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*[1], c'est à dire la distribution que vous utilisez actuellement. L'environnement virtuel que nous allons utiliser est *NEmu*[2].

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...

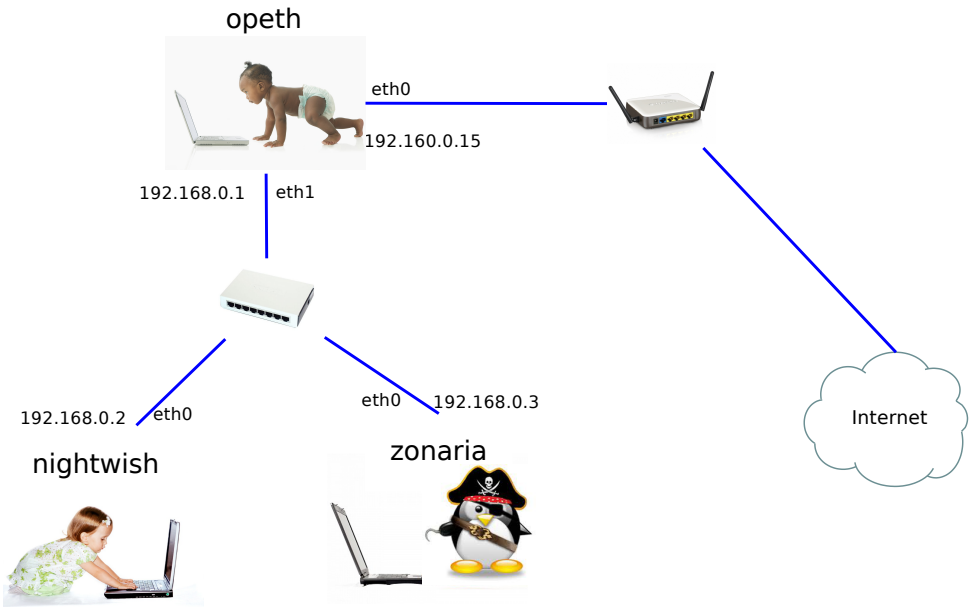
- Pour lancer le réseau virtuel :
  ```
  $ source /net/ens/vince/virt/nemu-init.rc
  $ nemu-kvm start
  $ nemu-vnet /net/ens/vince/virt/config/netspoof.py
  ```
- Pour quitter le réseau virtuel, tapez **quit()** dans le terminal principal.
- Pour sauvegarder le réseau virtuel, tapez **save()** et validez dans le terminal principal. Le réseau sera sauvegardé dans $\sim$ */netspoof.tgz*.
- Pour redémarrer (violemment) le réseau virtuel, tapez **reboot** et validez dans le terminal principal.
- Pour restaurer le réseau virtuel précédemment sauvegardé :
  ```
  $ nemu-restore ~/netspoof.tgz
  ```
- Les éditeurs *jed*[3], *nano*[4] et *vi*[5] sont installés sur le système.

1. http://www.debian.org
2. http://nemu.valab.net
3. http://www.jedsoft.org/jed
4. http://www.nano-editor.org
5. http://vim.sourceforge.net

Vincent Autefage
autefage@labri.fr

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. 3 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.
Atention : N'oubliez pas d'activer l'*IP forwarding* sur la passerelle (*opeth*).

Rappels :

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

3) L'interface *eth0* d'*opeth* est reliée à un routeur qui est lui même connecté à internet. Enregistrez *opeth* au près du routeur à l'aide de la commande suivante (sur *opeth*) :

```
# dhclient eth0
# iptables -t nat -A POSTROUTING --source 192.168.0.0/24 -j MASQUERADE
```

Vous obtenez ainsi automatiquement une adresse IP et une passerelle par défaut.

Vincent Autefage
autefage@labri.fr

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

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

5) 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.

6) 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

Lorsque une machine fait une requête à une autre machine sur un même réseau local, la machine appelante effectue une requête *arp* de manière à acquérir l'adresse physique (appelée aussi MAC) de la machine qu'elle cherche à joindre.

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

```
# arp -n
```

5.2 Principe

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*). Il faut ensuite transmettre ses requêtes à la véritable passerelle. De cette manière, notre machine pirate jouera le rôle de relais entre la victime et l'extérieur. Nous pourrons ainsi espionner toutes ses communications.

5.3 A l'abordage !

8) Passez tout d'abord en mode graphique sur *zonaria* grâce à la commande **startx**. Vous êtes maintenant sur l'environnement graphique léger *fluxbox*[6].

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

10) Ouvrez un terminal et utilisez la commande *arpspoof* de manière à réaliser le *man in the middle* :

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

11) 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 pourrez constater le florilège de paquets *arp* que vous êtes honteusement en train d'émettre...

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

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

14) Quels types de trames peut-on voir transiter ?

6. http://fluxbox.org

15) À quelles couches du modèle OSI appartiennent elles ?

16) Lorsque *nightwish* contacte un serveur web, plusieurs *GET* apparaissent. Pourquoi ?

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

18) Éteignez chaque machine correctement à l'aide de la commande **halt**. Tapez *quit()* dans la console principale pour quitter l'environnement virtuel.

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*[7] ou encore *arpalert*[8] qui permettent de détecter ce genre d'attaque.

7. http://ee.lbl.gov
8. http://www.arpalert.org/arpalert.html

Vincent Autefage
autefage@labri.fr