

**DNS SPOOFING.**  
**<http://nassih.com>**  
**© MOHAMED NASSIH.**

## **1. Serveur de nom.**

Un serveur de nom fait la résolution des noms en adresses IP. Il est l'un des composantes les plus critiques dans un réseau. La nécessité de mettre en place un serveur de nom dans un réseau vient du fait que le serveur principal (souvent chez le fournisseur d'accès Internet) pourra être non disponible.

Lorsqu'une machine sur Internet envoie une requête à un serveur de nom pour avoir l'adresse IP d'une adresse, [www.polymtl.ca](http://www.polymtl.ca) par exemple, le serveur de nom va répondre avec l'adresse IP correspondante s'il est responsable de ce nom de domaine, sinon il va interroger un serveur externe qui gère ce nom de domaine. Pour minimiser le nombre de requêtes vers des serveurs externes, le serveur de nom enregistre les réponses reçues dans un cache.

Une zone DNS définit en général un domaine. Chaque zone possède ses propres machines contenues dans cette zone et ses propres paramètres. Le serveur qui gère une zone est appelé le serveur de nom primaire, pour chaque serveur primaire, on pourra trouver plusieurs serveurs secondaires. Ces serveurs récupèrent les informations concernant une zone périodiquement. Cette récupération d'information est appelée transfert de zone.

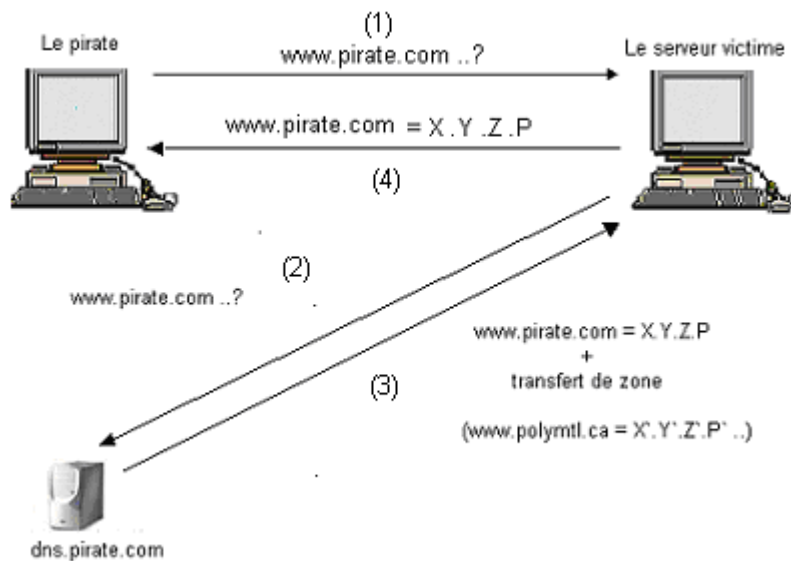
## **2. L'attaque DNS Spoofing.**

DNS Spoofing est un terme générique qui désigne plusieurs techniques qui ont comme objectif la redirection des machines sur le réseau vers des fausses adresses. Dans ce contexte on pourra citer deux types d'attaque, l'empoisonnement du cache du serveur de nom et le Spoofing de l'identificateur DNS.

### **2.1. L'empoisonnement du cache DNS.**

Dans ce cas le pirate a son propre domaine [pirate.com](http://pirate.com), avec son propre serveur de nom [dns.pirate.com](http://dns.pirate.com). Le pirate va jouer dans la configuration de son serveur, il va assigner à des serveurs connus comme par exemple [www.polymtl.ca](http://www.polymtl.ca) une adresse IP d'un autre serveur, ou tout

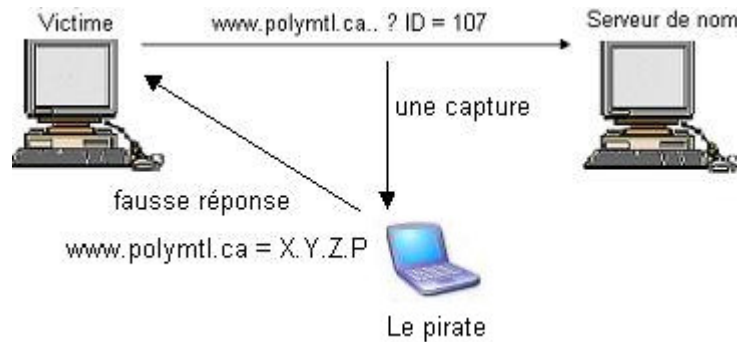
simplement de l'un de ses serveurs. Le pirate commence l'attaque par demander au serveur de nom victime la résolution de [www.pirate.com](http://www.pirate.com), le serveur de nom va contacter le serveur de nom responsable de ce domaine qu'est [dns.pirate.com](http://dns.pirate.com). Le serveur de nom [dns.pirate.com](http://dns.pirate.com) ne va pas fournir seulement l'adresse IP correspondante mais il va lui fournir tous les autres enregistrements (inclut celui de [www.polymtl.ca](http://www.polymtl.ca)) à travers un transfert de zone. Le cache du serveur victime est donc empoisonné. La figure 2.1 résume l'attaque.



**Figure 2.1 : l'empoisonnement du cache du serveur de nom.**

## 2.2. Spoofing de l'identificateur DNS.

Le client assigne à chaque requête envoyé vers un serveur de nom un identificateur de requête. Cet identificateur doit figurer dans la réponse. Une réponse est valide si les deux identificateurs sont identiques. Le pirate essaie de capturer une requête vers le serveur de nom, puis envoie une fausse réponse à la machine qui demande la résolution en utilisant le même identificateur.



**Figure 2.2 : Spoofing de l'identificateur d'une requête DNS.**

### 3. Outils de simulation.

Nous allons simuler l'attaque « Spoofing de l'identificateur DNS » en utilisant l'utilitaire dnsspoof qui fait partie de la même suite d'outils dsniff. Il répond à des requêtes dirigées vers un serveur de nom en utilisant des fausses adresses. L'option « -f » de dnsspoof permet de spécifier un fichier hosts qui contient ces fausses correspondances nom\_domaine/Adresse\_IP.

### 4. Démonstration.

Le tableau 3.3 donne l'adresse IP de chaque machine qu'on va utiliser dans notre simulation.

**Tableau 4.1 : les adresses IP des machines participants à l'attaque.**

Machine	Pirate	Victime	Serveur DNS	Serveurweb
Adresse IP	192.168.1.200	192.168.1.103	192.168.1.102	192.168.1.100

La figure 4.1 montre le fichier hosts qui contient les fausses réponses qui vont être utilisées par l'outil dnsspoof.

```
[root@Pirate hacker]# cat hosts
192.168.1.200  Serveurweb.testdomaine.com
[root@Pirate hacker]# _
```

**Figure 4.1 : le fichier hosts utilisé par dnsspoof.**

Nous démarrons l'attaque en exécutant la commande «dnsspoof -f hosts», voir la figure 4.2.

```
lroot@Pirate hackerl# dnsspoof -f hosts
Kernel filter, protocol ALL, raw packet socket
dnsspoof: listening on eth0 [udp dst port 53 and not src 192.168.1.200]
192.168.1.3.3488 > 192.168.1.102.53: 18739+ A? Serveurweb.testdomaine.com
192.168.1.3.3488 > 192.168.1.102.53: 37938+ A? Serveurweb.testdomaine.com
```

**Figure 4.2 : le démarrage de l'attaque dnsspoof.**

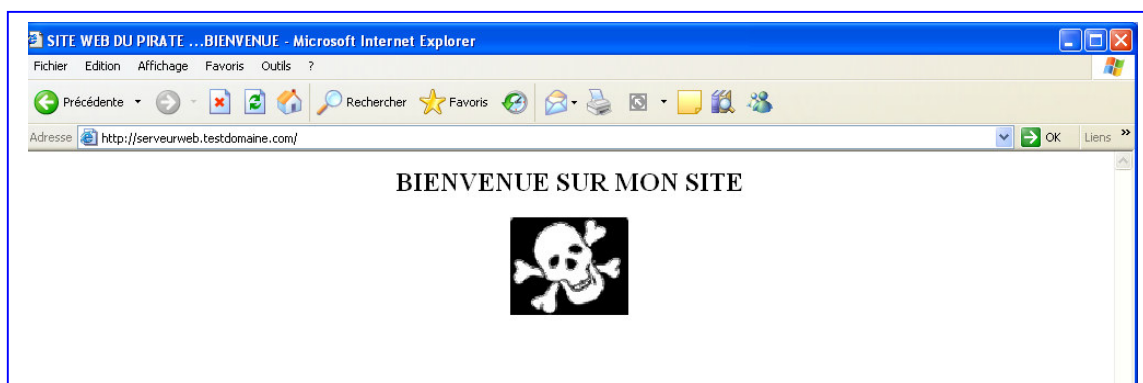
Puis nous envoyons un Ping vers le serveur Serveurweb à partir de la station Victime. - Voir la figure 4.3-. La machine Victime reçoit la réponse à partir de dnsspoof et envoie le Ping à la machine 192.168.1.200, au lieu de 192.168.1.100 qui est l'adresse IP réelle de la machine Serveurweb.

```
lroot@Victime rootl# ping Serveurweb.testdomaine.com
PING Serveurweb.testdomaine.com (192.168.1.200) 56(84) bytes of data.
64 bytes from Serveurweb.testdomaine.com (192.168.1.200): icmp_seq=1 ttl=64 time
=0.742 ms
64 bytes from Serveurweb.testdomaine.com (192.168.1.200): icmp_seq=2 ttl=64 time
=0.877 ms
64 bytes from Serveurweb.testdomaine.com (192.168.1.200): icmp_seq=3 ttl=64 time
=0.658 ms

--- Serveurweb.testdomaine.com ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2032ms
rtt min/avg/max/mdev = 0.658/0.759/0.877/0.090 ms
```

**Figure 4.3 : la redirection du trafic vers la machine du pirate.**

La figure 4.4 montre un autre test à partir de l'explorateur. Au lieu d'afficher la page web du serveur Serveurweb, le client a été redirigé vers le serveur web du pirate.



**Figure 4.4. la redirection vers la page web du pirate.**

## **5. Prévention et détection de l'attaque.**

Un serveur de nom doit être configuré pour ne pas résoudre directement les noms des hôtes sur lequel il n'a pas l'autorité, de cette façon le serveur de nom contrôle toutes les réponses pour voir s'elles possèdent une autorité. La mise en place d'un système de détection d'intrusion est aussi importante, surtout que ce type d'attaque est souvent combiné à d'autres attaques réseau comme l'empoisonnement de la cache ARP.