @[redacted].net
;; global options:  printcmd
[redacted].com.         3600    IN      SOA     [redacted].net. hostmaster.[redacted].net. 2006030100 10800 3600 60
4800 3600
[redacted].com.         3600    IN      NS      [redacted].net.
[redacted].com.         3600    IN      NS      [redacted].net.
[redacted].com.         3600    IN      MX      10 messagerie.[redacted].fr.
www.[redacted].com.     3600    IN      A       217.147.[redacted]
preview.[redacted].com. 3600    IN      A       217.147.[redacted]
[redacted].com.         3600    IN      SOA     [redacted].net. hostmaster.[redacted].net. 2006030100 10800 3600 60
4800 3600
;; Query time: 276 msec
;; SERVER: 217.147.[redacted]#53(217.147.[redacted])
;; WHEN: Sat May 10 18:03:12 2008
;; XFR size: 7 records (messages 3, bytes 345)

floux@floux-laptop:~$
```

Scan de ports

Maintenant que nous avons une liste de serveurs en main, nous allons pouvoir procéder à un scan de ports. L'objectif est ici d'établir une liste des ports ouverts ou non et de regarder les services qui tournent derrière. Cela nous permettra de rechercher des vulnérabilités exploitables via ces services.



Pour cette étape, j'ai choisi nmap, qui est bien connu (on le retrouve même dans Matrix ;-), mais pas forcement le meilleur !

Ainsi la commande:

```
nmap -sS -A x.x.x.x
```

va scanner l'hôte x.x.x.x avec la méthode SYN SCAN (-sS), on n'aura donc pas de log sur la machine distante. L'option -A va permettre de détecter la version des services tournant sur les ports du serveur.

Fingerprinting

Nous venons de faire un scan de ports, il me semble donc logique d'enchaîner directement sur le fingerprinting.
Cette étape consiste à relever la version de l'OS (Operating System) tournant sur le serveur. On appel cela aussi, relevé de bannière.

Cette étape ne peut être sautée du fait que les attaques ne seront pas les mêmes d'un OS à un autre, normal =). Déjà, avec l'argument -A passé dans nmap, on peut voir que l'OS à été récupéré (voir Illustration 6). Une autre commande permettant de réaliser cette tâche est l'option -O.

Une autre manière, est de demander une page inexistante sur le serveur, dans le but que celui-ci nous renvoi un message d'erreur, et là, avec un peu de chance, on pourra en savoir un peu plus sur lui.

Ici, on peut voir que le serveur fait tourner Apache 2.2.8, à partir de là on peut essayer de rechercher des failles sur des sites www.milw0rm.com.
De plus, il y a le très bon p0f, qui lui fait du fingerprinting passif. C'est-à-dire qu'il lira les paquets du réseau et à partir de ceux là, il en déduira l'OS correspondant à l'IP du paquet.
Cette technique est donc totalement furtive, l'auditeur ne pourra pas être détecté.

Une balade sur le site par une chaude soirée d'été

Après avoir exploité les failles techniques, nous allons attaquer les failles humaines. L'entreprise cible et son personnel vont donc être notre première cible pour la récupération d'informations.
Tout d'abord une petite visite sur le site de l'entreprise peut être un très bon début.

Souvent dans les rubriques « contacts », « notre groupe » ou encore « offres d'emploi », nous pouvons avoir le nom, prénom de personnes qui sont employées dans l'entreprise, ainsi nous allons pouvoir trouver les adresses mails, les numéros de téléphones des personnes susceptibles de nous délivrer un maximum d'informations sur les systèmes.

De nos jours il existe de plus en plus de sites communautaires qui détiennent des informations personnelles sur ses membres (ex : Facebook).

Ainsi en connaissant par cœur notre cible, nous pourrons plus facilement la mettre en confiance et lui soutirer des éléments cruciaux pour notre attaque.

Whois (t'es qui toi ?)

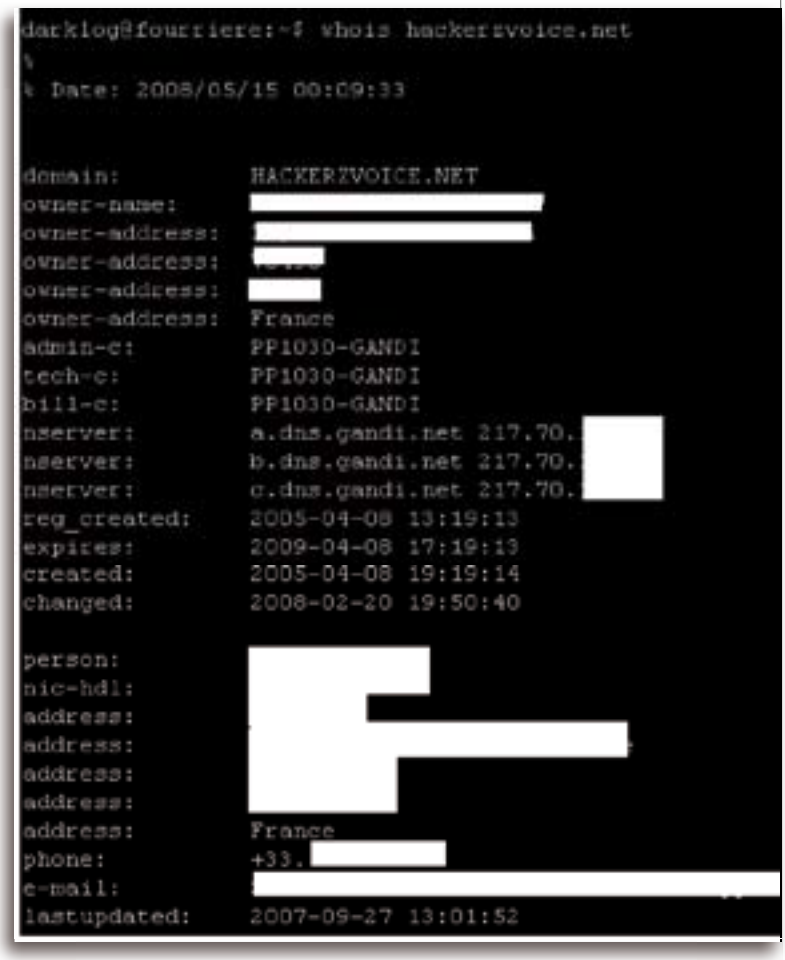
La notion de «whois» est également très importante dans la prise d'empreintes.
Cela permet de donner des indications pertinentes sur le serveur hébergeant le site internet de l'entreprise cible.

En effet lors de l'acquisition d'un serveur web, celui-ci est référencé avec les informations de son propriétaire à contacter en cas de litiges, l'endroit où il est implémenté physiquement, etc…

Il existe plusieurs types de fonction «whois» :

La première est la fonction Web. Par exemple sur le site http://www.raynette.fr/services/whois/

La seconde est la fonction sous un terminal Linux grace à la commande : « whois »



Il existe beaucoup d'autres solutions notamment la création de script avec des fonctions propres au langage utilisé.

Ce qu'il faut retenir de cette expérience, c'est que nous pouvons avoir le nom, le prénom, l'adresse postale, l'adresse mail et le numéro de téléphone du propriétaire du serveur.

Avec un peu de chance, nous pouvons avoir beaucoup de renseignement sur le directeur de l'entreprise. Ceci étant notre attaque va pouvoir cibler une personne. Voyons par la suite ce que nous pouvons avoir comme informations supplémentaires.

Le Social Engineering ou l'art de tromper les gens

Après avoir récupérer assez d'informations sur l'entreprise, et sur son personnel en particulier, nous allons pouvoir tester notre aptitude à tromper les gens. La technique du social engineering demande beaucoup de préparation, aucun paramètre ne doit être laissé pour compte.

Il faut ainsi créer son propre scénario, envisager le maximum de situations, et toujours garder son sang froid.

Tout d'abord nous allons prendre un premier contact avec la personne susceptible d'être faillible pour son entreprise. Le but étant de la mettre en confiance pour qu'elle nous divulgue le maximum d'informations à son propre insu.
Par exemple, nous recevons de nos jours de plus en plus d'appels téléphoniques pour des sondages, ou pour connaître le type de parpaing que nous avons utilisé pour construire notre maison.
Il va être d'autant plus facile de s'appuyer sur ce système pour soutirer des informations cruciales (entreprises partenaires, marque des serveurs, …).

Et pour résumer ?

Ce qui est important de toujours garder à l'esprit est le fait qu'une entreprise n'est pas totalement infaillible.
Il est toujours possible de trouver la petite brèche que ce soit au niveau technique que niveau humain.
Lors d'un pentest il est donc crucial de vérifier chaque entité susceptible d'être en contact avec l'information que l'entreprise traite (allant de la secrétaire, au sysadmin, en passant par la femme de ménage, et en revenant par les mainframes traitent les données).

Plus l'entreprise est consciente des dangers qu'elle court en s'exposant sur le net, et à la face du monde, plus l'attaque sera mise à l'épreuve et plus elle aura de chances d'échouer.