But du TP

L'objectif de ce TP est de vous présenter les outils clés utilisés pour l'administration et la surveillance d'un réseau. Ce TP s'appuie sur le cours *ResEl 102 : Présentation des notions de réseau utilisées au ResEl*.

Sommaire

1 Présentation des principaux outils

1.1 Configuration d'une carte reseau : `ifconfig`

Cette commande a pour objectif d'associer une adresse IP (ou plusieurs) a une carte réseau. Pour consulter la configuration de la machine que vous utilisez, il vous suffit d'exécuter la commande `/sbin/ifconfig` dans un terminal.

Pour pouvoir modifier la configuration d'une carte réseau, les droits superutilisateur sont nécessaires.

1.2 La table de routage : `route`

Lorsque vous postez une lettre, le centre de tri de La Poste va l'envoyer vers votre correspondant en utilisant son adresse postale.

Ici, nous sommes dans le même cas : lorsque que vous envoyez des informations, elles sont encapsulées dans des paquets IP (les enveloppes du courrier). Votre système d'exploitation va envoyer ces derniers sur la bonne carte réseau en utilisant sa table de routage (correspondance entre les villes et les codes postaux).

La commande `/sbin/route` affiche la table de routage de votre machine.

Voici un exemple de table de routage :

```
gateway:~# route -n
Kernel IP routing table
Destination     Gateway         Genmask         Flags Iface
192.168.0.0     172.16.19.1     255.255.255.0   UG
192.44.76.0     0.0.0.0         255.255.255.0   U     eth0
172.16.0.0      0.0.0.0         255.255.0.0     U     eth1
10.0.0.0        0.0.0.0         255.0.0.0       U     eth2
0.0.0.0         192.44.76.1     0.0.0.0         UG
```

Donnez pour cet exemple le nom de l'interface réseau sur laquelle les paquets suivants seront envoyés :

- un paquet a destination de 10.0.0.42 :
- un paquet a destination de 192.168.0.21 :
- un paquet a destination de 192.168.66.6 :
- un paquet a destination de `www.commentcamarche.net`[1] :

Vous devriez maintenant comprendre le resultat de l'exécution de la commande `/sbin/route` sur votre machine.

1.3 Correspondance adresse IP et adresse MAC : ARP

Exécutez la commande `/sbin/arp`, suivie de la commande `ping` vers la machine `pc-df-204.enst-bretagne.fr`, puis a nouveau la commande `arp`.

Que constatez vous de différent au niveau du résultat de la commande `arp` ?

Est-il possible de revenir a l'état précédent[2] ?

2 Sniffing

Dans cette partie nous allons créer une connexion entre un client (`telnet`) et un serveur (`netcat`) puis observer le traffic qui transite entre les 2 machines (acte de *sniffing*).

2.1 Préparation

Pour réaliser l'opération, nous allons ouvrir 3 terminaux :

- un sur la machine `local.maisel.enst-bretagne.fr` ;
- deux sur `sunshine.maisel.enst-bretagne.fr`.

Pour vous connecter sur `sunshine`, vous devez utiliser la commande `ssh`. Pour obtenir les droits superutilisateur, utilisez la commande `sudo`. Pour l'utilisation de ces deux commandes, reportez-vous au cours *ResEl 101 : Cours sur les outils Linux*.

[1] Si vous voulez connaître l'adresse IP associée a ce nom de domaine, utilisez la commande `dig`. Cette dernière va contacter le serveur DNS pour vous et vous renvoyer la réponse.

[2] Pour cela, aidez-vous de la page de manuel de arp : `man arp`

2.2 Présentation de `tethereal`

`tethereal` est un outil qui permet de lire les paquets qui sont recus et émis par les interfaces réseau. Pour avoir un résultat *human-readable* des paquets, il vous suffit de lancer la commande suivante avec les droits superutilisateur : `tethereal -T text -V -x`.

2.3 Création d'une communication entre un client telnet et un serveur netcat

`netcat` est aussi appelé « le couteau suisse des réseaux ». Lancez-le en écoute sur un port supérieur à 1024 depuis la machine sunshine (sur un de vos 2 terminaux).

Dans le terminal sur la machine local, à l'aide de la commande `telnet`[3], connectez-vous sur le port d'écoute de netcat que vous avez choisi précedament.

À partir de maintenant les caractères que vous écrivez dans le terminal `telnet` sur `local` sont envoyés sur votre serveur netcat de sunshine, et affiché dans le terminal de sunshine.

2.4 Sniffing

Maintenant exécutez la commande `tethereal` en mode superutilisateur (et avec le filtre que l'on vous a fourni) dans votre second terminal sur sunshine. Utilisez ensuite la communication que vous avez créé dans la section précédente.

Dans le terminal d'exécution de tethereal, vous voyez transiter les paquets entre telnet et netcat... Vous devriez pouvoir retrouver l'information que vous avez envoyé !

2.5 Utilisation de `netstat` et `lsof`

Quels types d'informations apportent les commandes `netstat` et `lsof`, en général ?

Et dans notre cas ?

3 Récuperation d'un mot de passe d'une connexion FTP

Une machine se connecte de maniere périodique au serveur FTP de sunshine. À l'aide de l'outil `tcpdump`[4], essayez de récuperer le mot de passe de sa session FTP ainsi que le nom de l'utilisateur. Si vous réussissez, connectez vous avec `lftp`, `gftp` ou `ftp` pour vérifier que vous avez bien récuperé un nom d'utilisateur et un mot de passe valide.

[3] La syntaxe est : `telnet sunshine numéro_de_port`

[4] `tcpdump` est un outil équivalent à `tethereal`.

4 Présentation d'un échange de paquets IPv6

Voici 2 paquets IPv6, expliquez leurs utilités d'après leurs champs spécifiques :

```
Ethernet II, Src: 00:05:5d:6c:0f:08, Dst: 33:33:00:00:00:01
    Destination: 33:33:00:00:00:01 (IPv6-Neighbor-Discovery_00:00:00:01)
    Source: 00:05:5d:6c:0f:08 (D-Link_6c:0f:08)
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 56
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: fe80::205:5dff:fe6c:f08 (fe80::205:5dff:fe6c:f08)
    Destination address: ff02::1 (ff02::1)
Internet Control Message Protocol v6
    Type: 134 (Router advertisement)
    Code: 0
    Checksum: 0x7b59 (correct)
    Cur hop limit: 64
    Flags: 0x00
        0... .... = Not managed
        .0.. .... = Not other
        ..0. .... = Not Home Agent
        ...0 0... = Router preference: Medium
    Router lifetime: 1800
    Reachable time: 0
    Retrans time: 0
    ICMPv6 options
        Type: 3 (Prefix information)
        Length: 32 bytes (4)
        Prefix length: 64
        Flags: 0xe0
            1... .... = Onlink
            .1.. .... = Auto
            ..1. .... = Router Address
            ...0 .... = Not site prefix
        Valid lifetime: 0x000000f0
        Preferred lifetime: 0x00000078
        Prefix: 2001:660:7302:3::
    ICMPv6 options
        Type: 1 (Source link-layer address)
        Length: 8 bytes (1)
        Link-layer address: 00:05:5d:6c:0f:08

Ethernet II, Src: 00:0d:93:b2:52:74, Dst: 33:33:ff:b2:52:74
    Destination: 33:33:ff:b2:52:74 (IPv6-Neighbor-Discovery_ff:b2:52:74)
    Source: 00:0d:93:b2:52:74 (AppleCom_b2:52:74)
```

```
    Type: IPv6 (0x86dd)
Internet Protocol Version 6
    Version: 6
    Traffic class: 0x00
    Flowlabel: 0x00000
    Payload length: 24
    Next header: ICMPv6 (0x3a)
    Hop limit: 255
    Source address: :: (::)
    Destination address: ff02::1:ffb2:5274 (ff02::1:ffb2:5274)
Internet Control Message Protocol v6
    Type: 135 (Neighbor solicitation)
    Code: 0
    Checksum: 0xa6e7 (correct)
    Target: 2001:660:7302:3:20d:93ff:feb2:5274 (2001:660:7302:3:20d:93ff:feb2:5274)
```

5 Aller plus loin : `iptables`

L'objectif est d'interdire à la machine de la partie 3 de se connecter sur sunshine via FTP, et de lui renvoyer par la même occasion un message d'erreur ICMP. Pour cela, il faut modifier le fichier de configuration du firewall (`iptables`) et relancer le firewall à l'aide de la commande suivante : `/etc/init.d/iptables restart`.

Pour compléter ce « script », nous vous conseillons de regarder ces trois documents :
- `http://christian.caleca.free.fr/netfilter/iptables.htm` ;
- `http://lea-linux.org/reseau/secu/iptables.html` ;
- `http://www.siliconvalleyccie.com/linux-hn/iptables-intro.htm`.

Quels outils utiliseriez-vous pour garder en mémoire la tentative de connexion de la machine de la partie 3 ?