

Lancer machines virtuelles

Lancer : `~/iut-vms/vnet/nemu-vnet <nom>`

Restore: `~/iut-vms/vnet/nemu-restore ~/vnet/netadm.tgz`

`save()` `reboot()` `quit()`

Commandes principales

passwd: Change le mot de passe d'un utilisateur

adduser: Ajoute un nouvel utilisateur

traceroute: Liste l'ensemble des routeurs empruntés par un paquet pour arriver à destination

ifup eth0: Configure une interface réseau définie dans le fichier `/etc/network/interfaces`

ifdown eth0: Déconfigure une interface réseau définie dans le fichier `/etc/network/interfaces`

ifconfig: Configure et affiche les informations des interfaces réseau IP. Argument possibles:

- -a: Affiche toutes les interfaces, actives ou non
- eth0: Obtenir les informations de l'interface eth0
- netmask: Assigner un masque de sous réseau
- up/down: Activer/désactiver une interface.

busybox httpd -f -vv -h /var/www: Lance un serveur web avec le code html présent dans le dossier `/var/www`. L'ip du serveur web est alors `http://IP_de_la_machine`

arp: Protocole effectuant la traduction d'une adresse IP en une adresse ethernet. Arguments possibles:

- -n: Affiche la table de correspondance entre adresse IP et MAC.

wireshark -i eth0 -k: Ouvrir wireshark en écoute sur l'interface eth0.

systemctl restart isc-dhcp-server: Redémarrer le service DHCP.

systemctl status isc-dhcp-server: Vérifier l'état du service DHCP.

dhclient -d eth0: Démarrer le client DHCP.

dhclient -r eth0: Indiquer la libération du bail.

Questions

Comment peut-on caractériser un réseau/24 ?

Un réseau /24 se caractérise par: "Les 24 bits de points fort soit les plus à gauche correspondent à la partie réseau de l'adresse IP." En gros cela veut dire que le masque de sous-réseau sera codé sur 24 bit, soit les 24 premiers bits à gauche auront comme valeur 1. Soit le masque de sous-réseau suivant: 255.255.255.0

Afin de créer une passerelle par défaut:

```
route add default gw + IP
```

Qu'est ce qu'une attaque "Man In The Middle " ?

C'est une attaque permettant d'intercepter des paquets entre deux parties, sans que ni l'un ni l'autre ne puisse s'en rendre compte.

Comment faire ?

Utiliser la commande `arp spoof -t <@IP victime> <@IP vraie passerelle>`

Qu'est ce que DHCP ?

Le DHCP est un protocole réseau chargé de la configuration automatique des adresses IP

Comment configurer le réseau DHCP ?

Ajoute une bloc subnet vide dans /etc/dhcp/dhccpd.conf.

Exemple:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
    range 192.168.1.2 192.168.1.12 // Autorise le client DHCP les 10 IP
de cet intervalle.
    // Si on veut affecter une adresse fixe:
    host server {
        hardware ethernet a2:00:00:00:00:07;
        fixed-address 192.168.1.13;
    }
}
```

Principaux PATH

Pour indiquer qu'un système doit faire office de passerelle, soit actier le routage IP ou l'IP forwarding:

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

Associer une adresse IP à un nom:

`nano /etc/hosts` et modifier le fichier

Fixer la configuration réseau:

`/etc/network/interfaces`

Exemple:

```
auto eth0
iface eth0 inet static
    address 192.168.1.3
    netmask 255.255.255.0
    gateway 192.168.1.1
```

`/etc/default/isc-dhcp-server` indiquer à la ligne `INTERFACESv4` la valeur `eth0`, afin de n'activer le futur service DHCP que sur la première interface réseau (`eth0`).

`/etc/dhcp/dhcpd.conf`: Fichier de configuration de DHCP.

`tail -20 /var/log/syslog`: Permet d'accéder aux 20 dernières lignes des logs DHCP.

`/var/lib/dhcp/dhclient.eth0.leases`: Permet d'accéder à tous les baux DHCP du client

`cat /var/lib/dhcp/dhclient.leases`: Permet d'accéder à tous les baux DHCP qu'à délivrer le serveur.