Exemple d'attaque : ARP Spoofing

1 Objectifs

L'objectif de ce TP est de vous initier à certaines techniques dites d'*attaque* afin de vous faire prendre conscience de certains dangers liés aux réseaux. Pour ce faire, vous allez utiliser un environnement virtuel émulant un réseau de machines sous *Debian*. L'environnement virtuel que nous allons utiliser est *NEmu*[1].

2 Que dit le droit pénal ?

Article 323-1 : *Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.*

Article 323-2 : *Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.*

Article 323-3 : *Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.*

Article 323-3-1 : *Le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus ou spécialement adaptés pour commettre une ou plusieurs des infractions prévues par les articles 323-1 à 323-3 est puni des peines prévues respectivement pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.*

L'article 323 du code pénal comporte d'autres alinéas qui durcissent le tableau dressé ci-dessus. Ce TP est fait dans un cadre pédagogique et dans le but de vous faire prendre conscience de l'importance de la sécurité en informatique. L'utilisation des outils présentés ici dans un autre cadre et notamment au sein de l'université sera très sévèrement punis tant sur le plan universitaire que pénal.

3 Avant de commencer...

- Pour lancer le réseau virtuel :
  ```
  $ cd ~/VMs/VNET
  $ ./vnet nethack
  ```
- Pour quitter le réseau virtuel, tapez **quit()** dans le terminal principal.
- Pour sauvegarder le réseau virtuel, tapez **save()** et validez dans le terminal principal. Le réseau sera sauvegardé dans ∼ */nethack.tgz*.
- Pour restaurer le réseau virtuel :

1. http://nemu.valab.net

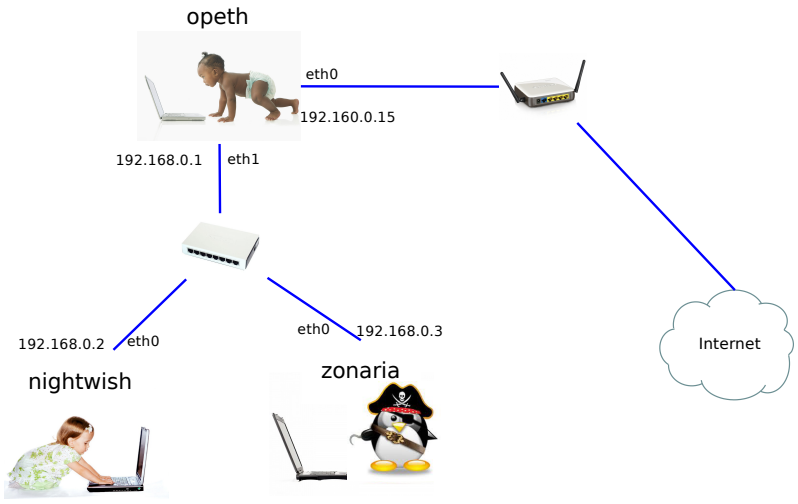
Vincent Autefage
autefage@labri.fr

```
$ cd ~/VMs/VNET
$ ./restore ~/nethack.tgz
```

– Les éditeurs *jed*, *nano* et *vi* sont installés sur le système.

4 Le réseau virtuel

Nous allons travailler sur le réseau suivant :



Les machines virtuelles vous sont livrées *nues*. C'est à dire qu'elles disposent uniquement des réglages élémentaires du système.

4.1 Amorçage du réseau

1) Lancez le réseau virtuel comme indiqué dans la section 3. Trois fenêtres correspondant aux consoles de chacune des machines devraient apparaître.

4.2 Configuration générale

2) Configurez le réseau virtuel (sauf l'interface *eth0* de *opeth*) comme indiqué sur le schéma grâce aux commandes **ifconfig** et **route**. Les masques de sous-réseaux sont tous de classe C.
Attention : N'oubliez pas d'activer l'*IP forwarding* sur la passerelle (*opeth*).

Rappels :

```
# ifconfig <iface> <@IP> netmask <netmask>
Exemple : ifconfig eth0 192.168.0.2 netmask 255.255.255.0
# route -n
# route add default gw <@IP passerelle>
# route del default
Exemple : route add default gw 192.168.0.1
```

Vincent Autefage
autefage@labri.fr

3) L'interface *eth0* d'*opeth* est reliée à un routeur qui fait plusieurs choses. Tout d'abord, il est capable de donner automatiquement une adresse IP aux machines qui lui demandent (serveur DHCP). Il est aussi connecté à Internet et permet de partager la connexion en faisant passerelle. Vous aurez donc deux niveaux de partage de connexion ! Le routeur partage avec *opeth*, qui partage ensuite avec le reste du réseau.

Configurez l'interface `eth0` d'*opeth* via le protocole DHCP en utilisant la commande :

```
# dhclient eth0
```

L'avantage de DHCP est qu'il configure à la fois l'adresse IP et la passerelle par défaut, ces deux infos étant fournies ici par le routeur. Vous pouvez vérifier que cela a fonctionné à l'aide d'*ifconfig* et de *route*.

Attention : le réseau correspondant à `eth0` sur *opeth* est 192.160.0.0 (pas 168 !). Il s'agit donc bien de deux réseaux différents pour `eth0` et `eth1`.

4) Lorsque l'on passe d'un réseau à un autre, il est d'usage de *masquer* les adresses des machines interne (par exemple 192.168.0.2 pour nightwish) en les remplaçant par celle de la passerelle. Cela est même souvent nécessaire car la machine destination pourrait se trouver, elle aussi, dans un réseau local de même adressage et ainsi envoyer les réponses à la mauvaise machine. Nous allons donc faire ce masquage au niveau d'*opeth*, et le routeur le fera lui-même aussi de son côté.

```
# iptables -t nat -A POSTROUTING --source 192.168.0.0/24 -j MASQUERADE
```

5) Tentez d'effectuer la commande suivante pour vérifier que *opeth* a bien accès à internet :

```
# wget www.labri.fr
```

Note : le ping est bloqué vers l'extérieur. C'est l'émulateur qui impose ça. On fait donc nos tests avec `wget`.

6) Recopiez le contenu du fichier */etc/resolv.conf* (sur *opeth*) sur *zonaria* et *nightwish*. Ceci permet d'indiquer à *zonaria* et *nightwish* le serveur DNS à utiliser.

7) Effectuez le test du *wget* sur *zonaria* et *nightwish*.

5 Mise en place d'une attaque de type *man in the middle*

5.1 ARP

Lorsqu'une machine veut communiquer avec une autre sur un même réseau local, elle effectue d'abord une requête *arp* de manière à acquérir l'adresse physique (appelée aussi MAC ou Ethernet) de la machine qu'elle cherche à joindre.

8) La table de correspondance entre adresse IP et MAC peut être consultée sur une machine grâce à la commande suivante :

```
# arp -n
```

Vincent Autefage
autefage@labri.fr

5.2 Principe de l'attaque

Les requêtes/réponses ARP étant faites en *broadcast*, le principe est de *spoofer*, c'est à dire inonder la victime (ici *nightwish*) de réponses ARP de manière à lui faire croire que l'adresse IP de la passerelle (ici *opeth*) qu'il souhaite contacter correspond à notre machine pirate (ici *zonaria*). Les communications à destination d'*opeth* seront donc dirigées vers nous au niveau physique. Pour passer inaperçu, il faut les retransmettre nous même à *opeth* au niveau physique, afin que la communication ait lieu (presque) normalement pour *nightwish*. De cette manière, *zonaria* peut intercepter tout le traffic de *nightwish* vers l'extérieur.

5.3 A l'abordage !

9) Passez tout d'abord en mode graphique sur *zonaria* grâce à la commande **startx**. Vous êtes maintenant sur l'environnement graphique léger *fluxbox*.

10) Sur *zonaria*, commencez par activer l'*IP forwarding*.

11) Ouvrez un terminal et utilisez la commande *arpspoof* de manière à réaliser votre attaque :

```
# arpspoof -t <@IP victime> <@IP vraie passerelle>
```

12) Ouvrez maintenant l'utilitaire *wireshark* (dans un nouveau terminal) afin de capturer le trafic qui passe sur votre interface réseau :

```
# wireshark -i eth0 -k
```

Vous constaterez le florilège de paquets ARP que vous êtes honteusement en train d'émettre...

13) Lancez une session graphique ainsi que le navigateur web sur *nightwish* et baladez vous un peu sur la toile...

14) Vous constaterez que *zonaria* trace tout ce que fait *nightwish*. Nous avons donc réussi.

15) (Questions annexes) Quels types de trames peut-on voir transiter ? À quelles couches du modèle OSI appartiennent elles ? Lorsque *nightwish* contacte un serveur web, plusieurs requêtes GET apparaissent. Pourquoi ?

16) En utilisant la page web de la mission FBI, tentez d'intercepter sur *zonaria* le mot de passe d'obama lorsque ce dernier se logue depuis *nightwish*.

17) Comment *nightwish* pourrait-il se rendre compte de cet ignoble complot ?

6 Conclusion

Vous avez pu constater la facilité ainsi que l'efficacité de cette méthode. En conclusion, nous pouvons affirmer qu'une adresse IP ne fait pas foie sur l'identité d'un interlocuteur. Il existe néanmoins des solutions comme *arpwatch* ou *arpalert* qui permettent de détecter ce genre d'attaque.

Vincent Autefage
autefage@labri.fr