Vulnérabilités de la couche 2

Introduction

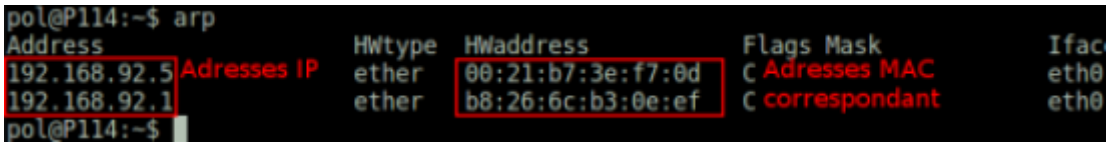
Si notre réseau initial comportait des concentrateurs[1)] à la place des commutateurs, l'ensemble des données seraient transmises sur tout le réseau quelles que soient les sources et destinations. Il serait trivial de capturer l'intégralité des paquets en écoutant passivement le réseau (*sniffing*) au moyen de logiciel comme tcpdump.

Nous allons voir dans ce chapitre comment capturer et rejouer des paquets qui ne nous sont pas destinés à travers le réseau de l'entreprise Corporate.

ARP: fonctionnement

Coté hôtes

Exécutons la commande `arp` depuis un ordinateur (linux) :



On peut voir les adresses IP correspondant aux adresses MAC des interfaces de deux hôtes sur le réseau.

Initialement, cet ordinateur ne connaît pas l'adresse physique de celui qu'il veut contacter, il va donc émettre une trame de diffusion. L'hôte concerné répondra avec une trame à destination du demandeur.
Voici un exemple de trame ARP :

Exemple d'en-tête ARP : protocole IPv4 sur Ethernet (28 octets)

Octet 1	Octet 2	Octet 3	Octet 4
0x0001		0x0800	
0x06	0x04	*Operation*	
Adresse MAC source (octets 1-4)			
Adresse MAC source (octets 5-6)		Adresse IP source (octets 1-2)	
Adresse IP source (octets 3-4)		Adresse MAC destination (octets 1-2)	
Adresse MAC destination (octets 3-6)			
Adresse IP destination (octets 1-4)			

Une fois que l'hôte de départ connaît l'adresse physique du destinataire, il rajoute cette entrée dans son cache ARP.

Côté commutateur

De son côté, le commutateur tient à jour une table d'adresses MAC correspondant aux ports sur lesquels sont branchés les interfaces des hôtes. Cet aspect sera abordé dans le chapitre suivant et va nous permettre de sécuriser en partie notre réseau en contrôlant l'association adresse MAC - port.

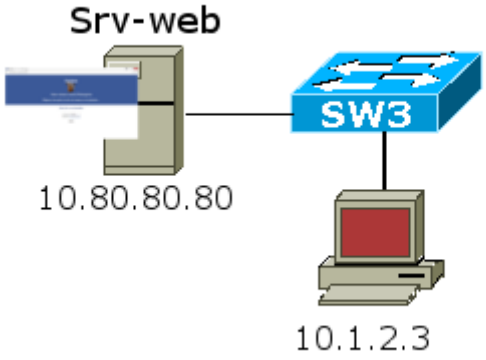
Usurpation

Démontrons qu'on peut facilement se faire passer pour celui qu'on n'est pas : nous allons usurper l'identité d'un hôte et d'un serveur afin de capturer les données qu'ils s'échangent.

Contexte

Reprenons notre réseau initial et intéressons nous au directeur de l'entreprise CORPORATE qui consulte le site “Facebouc”, fameux réseau social d'entreprise situé à l'adresse http://srv-web.corpora.te accessible uniquement depuis le réseau local.

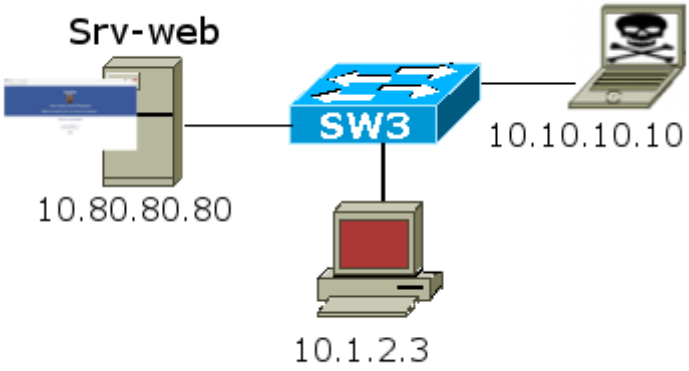
Schématiquement nous avons :



Pour des raisons de praticité des manipulations qui vont suivre, j'ai placé le serveur intranet dans le réseau local. S'il s'était trouvé dans le réseau 172.20.0.0/16, il aurait fallu changer la cible “10.80.80.80” en “10.0.19.77” (adresse de la passerelle dans notre réseau local) dans la suite.

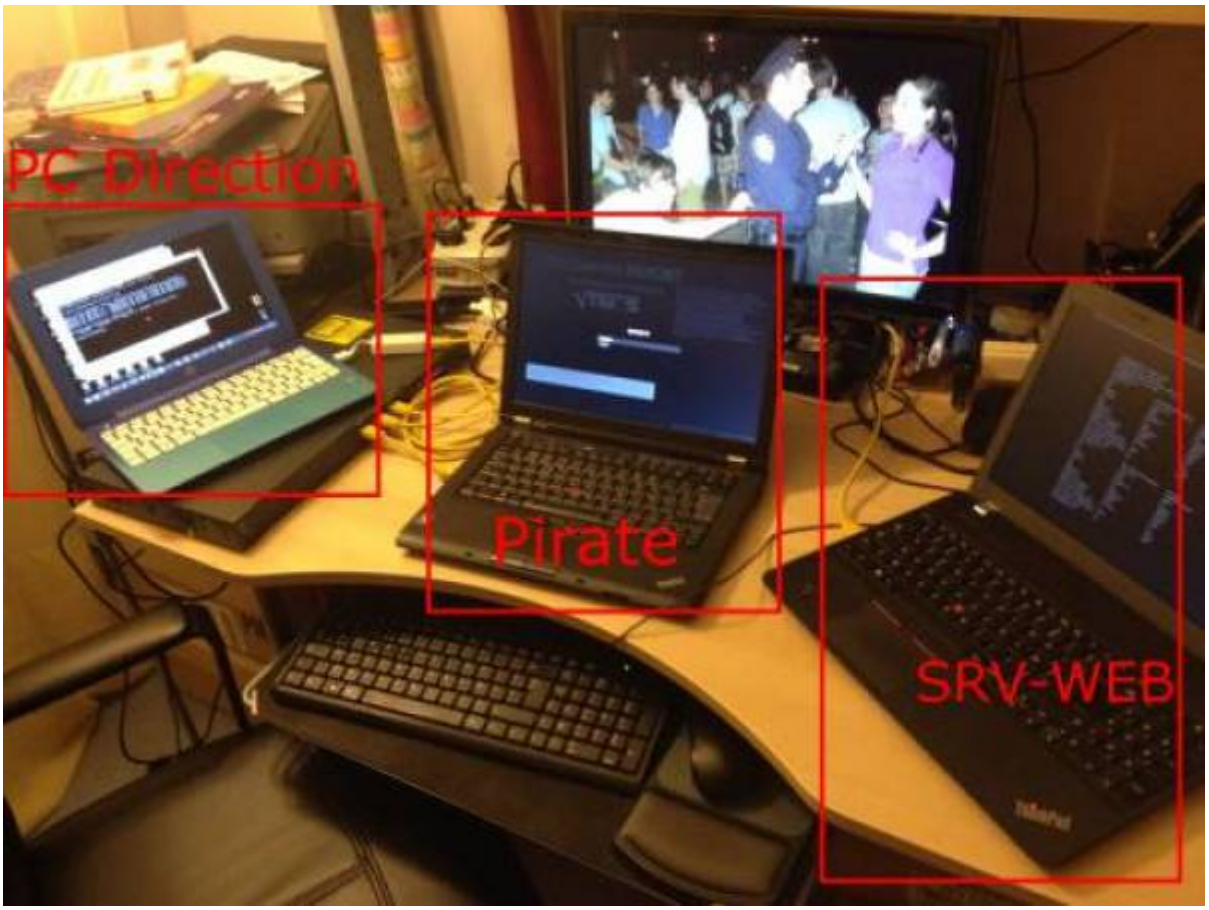
Notre directeur ignore qu'un collaborateur fâché avec l'entreprise a décidé de jouer les pirates en herbe. Présent dans l'entreprise, il branche son ordinateur portable sur une prise réseau murale.

Le serveur DHCP faisant son travail à merveille, nous avons maintenant le schéma suivant :



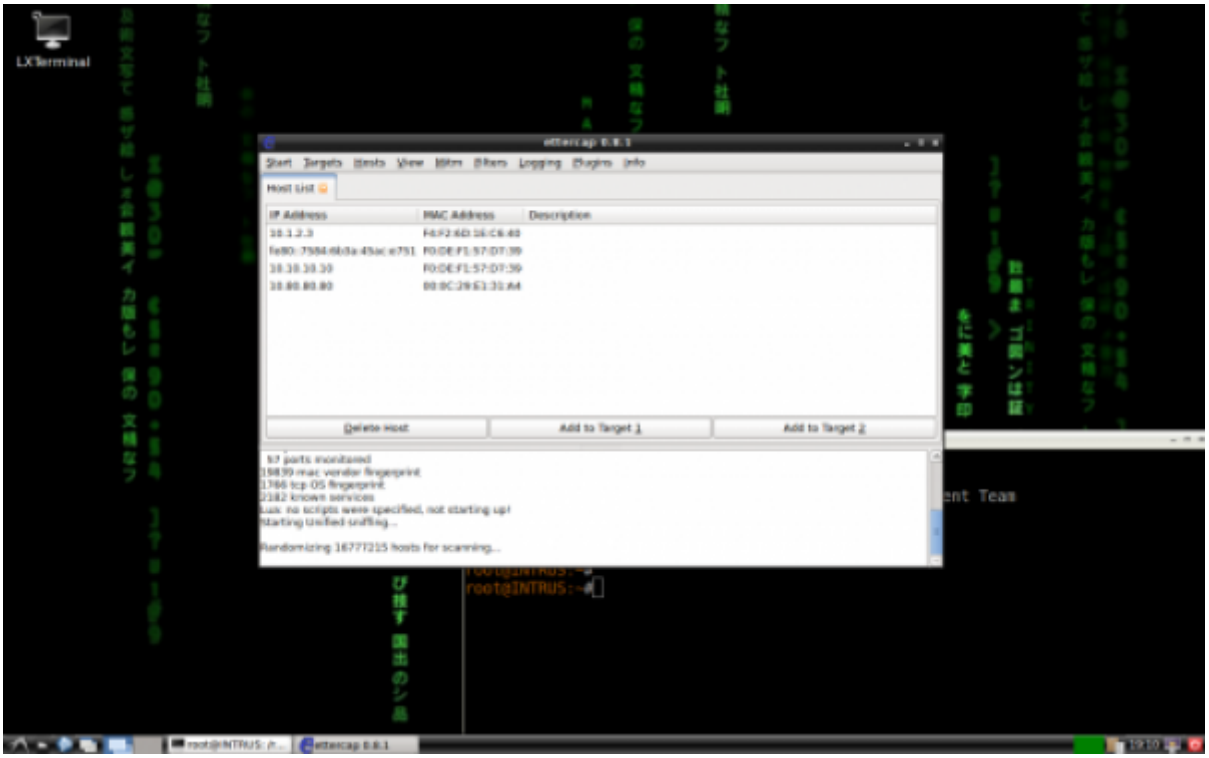
Démonstration

Le “champ de bataille” dans le cadre de la démonstration :



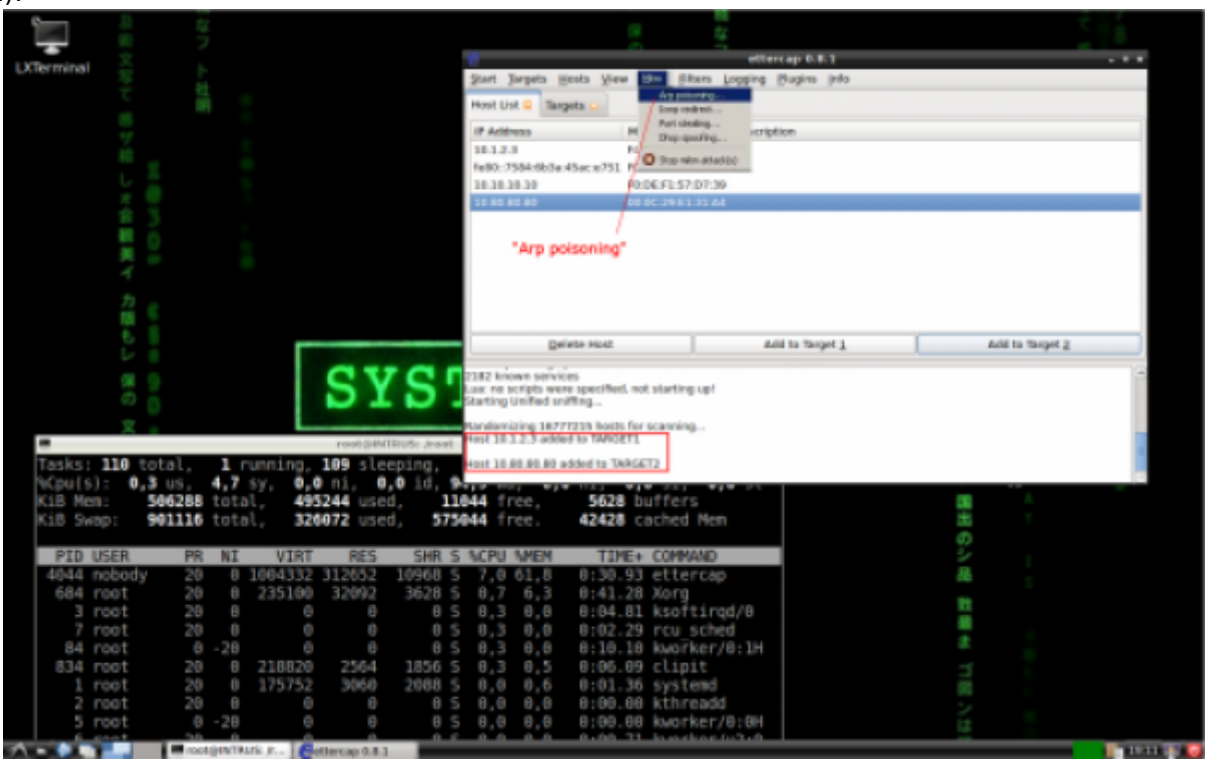
Le PC de la direction fonctionne tant bien que mal sous Windows 8 et le serveur web fonctionne sous Linux Debian 7 à jour. Quant à notre apprenti pirate, il s'est procuré une distribution “live” ressemblant étrangement à un mélange entre TAILS et Kali.

Notre pirate utilise Ettercap, outil permettant de capturer des paquets, visualiser les connexions, empoisonner les caches ARP et bien d'autres choses fort sympathiques.
Pour ce faire il va scanner les hôtes du réseau et trouver notre serveur web et notre PC client :

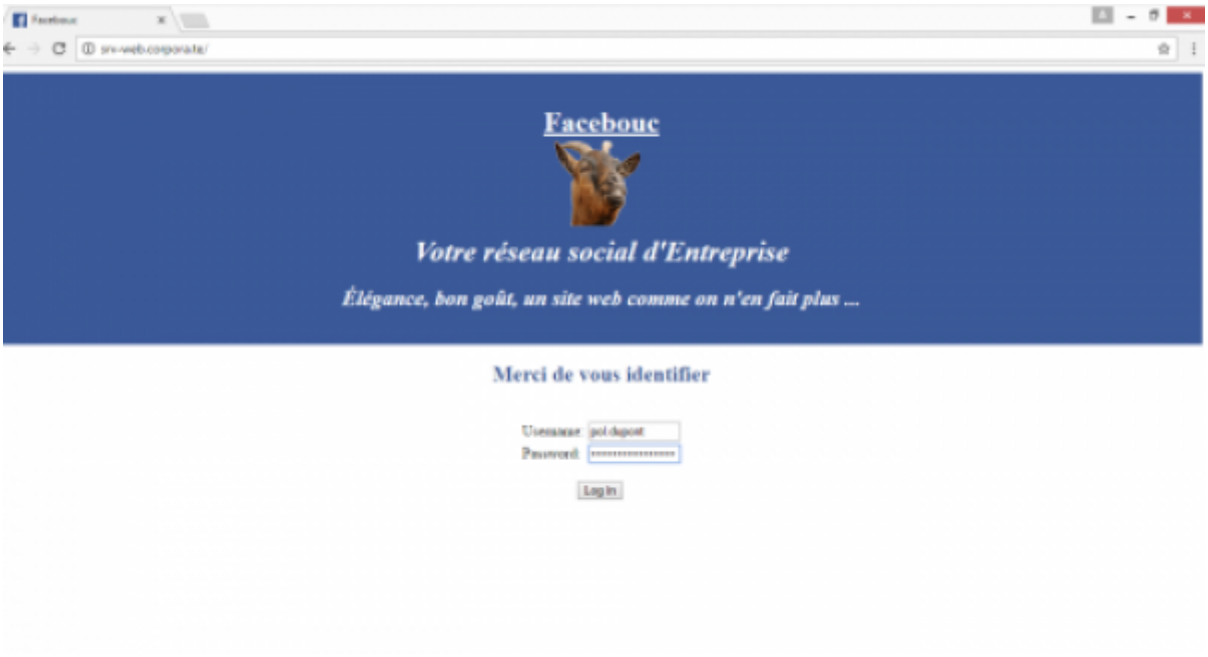


puis il va cibler d'un côté notre client (10.1.2.3) et de l'autre notre serveur web (10.80.80.80).

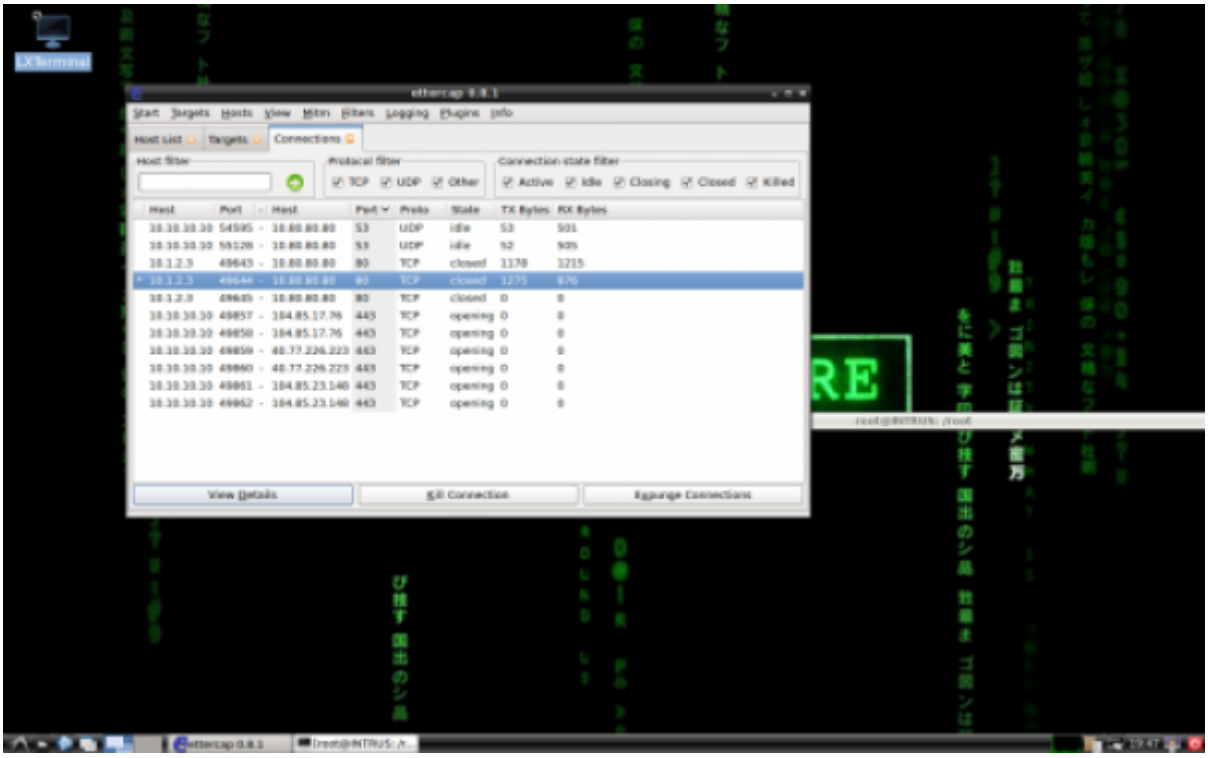
Il ne lui reste plus qu'à procéder à l'empoisonnement des tables ARP des deux hôtes en leur faisant croire qu'ils s'adressent à leur destinataire prévu et retransmettre les paquets “normalement” jusqu'au destinataire afin que personne ne soupçonne l'attaque (principe de l'attaque de l'homme du milieu).



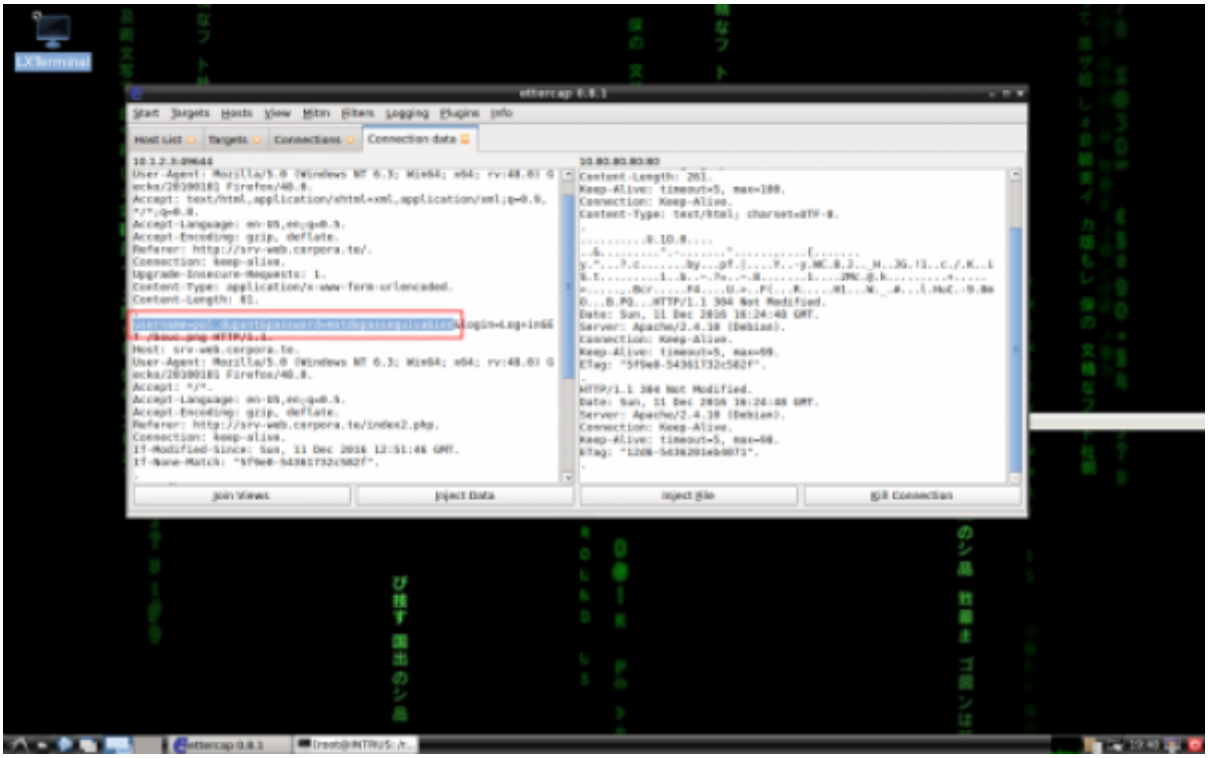
Notre directeur se rend sur son réseau social d'entreprise préféré et rentre son identifiant et son mot de passe :



Or, sur cette page non chiffrée, il transmet ces éléments en clair et notre pirate capture aisément ces informations :



et voilà ce qu'il voit :



Notre directeur imprudent s'est fait voler ses identifiants et notre collaborateur indélicat part insérer quelques articles bien sentis en se faisant passer pour son patron.

Analyse

Les causes sont doubles :

- Absence de chiffrement de la page web consultée: les données transitent en clair sur le réseau.
- Absence de protection contre l'empoisonnement ARP sur les équipements de niveau 2 : on peut changer d'adresse MAC à la volée, forger des trames pour corrompre les caches ARP des hôtes du réseau sans qu'on s'en rende compte.

Dans le prochain chapitre nous verrons comment surveiller le réseau pour être alerté en cas de comportement suspect et utiliserons port security pour se prémunir de l'attaque vue plus haut.

DHCP Spoofing

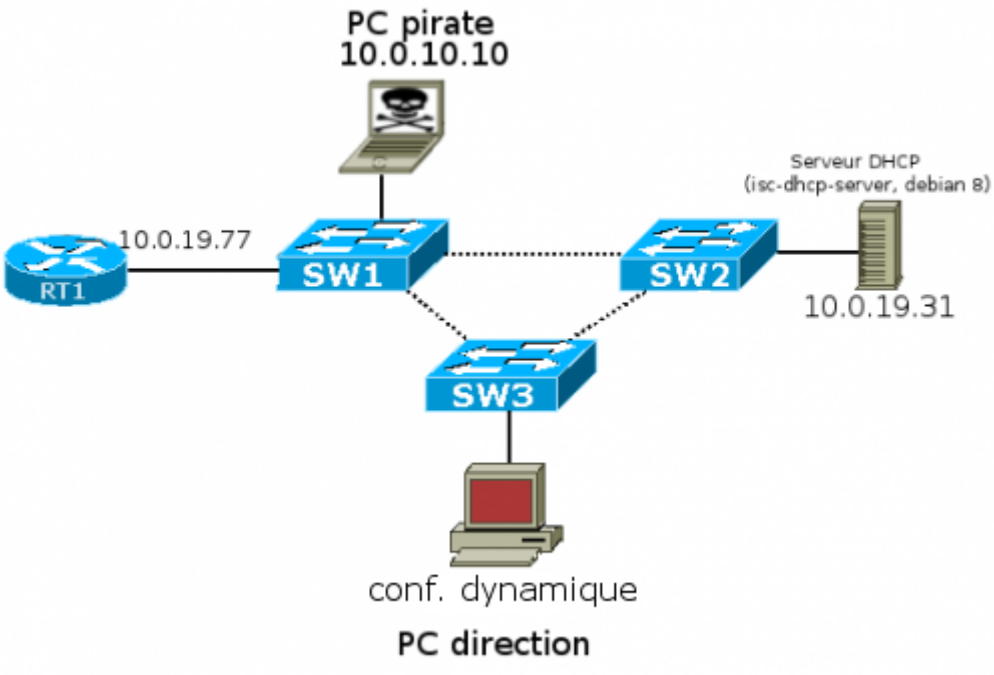
Contexte

Reprenons notre réseau initial et intéressons nous au serveur DHCP qui délivre la configuration réseau aux hôtes situés sur le réseau 10.0.0.0/8. Configuration :

- OS : Debian 8
- DHCPD : isc-dhcp-server
- Adresse IP : 10.0.19.31
- Configuration pour les clients:

- Intervalle d'adresses attribuées : 10.1.0.0 - 10.1.100.100
- Passerelle : 10.0.19.77 (routeur)
- domaine : corpora.te

Les commutateurs n'ont pas de paramètres spécifiques hormis leur nom (SW1, SW2 et SW3) et l'auto MDIX activé.
Notre collaborateur indélicat souhaite maintenant récupérer l'ensemble du trafic sortant sur Internet depuis le réseau local de l'entreprise, en se branchant sur une prise murale dans un bureau du secrétariat, et en s'attribuant lui-même une adresse IP dans le réseau.



Le PC pirate va offrir un service DHCP aux hôtes situés sur réseau (10.0.0.0/8) et se faire passer pour la passerelle par défaut :

Configuration :

- OS : Debian 8 modifiée
- DHCPD : isc-dhcp-server
- Adresse IP : 10.0.10.10
- Configuration pour les clients:
  - Intervalle d'adresses attribuées : 10.1.0.0 - 10.1.100.100
  - **Passerelle : 10.0.10.10 (lui-même)**
  - domaine : corpora.te

Il suffira au pirate de router correctement l'ensemble des paquets qui transitent par lui entre les hôtes du réseau local et le routeur de l'entreprise.

Dans le cas présent, le “premier” disponible répondra. On pourrait tout aussi occuper toutes les adresses disponibles du serveur DHCP au moyen de logiciels comme Yersinia[2)] et ainsi être le seul serveur disponible pour attribuer des adresses.
Par définition la passerelle n'interceptera pas les paquets faisant l'objet d'une remise directe au sein du même réseau.

Démonstration

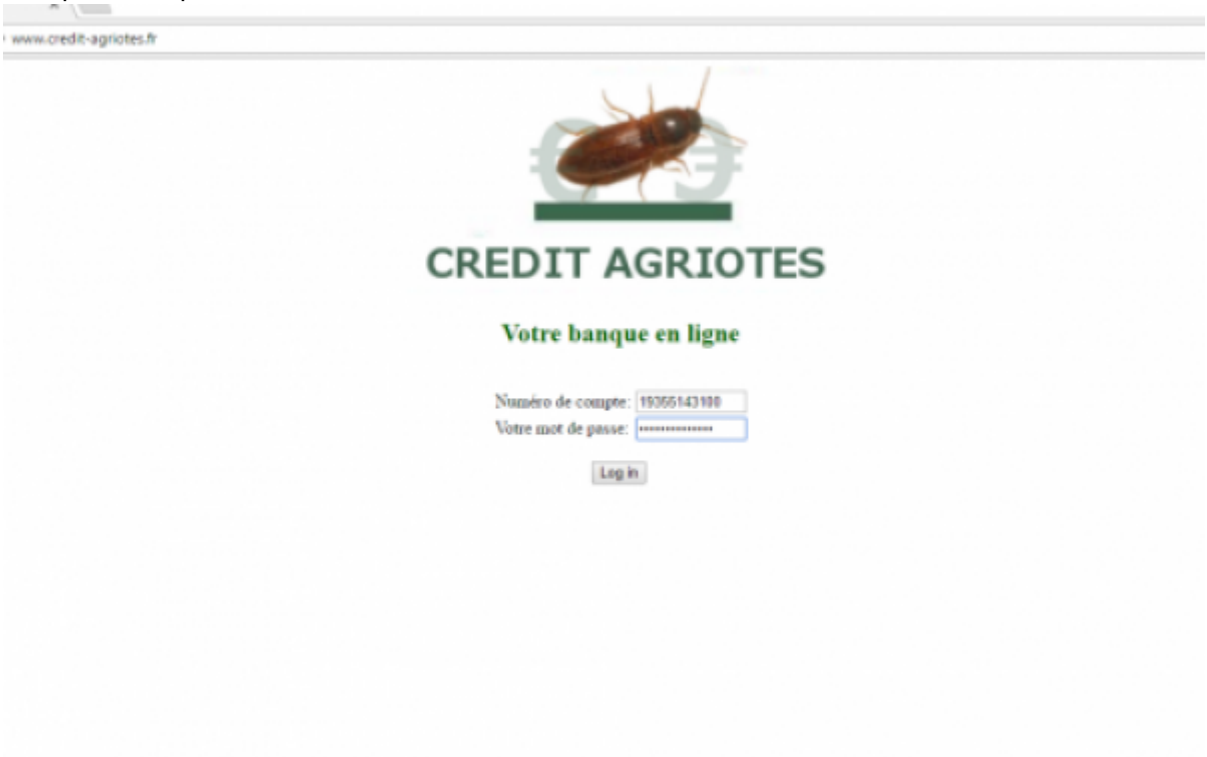
Le directeur de l'entreprise Corporate souhaite consulter son compte en banque en ligne. En temps normal, il allume son poste de travail et reçoit la configuration réseau suivante du serveur DHCP situé à l'adresse 10.0.19.31 :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : corpora.te
   Adresse IPv4. . . . . . . . . . . . . .: 10.1.0.0
   Masque de sous-réseau. . . . . . . . . : 255.0.0.0
   Passerelle par défaut. . . . . . . . . : 10.0.19.77
```

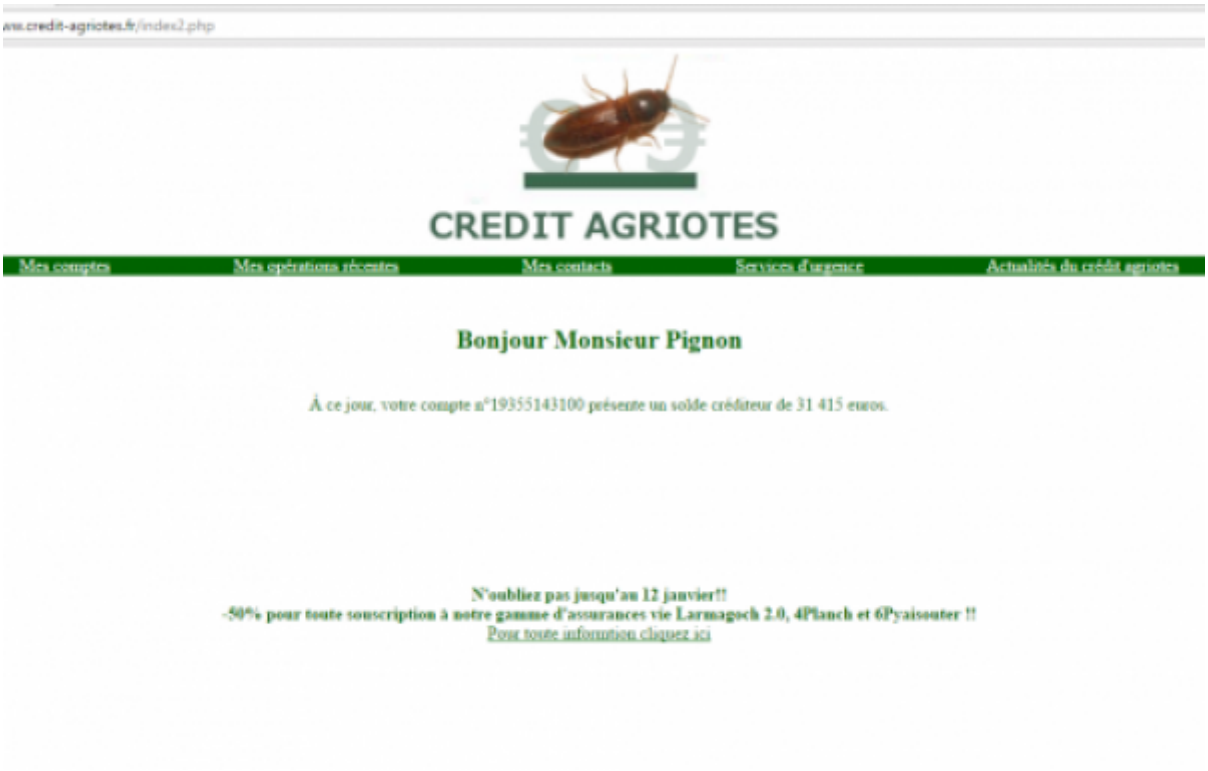
Or, notre pirate situé sur le réseau exécute son serveur DHCP de son côté et au démarrage du système, le poste de travail du directeur reçoit cette configuration :

```
Carte Ethernet Ethernet :

   Suffixe DNS propre à la connexion. . . : corpora.te
   Adresse IPv4. . . . . . . . . . . . . .: 10.1.0.2
   Masque de sous-réseau. . . . . . . . . : 255.0.0.0
   Passerelle par défaut. . . . . . . . . : 10.0.10.10
```

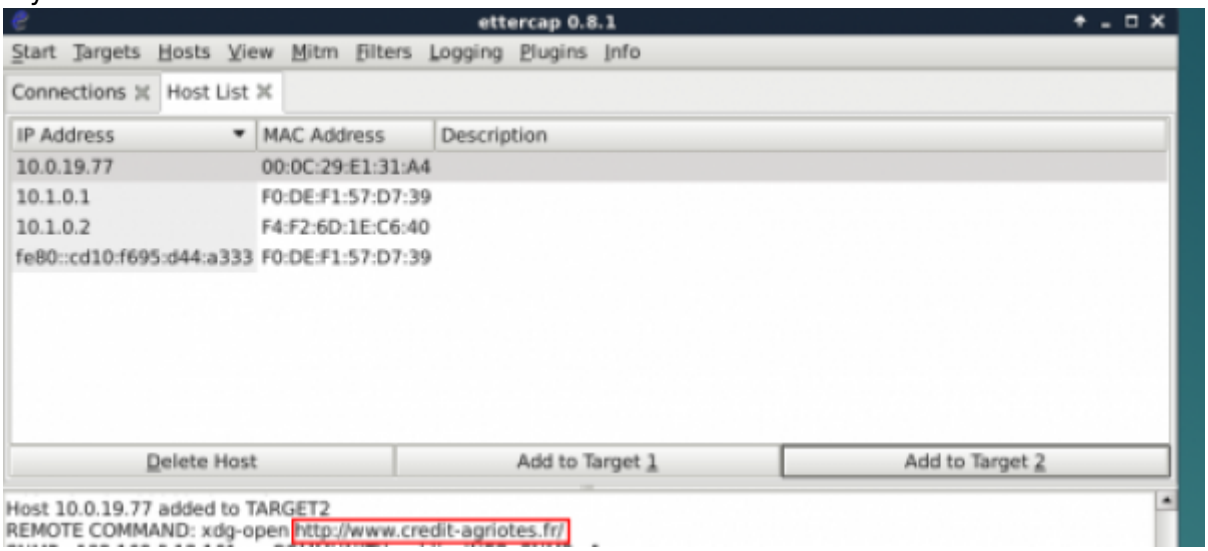
Le directeur de Corporate se rend sur le site web de sa banque en ligne au moyen de son navigateur préféré depuis son poste de travail:



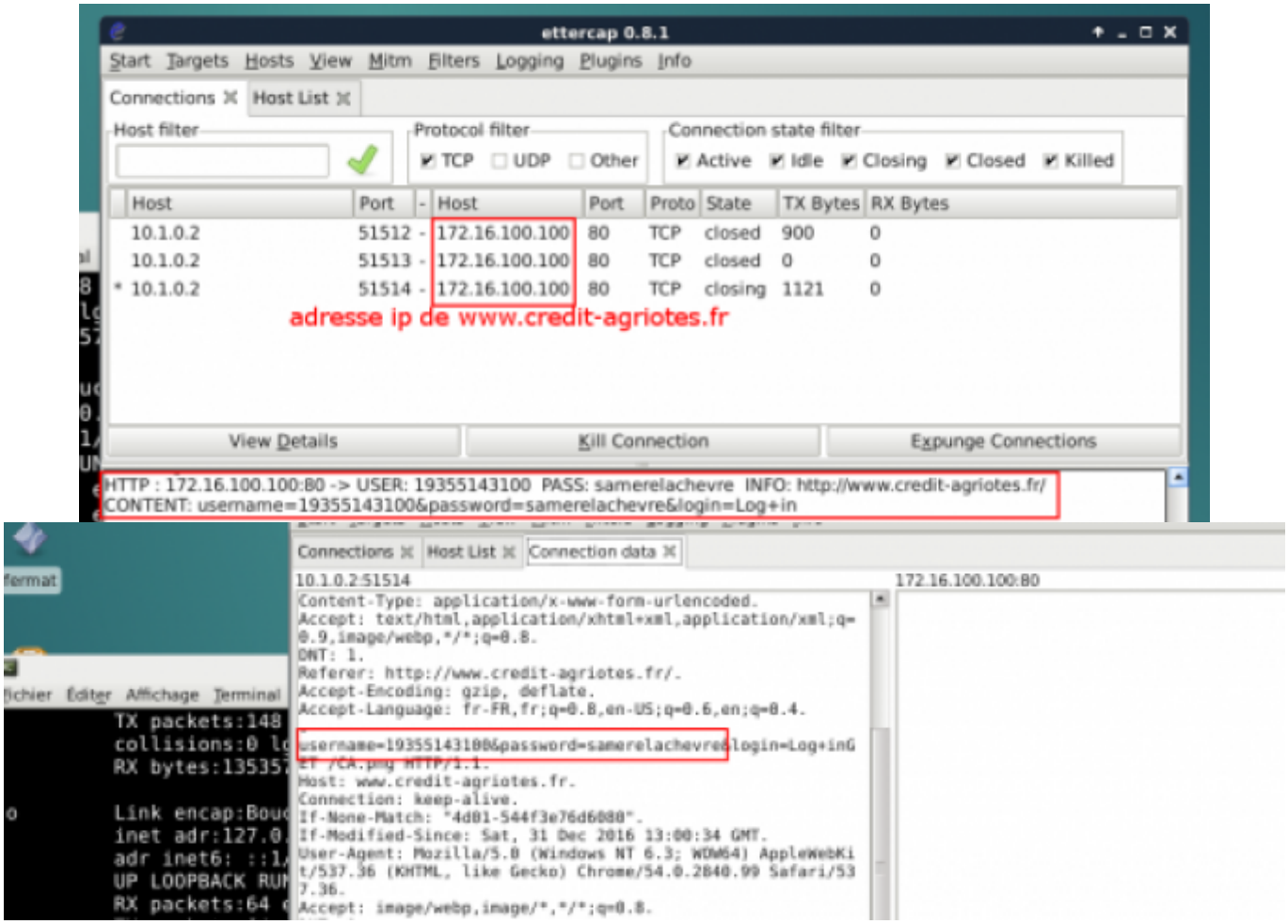
et renseigne son identifiant et mot de passe pour consulter ses comptes



Notre pirate ne rate rien de ce qui transite par son ordinateur désigné comme passerelle par défaut:
Nous voyons le site consulté :



Et nous pouvons tranquillement analyser les trames pour récupérer login et mot de passe :



Analyse

Ici aussi les causes sont doubles :

- Absence de chiffrement de la page web consultée: les données transitent en clair sur le réseau.
- Absence de protection contre un serveur DHCP pirate: celui-ci émet des trames DHCP OFFER sans cesse et répond aux demandes DHCP DISCOVER pour fournir la configuration en premier.

Dans le prochain chapitre nous verrons comment utiliser la technique du DHCP snooping pour protéger notre réseau d'un serveur DHCP indésirable.

Conclusion

Nous avons préparé, exécuté et analysé deux types d'attaques montrant la faiblesse de la sécurité de la couche 2. Ces attaques ne sont naturellement pas exhaustives... nous pouvons évoquer rapidement la saturation des tables d'adresses MAC pour bloquer le fonctionnement des commutateurs ou encore l'accaparement de toutes les adresses délivrées par le serveur DHCP par notre machine pirate avec yersinia[3] ou gobbler[4] par exemple.

Allons au chapitre suivant pour aborder les techniques pour s'en prémunir et/ou atténuer leurs effets.

1)
https://fr.wikipedia.org/wiki/Hub_Ethernet
2) 3)
,
http://www.yersinia.net/attacks.htm
4)
https://sourceforge.net/projects/gobbler/