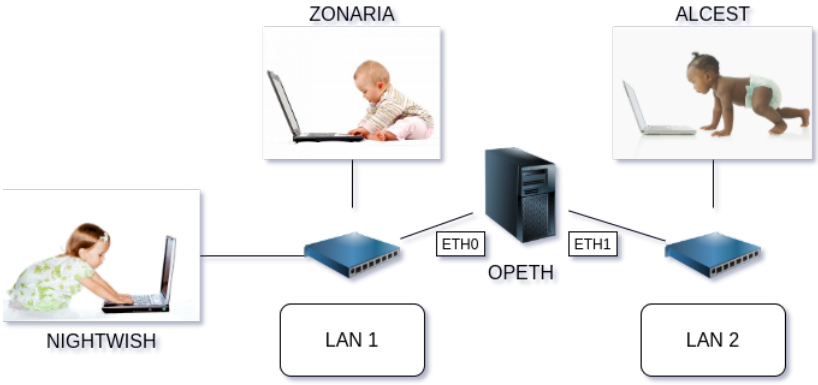
1 Objectifs

L'objectif de ce TP est de vous familiariser avec certains aspects de l'administration système et réseau sur un système de type Linux. Pour ce faire, vous allez utiliser un environnement virtuel émulant un réseau de machines sous *Debian*[1]. L'environnement virtuel que nous allons utiliser est *NEmu*[2].

2 Le réseau

Nous allons travailler sur le réseau suivant :



Nous pouvons constater que ce réseau est composé de deux sous-réseaux : *LAN 1* et *LAN 2*. *LAN 1* est composé des machines *nightwish*, *zonaria* et *opeth*. *LAN 2* est composé des machines *alcest* et *opeth*. La machine *opeth* est donc à la fois dans les deux réseaux jouant ainsi le rôle de passerelle. Les machines virtuelles vous sont livrées *nues*. C'est à dire qu'elles disposent uniquement des réglages élémentaires du système.

3 Avant de commencer...

- Dans un terminal régulier :
  - Pour lancer le réseau virtuel :
    `/net/ens/nemu/nemu-vnet netadm`
  - Pour restaurer le réseau virtuel précédemment sauvegardé :
    `/net/ens/nemu/nemu-restore ~/vnet/netadm.tgz`
- Dans le terminal de *NEmu* :
  - 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 `~/vnet/netadm.tgz`
  - Pour redémarrer (violemment) l'ensemble du réseau virtuel, tapez **reboot()** et validez dans le terminal principal
  - Pour redémarrer une seule machine virtuelle : **RebootVNode('<nom de la VM>')**
- Dans le terminal de chaque machine virtuelle :
  - Vous êtes administrateur de la machine virtuelle : compte **root** et mot de passe **plop**
  - Vous disposez d'éditeurs de texte simples dans les machines virtuelles : *micro*, *nano* et *vim*
  - Démarrez l'interface graphique par **startx**
  - Redémarrez une machine virtuelle par **reboot**
  - Arrêtez proprement une machine virtuelle par **poweroff** ou **halt**
  - Souris piégée dans une machine virtuelle : **CTRL+ALT+G**
  - Le pavé numérique n'est pas directement disponible : taper 2 fois sur la touche **Verr Num** pour l'activer
  - L'affichage dans une fenêtre est trop long : **Shift+PageUp** ou **Shift+PageDown** pour naviguer

1. http://www.debian.org
2. https://gitlab.com/v-a/nemu

Vincent Autefage
vincent.autefage@u-bordeaux.fr

1) Lancez le réseau virtuel comme indiqué ci-dessus. 4 fenêtres correspondant aux consoles de chacune des machines devraient apparaître.

4 Administration système

4.1 Gestion des utilisateurs

2) Les machines étant neuves, le seul compte existant est celui de l'administrateur. Identifiez vous donc en tant que *root*.

3) Changez le mot de passe *root* sur une des machines à l'aide de la commande **passwd** :

```
# passwd <login>
```

4) Ajoutez un nouvel utilisateur sur une des machines à l'aide de la commande **adduser** :

```
# adduser <login>
```

5) Tentez de vous connecter sur le compte de votre nouvel utilisateur à l'aide de la commande **login** :

```
# login <login>
```

6) Revenez sur le compte administrateur en quittant le compte courant avec la commande **exit**.

4.2 Gestion du système

Comme vous pouvez le constater à l'aide de la commande **hostname** ainsi que sur votre *prompt*, les machines portent toutes le même nom : *debian*. La commande **hostname** permet également de changer le nom de la machine :

```
# hostname <name>
```

Il est également nécessaire de se déconnecter et de se ré-identifier pour que les changements soient visibles.

7) Renommez une des machines, déconnectez-vous et ré-identifiez vous pour voir les changements. Redémarrez la machine grâce à la commande **reboot**. Que constatez vous ?

8) Pour régler ce problème il est nécessaire d'écrire en dur dans la configuration de la machine le nom désiré. Le nom doit être indiqué dans le fichier `/etc/hostname`. Configurez le nom de chaque machine tel qu'indiqué dans le schéma du réseau. Redémarrez ensuite chaque machine pour vérifier que vos changements sont bien enregistrés.

5 Administration de réseaux locaux

5.1 Plan d'adressage

Comme vous pouvez le constater sur le schéma du réseau, les machines *nightwish* et *zonaria* sont reliées au même switch tandis que *alcest* se trouve sur un switch différent. Les deux switchs sont reliés par la machine *opeth*. Le but est ici de créer deux sous-réseaux /**24**, soit un par switch.

9) Comment peut-on caractériser un réseau /**24** ?

10) Choisissez 2 réseaux distincts de cette taille. Le premier définira l'espace d'adressage du switch reliant *nightwish* et *zonaria* à *opeth*, et le deuxième celui entre *alcest* et *opeth*.

Vincent Autefage
vincent.autefage@u-bordeaux.fr

11) Choisissez en conséquence les adresses IP de :
- *eth0* sur *opeth*
- *eth0* sur *nightwish*
- *eth0* sur *zonaria*
- *eth1* sur *opeth*
- *eth0* sur *alcest*

5.2 Configuration dynamique

12) Attribuez les adresses IP grâce à la commande **ifconfig** ou **ip** :

```
# ifconfig                                  # lister les interfaces allumées
# ifconfig -a                               # lister toutes les interfaces
# ifconfig <iface> <@IP> netmask <netmask>  # configurer l'interface
# ifconfig <iface> up                       # allumer l'interface
# ifconfig <iface> down                     # éteindre l'interface

Exemple : ifconfig eth0 192.168.0.1 netmask 255.255.255.0
```

```
# ip -br addr                               # lister toutes les interfaces
# ip addr add <@IP>/<netmask> dev <iface>   # configurer l'interface
# ip link set <iface> up                    # allumer l'interface
# ip link set <iface> down                  # éteindre l'interface

Exemple : ip addr add 192.168.0.1/24 dev eth0
```

13) Testez votre configuration à l'aide de la commande **ping** entre les machines d'un même sous-réseau.
Attention : à ce stade, la communication entre *nightwish* et *alcest* est impossible car *opeth* rejette les paquets qui ne lui sont pas directement destinés.

14) Pour régler le problème, nous allons indiquer au système (*opeth*) qu'il doit transmettre les paquets qui ne lui sont pas destinés :

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

15) Pourquoi ne peut-on toujours pas faire communiquer *nightwish* et *alcest* ?

16) Indiquez sur *nightwish*, *zonaria* et *alcest* que *opeth* doit être leur passerelle par défaut grâce à la commande **route** ou **ip** :

```
# route -n                                      # lister toutes les routes
# route add default gw <@IP passerelle>         # ajouter une route par défaut
# route del default gw <@IP passerelle>         # supprimer une route par défaut

Exemple : route add default gw 192.168.0.1
```

```
# ip route                                      # lister toutes les routes
# ip route add default via <@IP passerelle>     # ajouter une route par défaut
# ip route del default via <@IP passerelle>     # supprimer une route par défaut

Exemple : ip route add default via 192.168.0.1
```

Il est également possible d'indiquer une passerelle spécifique par réseau de destination :

```
# route add -net <@IP réseau> netmask <netmask> gw <@IP passerelle>
Exemple : route add -net 192.168.1.0 netmask 255.255.255.0 gw 192.168.0.1
```

```
# ip route add <@IP réseau>/<netmask> via <@IP passerelle>
Exemple : ip route add 192.168.1.0/24 via 192.168.0.1
```

17) Testez maintenant la communication entre *nightwish* et *alcest* à l'aide de **ping** et **ssh**.

```
# ssh <login>@<destination>
Exemple: ssh root@192.168.0.1
```

18) Tracez le chemin de vos échanges grâce à la commande **traceroute** qui permet de lister l'ensemble des routeurs empruntés par votre paquet pour arriver à destination.

```
# traceroute <destination>
Exemple: traceroute 192.168.0.1
```

19) Mettez à jour les informations dans `/etc/hosts` sur *nightwish* pour pouvoir contacter *zonaria*, *alcest* et *opeth* par leur nom plutôt que par leurs adresses IP.

20) Redémarrez maintenant chaque machine à l'aide de la commande **reboot**. Que constatez vous en consultant la configuration réseau (adressage et table de routage) de vos machines ?

5.3 Configuration Statique

Les commandes telles que **route**, **ifconfig** et **ip** permettent d'effectuer des modifications temporaires mais ne permettent malheureusement pas de conserver la configuration lors du redémarrage de la machine.

21) Pour résoudre ce problème, nous allons devoir fixer la configuration réseau dans le fichier `/etc/network/interfaces` de chaque machine en respectant la syntaxe en exemple ci-dessous.
Attention : ne pas modifier les lignes déjà présentes dans le fichier.

```
auto eth0
iface eth0 inet static
  address 192.168.0.1
  netmask 255.255.255.0
  gateway 192.168.0.254
```

22) Après modification de la configuration l'interface doit être démarrée avec la commande suivante :

```
ifup eth0
```

23) On peut également éteindre l'interface grâce à la commande suivante :

```
ifdown eth0
```

24) Configurez le fichier `/etc/network/interfaces` de chaque machine et vérifier la validité de votre configuration avec les commandes **ip**, **ifconfig**, **route**, **ping** et **traceroute**.

25) Dans le cas de la machine *opeth*, nous allons devoir autoriser le transfert de paquet directement dans le fichier `/etc/network/interfaces` en ajoutant un appel de commande au démarrage de l'interface.

```
auto eth0
iface eth0 inet static
  address 192.168.0.1
  netmask 255.255.255.0
  gateway 192.168.0.254
  up echo 1 > /proc/sys/net/ipv4/ip_forward
```

26) Vérifiez la validité de votre configuration avec les commandes **ip**, **ifconfig**, **route** et **ping** après avoir démarrer / éteint vos interfaces réseaux.

5.4 Mise en place d'un serveur web

Nous allons mettre en place des serveurs web sur les machines *nightwish* et *zonaria* qui devront être accédés depuis *alcest*.

27) Passez en mode graphique sur *nightwish* et *zonaria* :

```
# startx
```

28) Écrivez une page simple dans le répertoire */var/www* des machines *nightwish* et *zonaria*.

29) Lancez (sur les deux machines) dans un terminal dédié le serveur web à l'aide de la commande suivante :

```
# busybox httpd -f -vv -h /var/www
```

30) Lancez le navigateur web et essayez de vous connecter à votre site web grâce à l'URL locale `http://127.0.0.1`

31) Essayez de vous connecter aux deux sites depuis *alcest* en utilisant leur adresse IP en guise d'URL.

32) Complétez le fichier `/etc/hosts` de la machine *alcest* de manière à pourvoir contacter vos sites avec un nom plutôt que d'utiliser les adresses IP.

6 Mise en place d'une attaque réseau de type *Man In The Middle*

6.1 Préambule juridique

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 des aspects de sécurité dans la mise en place d'un système informatique. L'utilisation des outils présentés ici dans un autre cadre et notamment au sein de l'université est sévèrement puni tant sur le plan universitaire que pénal.

6.2 Le protocole 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.

33) La table de correspondance entre adresse IP et MAC peut être consultée sur une machine grâce aux commandes suivantes.

```
# arp -n
# ip neigh
```

6.3 Principe

Les requêtes (*broadcast*) et réponses (*unicast*) ARP permettent de faire le lien ; le principe est donc de *flooder*, 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 les messages IP de la victime 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. Ce type d'attaque par vole d'identité s'appelle du *spoofing*. La technique qui consiste à s'insérer dans une communication en tant que relais intermédiaire illicite s'appelle l'attaque de *l'homme du milieu* ou *Man In The Midlle* (MITM).

6.4 A l'abordage !

34) Passez tout d'abord en mode graphique sur *zonaria*.

35) Sur *zonaria*, commencez par activer l'*IP forwarding* qui permet à une machine de devenir passerelle en autorisant la ré-émission de paquets qui transitent à travers elle.

Rappels :

```
# echo 1 > /proc/sys/net/ipv4/ip_forward
```

36) Ouvrez un terminal et utilisez la commande **arpspoof**[3] de manière à réaliser le *man in the middle*.

```
# arpspoof -t <@IP victime> <@IP vraie passerelle>
Ici : arpspoof -t <@IP nightwish> <@IP opeth>
```

37) Ouvrez maintenant l'utilitaire **wireshark**[4] (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...

38) Lancez une session graphique ainsi que le navigateur web sur *alcest* et connectez vous au serveur web de *nightwish*.

39) Vous constaterez que *zonaria* trace tout ce qu'envoie *nightwish*. Nous avons donc réussi.

40) Stoppez l'attaque ARP en cours puis réaliser l'attaque dans le sens inverse ; faite croire à *opeth* que *zonaria* est en fait *nightwish*.

41) Stoppez le serveur web de *nightwish*.

42) Ajoutez une authentification au site web de *nightwish* grâce à la commande suivante :

```
# echo "/:<username>:$(busybox httpd -m '<password>')" > /etc/httpd.conf
Exemple: echo "/:monsuperuser:$(busybox httpd -m 'monsupermotdepasse')" > /etc/httpd.conf
```

3. http://www.monkey.org/~dugsong/dsniff
4. http://www.wireshark.org

43) Relancez le serveur web à l'aide de la commande suivante :

```
# busybox httpd -f -vv -h /var/www -r "Restricted Area:" -c /etc/httpd.conf
```

44) Connectez vous au site web depuis *alcest*.

45) Tentez de retrouver les identifiants de connexion dans l'instance **wireshark** sur *zonaria*. Vous constaterez qu'il est assez aisé de récupérer les informations contenues dans une requête web pour peu qu'elles soient sensibles...

46) Comment pourriez-vous vous prémunir d'une telle attaque ?

47) Éteindre chaque machine correctement à l'aide de la commande **poweroff**.

7 Création d'un réseau étendu

48) Mettez vous par groupe de 2 machines physiques. Vous allez maintenant créer un super-réseau composé de chacun de vos sous-réseaux. Pour ce faire, **l'un** des groupes doit héberger le switch principal. Pour cela, récupérez d'abord l'adresse IP du poste physique de ce groupe :

```
$ /sbin/ifconfig eth0
```

Lancez ensuite le réseau virtuel comme ceci (pour le premier groupe) :
`/net/ens/nemu/nemu-vnet netadm`

```
[nemu]-> slink()
```

L'autre groupe doit **ensuite** lancer le réseau virtuel comme ceci :
`/net/ens/nemu/nemu-vnet netadm`

```
[nemu]-> clink('<@IP du groupe principal>')
```

Exemple :

```
# Premier groupe [adresse IP physique : 192.168.42.42]
[nemu]-> slink()

# Second groupe
[nemu]-> clink('192.168.42.42')
```

49) Configurez maintenant chacun vos sous-réseaux (**ip**, **ifconfig** et **route**) en vérifiant bien que vous n'utilisez pas les mêmes adresses de sous-réseaux. Par exemple, si un des groupes utilise l'adresse de sous-réseau 10.0.0.0/24 (netmask 255.255.255.0), entre *opeth*, *nightwish* et *zonaria*, il ne faut pas que l'autre groupe fasse de même. Tous les masques doivent être en /**24**.

50) Configurez maintenant l'interface *eth2* de *opeth* qui est reliée au switch principal qui permet de faire la jointure entre les sous-réseaux de vos deux groupes.

51) Vous devez maintenant indiquer les routes nécessaires afin de pouvoir faire communiquer toutes les machines du super-réseau. Pour ce faire, vous avez juste à configurer les passerelles par défaut sur vos deux machines *opeth*.

52) Vérifiez votre configuration avec les commandes **ip**, **ifconfig**, **route**, **traceroute** et **ping**.

53) Ajoutez un site web sur chacune de vos machines *nightwish* et tentez d'y accéder mutuellement depuis vos machines *alcest*.

8 Réaliser une attaque par dictionnaire

Nous allons tenter de réaliser une attaque par dictionnaire dans le but de percer l'authentification à un site web protégé par mot de passe. Une telle attaque se base sur une liste de mots de passe appelée *wordlist* généralement stockée sous forme de fichier texte. Cette liste de mots de passes peut être obtenue par génération automatique ou bien extraite d'un vol de données préalable. Certaines listes se vendent également sur le *darkweb*.

54) Sécurisez votre site web présent sur *nightwish* comme vu dans la section 6.4 avec le login **admin**. Votre mot de passe doit figurer dans le fichier `/usr/share/john/password.lst`.
Attention : Ne communiquez pas votre mot de passe à l'autre groupe, celui-ci va essayer de le découvrir tout seul.

55) Tentez de découvrir le mot de passe de l'autre groupe depuis votre machine *zonaria* en réalisant une attaque par dictionnaire à l'aide du programme *hydra* :

```
# hydra -V -f -l admin -P /usr/share/john/password.lst http-get://<IP nightwish de l'autre groupe>
```

56) Comment pourriez vous faire pour lancer une telle attaque sans connaître le login ?

57) Comment pourriez vous faire pour lancer une telle attaque sur plusieurs sites web différents ?

58) Comment pourriez vous vous prémunir d'une telle attaque ?

9 Fin

59) Éteindre chaque machine correctement à l'aide de la commande **poweroff**. Vous pouvez ensuite sauvegarder votre session à l'aide de la commande **save()** et quitter l'environnement avec la commande **quit()** dans le terminal principal.

Vincent Autefage
vincent.autefage@u-bordeaux.fr