Sûreté et sécurité

Exercices 1, outils de base

1 Configuration d'un réseau de machines linux (IPv4)

Question A. Premier réseau. Dans Marionnet construire un réseau contenant 2 machines `m1`, `m2`, `m3`, connectées via un hub. À l'aide de ifconfig configurer les IP des machines du réseau à 192.168.2.11, 192.168.2.12 et 192.168.2.13. Vérifier que vous pouvez bien atteindre chacune des machine à partir des deux autres avec `ping`.

Question B. Réseau persistant. Éteindre les machines du réseau précédent (pour cela toujours utiliser le bouton *Shutdown all*). Redémarrer (*Start all*). Pouvez-vous faire un `ping` entre deux machines ? Rendre la configuration réseau persistante en utilisant le fichier `/etc/network/interfaces` (`man interfaces` en cas de doute). Tester avec ping (pensez à activer la configuration). Éteindre, rallumer, tester.

Question C. Écoute réseau. lancer la commande `tcpdump` sur `m2` et depuis `m1` faire un ping vers `m3`. Que fait `tcpdump` ? Testez un ping de `m1` vers lui-même. Expliquer la différence. Remplacer le hub par un switch et recommencer le ping de `m1` vers `m3`. Expliquer la différence. Remettez un hub à la place du switch pour la suite, nous n'en avons pas fini d'écouter le réseau. Un outil plus élaboré pour l'écoute du réseau est `wireshark`. Testez-le.

Question D. Noms de machine. Changer le nom de chacune des trois machines `m1`, `m2`, `m3`. Appelez les : `tommie`, `peter` et `john`. Sur un réseau réel on pourrait changer le nom des machines en utilisant le fichier `/etc/hostname`. Sur Marionnet Pour y arriver, il est nécessaire d'éteindre toutes les machines et de modifier ce nom dans les menus (mais le fichier `hostname` sera bien modifié).

Depuis Tommie faites `ping tommie`. Comment faire pour que Tommie puisse "pinguer" John ?

En utilisant le fichier `/etc/hosts` faire en sorte que Tommie puisse trouver l'adresse des deux autres machines à partir de leurs nom.

Question E. Serveur de nom. La méthode basée sur `/etc/hosts` suppose que chaque machine du réseau ait la liste de l'ensemble des noms du réseau et les adresses IP associées, dont elle pourrait avoir besoin. Cela n'est bien entendu pas pratique et même sur un petit réseau il vaut mieux déléguer cette connaissance à un serveur de nom que chaque machine pourra alors interroger. N'importe quelle machine du réseau peut servir de serveur de nom. Nous allons en installer une nouvelle, appelée `ns1`. Le plus difficile est de configurer le serveur de nom, `bind`, en particulier de créer les bons fichiers de zone. En voici un qui devrait faire l'affaire.

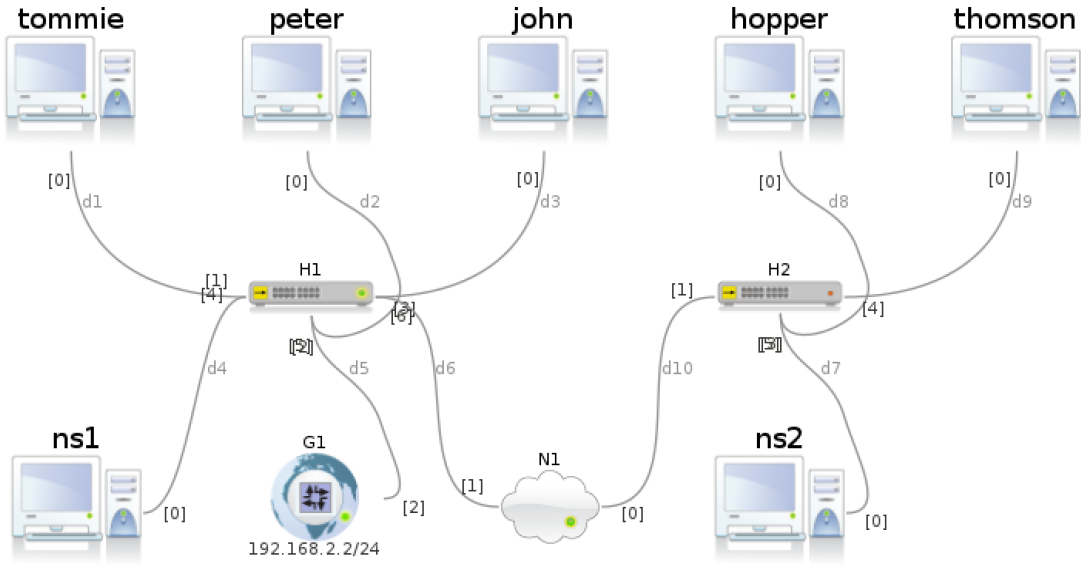
```
$TTL 86400
$ORIGIN sport.org.
@ IN SOA sport.org. root.sport.org. (
  2016021621 ; increment n'oublie pas !
  28800      ; refresh
  3600       ; update retry
  2W         ; expire
  38400      ; minimum
);
        IN NS ns1
ns1     IN A 192.168.2.10
tommie  IN A 192.168.2.11
peter   IN A 192.168.2.12
john    IN A 192.168.2.13
www     IN A 192.168.2.11
```

Nommez ce fichier `/etc/bind/zones/sport.org.db` et appelez le dans `/etc/bind/named.conf.local` de la façon suivante :

```
zone "sport.org" {
    type master;
    allow-transfer {
       127.0.0.1;
       localnets;
    };
    file "/etc/bind/zones/sport.org.db";
    allow-query {any; };
};
```

Démarrez le serveur de nom à l'aide de la commande `/etc/init.d/bind9 start`. Il faut aussi modifier `/etc/resolv.conf` sur chacune des machines, voyez vous comment ? Testez votre configuration en faisant des ping sur les noms de machines (en donnant explicitement le domaine et sans le donner). Testez également avec `dig` (ou `nslookup`).

Question F. Augmenter le réseau. Agrandir le réseau en ajoutant trois machines `hopper` d'IP 192.168.2.21, `thomson` d'IP 192.168.2.22 et `ns2` d'IP 192.168.2.20, connectez les avec un hub relié au premier hub par un sous-réseau inconnu. Vous pouvez également ajouter une passerelle vers le grand internet, comme sur l'illustration mais elle ne fonctionnera sans doute pas. Configurez ns2 en serveur de nom sur le domaine `informatique.org` pour ces trois nouvelles machines. Testez. Pouvez-vous faire un ping de Tommie à Hopper ? En utilisant les noms de machines ou les IPs ? Pourquoi ?



Question G. Relais DNS En ajoutant la clause suivante dans `/etc/bind/named.conf.local` sur `ns1` vous permettrez aux requêtes arrivant à `ns1.sport.org` d'être transmises par `ns1` à `ns2` et à la réponse de `ns2` d'être transmise par `ns1` (selon la configuration, cette réponse pourra aussi être pourra alors être mis en cache par `ns1` pour accélérer les réponses suivantes).

```
zone "informatique.org" {
        type forward;
        forwarders {
                192.1698.2.20;
        };
};
```

Faîtes de même sur ns2.

Question H. Serveur web Lancez le service apache2 sur Tommie pour en faire un serveur web. Testez avec le navigateur web `lynx` à partir de n'importe quelle autre machine du réseau. Par défaut les pages servies sont le contenu de `/var/www/`. Transformez la page par défaut de façon à ce qu'elle contienne un formulaire. Lancez une écoute du réseau avec `wireshark` sur Thomson et connectez-vous depuis Hopper via lynx sur le serveur. Renseignez le formulaire. Que voit Thomson ? Au début l'internet était comme ça, et il était très facile d'écouter les mots de passe de ses voisins de réseau. heureusement la cryptographie est venue à la rescousse.

2 Utilisation de ssh

Question I. Clé publique, clé privée. générer une paire de clés ssh sur votre compte sercal et placer votre clé publique sur la machine virtualbox de façon à pouvoir vous loguer en tant que `personne` directement sur la machine virtuelle sans taper de mot de passe. Pouvez-vous utiliser votre paire de clé pour vous loguer sur les autres machines du sercal. Pourquoi ?

Question J. Copier avec `scp`. Testez votre clé en copiant un fichier depuis votre compte vers la machine, puis dnas le sens inverse (mais toujours à partir de l'hôte).

Question K. Tunnel `ssh`. Créer un tunnel ssh pour que Hopper puisse se connecter au formulaire web de Tommie sans divulguer d'informations aux tiers.

Les tunnels ssh peuvent rendre de nombreux services mais ça n'est pas très pratique lorsqu'il s'agit seulement de donner de la confidentialité à une communication avec un serveur. Il vaut mieux

configurer son serveur pour utiliser la crypto nativement (quitte à utiliser starttls).

3 SSL et TLS avec openssl

Le livre Openssl Cookbook de Ivan Ristic contient deux chapitres libres d'accès très utiles pour comprendre l'utilisation de openssl. En vous aidant de ce livre effectuez les tâches suivantes.

Question L. Help ! lister les commandes disponibles et pour la commande `rsa` lister les options possibles.

Question M. Clé RSA. Générer une paire de clés RSA (public, privé) de taille de clé 2048 protégée par AES 256, dans des fichiers séparés et vérifier le contenu des deux clés.

Question N. Génération d'un certificat auto-signé. Créer une demande de CSR pour votre clé au nom de master-pls.org. Comme aucune autorité de certification ne doit être dérangée pendant le TP, signez vous même le certificat. Optionnel : installer le certificat dans Apache et configurez la résolution de nom de façon à pouvoir le tester.

Question O. Utilisation de la commande `s_client`. Utiliser `telnet lipn.fr 80` pour vous connecter comme client web sans ssl au serveur du LIPN. Tapez les deux lignes suivantes suivies d'une ligne vide (rapidement) :

```
HEAD / HTTP/1.0
Host: lipn.fr
```

Que dit la réponse ? Utiliser `s_client` pour vous faire la même requête en ssl.

4 Pretty good privacy avec gnupg

Question P. GPH. En utilisant le *GNU Privacy Handbook* (GPH), créer une paire de clés gpg et un certificat de répudiation, échanger vos clés publiques et échangez des messages cryptés (tester également les messages cryptés de façon symétrique). Construire un réseau de confiance, en vérifiant les signatures *IRL*.

5 Backups

Question Q. Exemple de backupninja. Installer backupninja sur la machine virtuelle VirtualBox et configurez là pour effectuer une sauvegarde des quelques éléments sur votre compte sercal (utiliser une clé ssh. Pensez à la supprimer à la fin du TP).

6 Docker

Question R. Whalesay. Faire le tutoriel en ligne de Docker (il n'est pas nécessaire de vous créer un compte sur le Hub Docker).

Question S. Dockerfile. Utiliser une image pour installer un service dans un conteneur (par exemple phpbb), modifier le Dockerfile pour faire une image qui vous convienne.

7 Bréviaire de commandes `Docker` (en construction)

Docker hub	
`search` terme	retourne une liste d'images publiques
`pull` hub-image	charger une image
`login -u pb`	se loguer sur un registre docker (hub,...)
`push` image	envoyer une image

Conteneurs	
`run` image commande	exécute la commande dans un nouveau conteneur
`run -t -i` img `/bin/sh`	exécute `i` nteractivement sh dans un `t` ty
`run -d` ...	démonise le conteneur
`ps`	affiche la liste des conteneurs actifs
`ps -l`	affiche le dernier conteneur démarré
`ps -a`	affiche les conteneurs actifs et stoppés
`kill` conteneur	termine le conteneur
`logs` conteneur	voir l'affichage du conteneur
`logs -f` conteneur	comme `tail -f`
`stop` conteneur	stopper le conteneur
`run -P` ...	map tous les ports vers des ports éphémères
`run -p 82:80` ...	map le port 80 du conteneur vers le 82 de l'hôte
`port` conteneur `80`	retourne 82
`top` conteneur	liste les processus du conteneur
`inspect` conteneur	retourne un json config/status
`rm` conteneur	

Images	
`images`	liste les images locales
`run ubuntu:14.04`	exécute l'image du repo ubuntu, taguée 14.04
`run ubuntu`	exécute l'image du repo ubuntu, taguée latest
`pull` hub-image	pre-load une image (par layers)
`ubuntu`	image racine (Docker Inc)
`mindsized/thym`	image utilisateur
cible	image cible : `user/nom_image:tag`
`commit -m` msg id cible	crée une image à partir du conteneur id
`tag` img-id cible	crée un nouveau tag pour une image (la même ?)
`build -t` cible	crée une image à partir du `./Dockerfile` [...]
`build -f` dockerfile	pour spécifier le Dockerfile

Syntaxe des `Dockerfile`	`Références`
INSTRUCTION statement	ligne d'un fichier `Dockerfile`
`# un commentaire`	ligne de commentaire
`FROM` image	conteneur initial
`MAINTAINER` pb <p@siz.dk>	doit-il avoir un rapport avec le compte dhub ?
`RUN` commande	exécute la commande (en tant que root)
`CMD` ["cmd", "param1",...]	commande par défaut à exécuter au lancement
`VOLUME` /myvol	crée un point de montage...
`USER` personne	change l'utilisateur courant
`WORKDIR` /opt/bla	change le répertoire courant
...	