TP1 : Outils de l'administrateur réseau et installation du service DNS

Préambule : Obtenir votre topologie pour sur le cyber-range

Se connecter au cyber-range avec le client hyneview, votre login (de la forme « fise_lastname ») et le mdp spécifique qui vous a été transmis en TP. Le nom du serveur est **matrix.telecomnancy.univ-lorraine.fr:4063**

Ouvrir la fenêtre (Fichier > Ouvrir) listant les topologies et trouver la topologie intitulée « Bootcamp votre_nom ».

Vous avez maintenant à disposition un embryon de SI d'entreprise (virtualisé) qu'il va falloir progressivement enrichir avec de nouveaux services à installer et configurer (DNS, web, mail, LDAP, etc.) au fur et à mesure des séances de TP.

Ces TPs sont faits pour vous familiariser avec certains services réseau essentiels. N'ayez pas peur de tester et de vous tromper ici où il n'y a pas de conséquences. Le cyber-range permet de restaurer facilement une image à son état initial.

Vérifier que les interfances WAN et LAN ont bien des adresses IP. Si besoin, configurer les inferfaces WAN/LAN de pfsense : menu 1 (assign interfaces), no VLANs, WAN sur em0, LAN sur em1 et appliquer la mise à jour. Vérifier la connectivité du client.

A noter : Le login et mdp des images linux est « hns ». Le login et mdp par défaut de pfsense sont respectivement : « admin » et « pfsense ».

Partie I : Configuration réseau d'une machine sous Linux-debian

1. Les commandes **ip link** et **ip address** permettent d'afficher et de modifier la configuration des interfaces réseaux. Identifier et indiquer les différents paramètres utiles à la configuration de votre interface réseau principale. La commande **ip link** permet également d'activer ou de désactiver une interface (ip link set up/down dev <if>). La commande **ifconfig** permettait auparavant d'obtenir ces informations, mais il est déconseillé de l'utiliser depuis qu'elle est dépréciée.

2. Les commandes **ip route** et **ip -6 route** permettent d'afficher et de manipuler les tables de routage de votre système. Quelles sont les gateways par défaut respectives du serveur et du client ?

3. La commande **systemctl** est désormais la norme pour configurer les services, l'ancienne commande **service** et les scipts d'initialisation initctl (*upstart*) étant dépréciés.
   - **systemctl start/stop/restart** *nom_du_service.service* permet de démarrer, d'arrêter ou de redémarrer des services du système d'exploitation ;
   - **systemctl enable/disable** *nom_du_service.service* permet de configurer un service pour qu'il se lance au démarrage ;
   - **systemctl** is-active *nom_du_service.service* permet de vérifier si un service est actif ;
   - **systemctl** status *nom_du_service.service* permet d'obtenir les dernières entrées du service dans le log system ;
   - **systemctl** list-units --type=service permet de lister tous les services actifs du système.

   Essayer les 3 dernières commandes avec le service *networking*.

4. La configuration des interfaces réseaux peut être faite manuellement dans le fichier **/etc/network/interfaces** (ou /etc/sysconfig/network dans certains systèmes). Il permet de définir une configuration manuelle ou via DHCP pour chaque inferface comme illustré par les exemples ci-dessous.

```
auto eth0
iface eth0 inet static
        address 192.168.1.10
        netmask 255.255.255.0
        gateway 192.168.1.1
```

```
auto eth0
iface eth0 inet dhcp
```

   D'autres commandes sont utiles :
   - Redémarrer le service réseau : systemctl restart networking.service
   - Démonter et remonter une interface : ifdown eth0 ; ifup eth0 ;
   - Configurer une route par défaut: ip route add default gw 192.168.1.1 dev eth0

5. De nombreux autres utilitaires ou commandes systèmes constituent la boite à outil de l'administrateur. Pour chacune des commandes listées ci-après, l'installer (si besoin) **sur le serveur**, lire la page de son manuel, donner son utilité, expliquer son fonctionnement et donner un exemple d'utilisation : **ping/ping6**, **traceroute**, **netstat**, **nmap**, **host**

6. **ssh** est un utilitaire fondamental qui permet de se connecter de manière sécurisée (à travers une connexion chiffrée) à un hôte distant (voir également son corollaire scp). Installer et paramétrer le service ssh sur le serveur et tester son bon fonctionnement depuis le client.

Partie II : Configuration du service DNS

II.1. DNS côté client

Rappel: relire si besoin les slides du cours de RS présentant le service DNS.

1. Configurer le service de résolution **du client** afin qu'il utilise le serveur DNS de l'école 193.50.27.27. Il faut pour cela remplacer l'adresse IP spécifiée pour le *nameserver* dans le fichier **resolv.conf**. Vérifier la bonne prise en compte du nouveau serveur DNS en effectuant une capture réseau sur le switch au niveau de la topologie.

2. Observer avec Wireshark les requêtes DNS générées lors de la consultation de sites web. Expliquer l'utilité de ce service.

3. Montrer comment la résolution locale avec le fichier **/etc/hosts** peut prendre le pas sur le service DNS. Quel en est l'impact est terme de sécurité? Pour information, l'ordre de consultation des bases de données est défini dans le fichier /etc/nsswitch.conf.

4. **dig** permet d'envoyer des requêtes DNS et de consulter les réponses. **nslookup** et **host** proposent un service similaire mais moins complet. A l'aide de l'outil **dig** , effectuer différents types de requêtes DNS (directe, inverse, mail exchange, name server, etc.). Pour chaque requête, expliquer les éléments de réponses donnés.

5. Interroger l'annuaire DNS inversé avec la commande **whois** pour obtenir des informations relatives à quelques domaines de votre choix.

II.2. DNS côté serveur

1. Installer le programme Berkley Internet Naming Daemon (*sudo apt-get install **bind9***) qui permet d'exécuter un serveur DNS. Redémarrer le service :
   sudo systemctl restart bind9.service

2. Les fichiers de configuration de **bind** sont stockés dans */etc/bind/* . Configurer votre serveur comme simple relais (avec mise en cache des réponses) vers le serveur DNS de la topology au dessus de la votre dans le cyberrange, à savoir 172.16.1.1 . Il faut pour cela décommenter la section *forwarders* du fichier *named.conf.options*. Et ajouter l'option *forward first ;*

3. Configurer ensuite votre client afin d'utiliser le serveur de résolution nouvellement configuré. Capturer une requête DNS avec Wireshark et vérifier qu'elle passe bien par votre serveur.

4. A l'aide d'une nouvelle capture de paquets, illustrer le bon fonctionnement du serveur relais. Quel est l'utilité de ce type de serveur ?

5. Configurer le serveur bind afin qu'il permette la résolution directe des machines de votre zone *votre_nom.bootcamp.univ-lorraine.fr*. Pour cela, ajouter la zone suivante au fichier *named.conf.local*

```
zone "votre_nom.bootcamp.univ-lorraine.fr" {
    type master;
    file "/etc/bind/db.votre_nom.bootcamp.univ-lorraine.fr";
};
```

   Créer ensuite le fichier de renseignement du domaine en vous inspirant de *db.local* . Les liens suivant peuvent vous aider à renseigner votre zone :
   - https://help.ubuntu.com/community/BIND9ServerHowto
   - https://www.installerunserveur.com/configuration-bind9

   Vous devez notamment créer les entrées de type NS, MX pour votre domaine pointant vers votre adresse IP WAN. Le nom www peut être un alias (type CNAME) vers le nom choisi pour votre serveur.

   Enfin, il faut créer une règle de redirection du port DNS (53) du WAN vers l'adresse IP LAN de votre serveur afin que les requêtes DNS venant de l'extérieur lui parvienne. Vérifiez également que les services DNS de pfsense (Resolver et Forwarder) sont désactivés afin qu'il n'interfère pas avec le service DNS que vous mettez en place.

   Une fois votre zone configurée, relancer le service bind et vérifier qu'il n'y a pas d'erreur en consultant le syslog :
   sudo tail /var/log/syslog

   Tester le bon fonctionnement de votre zone depuis le client en demandant la résolution des différents noms.

> Questions facultatives <

6. Faire de même avec la résolution inverse en créant la zone suivante et en vous inspirant du fichier *db.127* pour créer le fichier correspondant. Vérifier avec **dig -x** la résolution inverse.

```
zone "X.168.192.in-addr.arpa" {
        type master;
        notify no;
        file "/etc/bind/db.192";
};
```

7. Configurer une seconde VM en tant que serveur secondaire de votre zone et configurer le transfert de zone entre le maître et l'esclave.

Au niveau du maître, il faut rajouter la clause « allow-transfer { @IP_esclave; }; » pour chaque zone (normale et inverse).

Au niveau esclave, il faut remplacer le « type »par *slave* et ajouter la ligne : « master {@IP_DNS_principal ;} ; »

Montrer à l'aide d'une capture comment se fait le transfert.