Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

Réseaux Avancés II

Examen — mai 2018

Durée : 1h30 — Tous documents autorisés

Programmation Python avec Scapy — 9 points

1 – 4pts *Dans cet exercice vous considérerez que vous pouvez intercepter tout le trafic qui circule dans le réseau.*

On veut pouvoir **identifier** si une machine qui réalise un « *ping* » dans le réseau, c-à-d l'envoi de paquet ICMP, exécute l'OS Windows ou l'OS Linux.

xterm

```
pef@ns:/home/pef$ ping -c 2 8.8.8.8
PING 8.8.8.8 (8.8.8.8) 56(84) bytes of data.
64 bytes from 8.8.8.8: icmp_seq=1 ttl=58 time=13.6 ms
64 bytes from 8.8.8.8: icmp_seq=2 ttl=58 time=13.6 ms

--- 8.8.8.8 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 13.618/13.650/13.682/0.032 ms
```

Suivant l'OS qu'elle utilise le paquet ICMP est différent :

xterm

```
>>> ping_linux
<Ether  dst=00:11:de:ad:be:ef src=00:50:56:c0:00:08 type=IPv4 |<IP  version=4L
ihl=5L tos=0x0 len=84 id=54669\
 flags= frag=0L ttl=64 proto=icmp chksum=0x252d src=192.168.127.1
dst=192.168.127.156 options=[]
|<ICMP  type=echo-request code=0 chksum=0xdbb7 id=0xdd4e seq=0x1
|<Raw  load='Uv\xf8Z\x00\x00\x00\x00\x88\x14\x0b\x00\x00\x00\x00\x1f
!"#$%&\'()*+,-./01234567' |>>>>

>>> ping_pc
<Ether  dst=00:11:de:ad:be:ef src=00:0c:29:d1:27:40 type=IPv4 |<IP  version=4L
ihl=5L tos=0x0 len=60 id=758\
 flags= frag=0L ttl=128 proto=icmp chksum=0xb740 src=192.168.127.157
dst=192.168.127.156 options=[]
|<ICMP  type=echo-request code=0 chksum=0x4d5a id=0x1 seq=0x1
|<Raw  load='abcdefghijklmnopqrstuvwabcdefghi' |>>>>
```

Écrivez un programme utilisant la **bibliothèque Scapy** qui permet :

- d'intercepter des paquets ICMP
- d'indiquer si la machine dont le paquet a été intercepté tourne sous Linux ou Windows.

Vous éviterez de donner plusieurs fois la même information.

2 – 5pts Écrire un programme de « *chat* » **dissimulant les messages échangés** dans le contenu de paquet ICMP.

- ▷ *Vous déciderez et décrirez comment les informations nécessaires à son fonctionnement sont échangées, ou non, entre les interlocuteurs (choisissez les options les plus simples) ;*
- ▷ *Vous prendrez soin à ce que les paquets échangés ressemblent à un « ping » normal.*

Est-ce que le fonctionnement de votre programme peut être gêné par la machine sur laquelle il est exécuté ? Si oui, comment y remédier ?

IPv6 — 11 points

3 – Analysez la trame suivante :
4pts

```
0000   00 05 73 A0 00 00 DA E7  8F CD 7C F5 86 DD 60 0D   ..s.......|...`.
0010   37 8C 00 28 06 40 26 07  53 00 00 60 00 5C D8 E7   7..(.@&.S..`.\..
0020   8F FF FE CD 7C F5 26 07  F8 B0 40 04 08 02 00 00   ....|.&...@.....
0030   00 00 00 00 20 04 D5 DA  01 BB F7 DE 05 BF 00 00   .... ...........
0040   00 00 A0 02 70 80 00 B5  00 00 02 04 05 A0 04 02   ....p...........
0050   08 0A 01 37 20 4A 00 00  00 00 01 03 03 08         ...7 J........
```

a. Que contient la trame ? *(2pts)*
Vous donnerez une description pertinente.

b. Est-elle passée par un routeur ? *(1pt)*

c. Est-ce que les adresses IPv6 ont été obtenues par « **auto-configuration** » ? *(1pt)*
Analysez ces adresses et justifiez votre réponse.

4 – Le réseau d'entreprise a été décomposé :
5pts

- en différentes « *locations* » associés à des VLANs :

notation décimale	**VLAN**
1	
2	
3	
4	

- en différents « *usages* » :

not. décimale	**Usage**
01	
02	
10	

L'entreprise obtient du RIPE NCC le préfixe réseau IPv6 `2001:2:a::/48`.

Questions :

a. Vous donnerez un premier plan d'adressage en IPv6 des différents VLANs en notation hexadécimale regroupée par « *nibble* » ou quartet, privilégiant le **routage**. *(2pts)*

b. Vous donnerez l'adresse IPv6 de la machine *M* d'adresse MAC « `00:05:73:a0:00:00` » pour son appartenance au VLAN 4 et pour un usage 10. *(1pt)*

c. Sur quelle taille de préfixe vont être définies les informations de routage entre les différents réseaux ? *(1pt)*

d. Donnez une règle de firewall permettant le blocage de l'accès au Web pour la machine *M*. *(1pt)*
Est-ce qu'il est possible d'étendre cette règle à l'usage « `10` » ? *Si oui comment ?*

5 – a. Est-ce que le « *broadcast* » est toujours utilisé dans IPv6 et pourquoi ? *(1pt)*
2pts

b. Expliquez comment il est possible d'utiliser le protocole « *ping* » pour découvrir les autres machines d'un réseau local ? *(1pt)*