Faculté des Sciences & Techniques — Université de Limoges

Master 1ère année

Réseaux Avancés II

Examen — mai 2019

Durée : 1h30 — Tous documents autorisés

Programmation Python avec Scapy — 10 points

1 – 4pts Lors de l'examen de RésAvI de janvier 2019, vous avez écrit un programe d'**exfiltration de donnés** d'un secret utilisant le champs TOS d'un paquet pour transmettre un octet de ces données à la fois.

```
xterm
>>> IP().show()
###[ IP ]###
  version= 4
  ihl= None
  tos= 0x0
  len= None
  id= 1
  flags=
  frag= 0
  ttl= 64
  proto= hopopt
  chksum= None
  src= 127.0.0.1
  dst= 127.0.0.1
```

a. Comment allez vous reconnaître les paquets de votre interlocuteur ? *(1pt)*

b. Écrivez un programme Python/Scapy réalisant la récupération du message envoyé par cette méthode. *(3pts)*

2 – 6pts On veut programmer un outil d'« *OS fingerprint* », c-à-d qui découvre la nature de l'OS utilisé par la machine, en se basant sur l'observation suivante :

OS	TTL	taille fenêtre TCP
Linux kernel 2.x	64	5840
Android/Chrome OS	64	5720
Windows XP	128	65536
Windows 7	128	4128
Cisco	255	4128
FreeBSD	64	65535

On remarque que lors de l'établissement de la communication TCP, chaque machine envoie la valeur de sa fenêtre, « window », et la valeur du TTL.

Suivant les différentes combinaisons de valeurs, on peut identifier l'OS utilisé par la machine qui a envoyé le paquet.

Dans Scapy, pour obtenir les champs composant TCP :

```
xterm
>>> ls(TCP())
sport     : ShortEnumField                = 20              (20)
dport     : ShortEnumField                = 80              (80)
seq       : IntField                      = 0               (0)
ack       : IntField                      = 0               (0)
dataofs   : BitField (4 bits)             = None            (None)
reserved  : BitField (3 bits)             = 0               (0)
flags     : FlagsField (9 bits)           = 2               (2)
window    : ShortField                    = 8192            (8192)
chksum    : XShortField                   = None            (None)
urgptr    : ShortField                    = 0               (0)
options   : TCPOptionsField               = {}              ({})
```

a. Si on peut observer les paquets échangés lors de l'établissement de la communication TCP, est-ce que l'on peut identifier l'OS : *(1pt)*
   - ◇ uniquement du client ?
   - ◇ uniquement du serveur ?
   - ◇ les deux simultanément ?

b. Est-ce qu'il est possible d'identifier l'OS d'une machine de manière active, c-à-d en provoquant l'échange de paquets TCP ? *(1pt)*

c. Écrivez un programme Python utilisant Scapy qui réalise le travail d'identification des OS en écoutant le trafic circulant dans un réseau (on considérera que l'on est capable d'intercepter tout les paquets échangés). *(4pts)*
   Pour chaque machine, on affichera : son adresse IP et l'OS détecté (dans le cas où on n'aura pas pu réaliser cette identification on indiquera « OS inconnu »).

▬▬▬ IPv6 — 10 points

3 – Analysez la trame suivante :
5pts

```
0000   78 92 9C E4 5B 83 DE 30  05 DD 1C B4 86 DD 60 00   x...[..0......`.
0010   00 00 00 18 2C 2F 26 07  53 00 00 60 00 5C DC 30   ....,/&.S..`.\.0
0020   05 FF FE DD 1C B4 20 01  41 D0 FE 0B 85 00 A8 E2   ...... .A.......
0030   43 FF FE 2A AC 3D 11 00  00 11 D1 56 C0 4E 00 00   C..*.=.....V.N..
0040   00 00 03 77 77 77 06 67  6F 6F 67 6C 65 03         ...www.google.
```

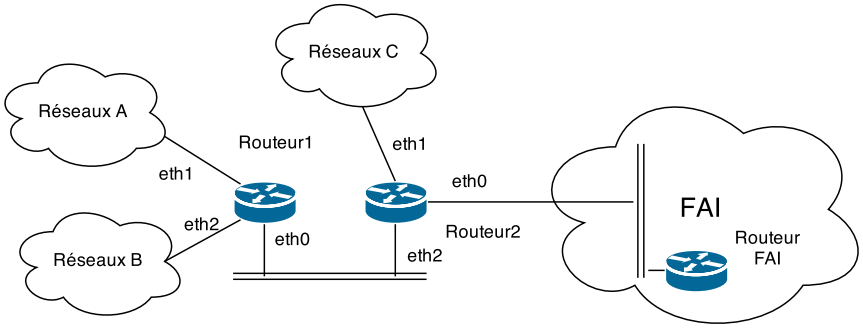
a. Que contient la trame ? *(2pts)*
Vous donnerez une description pertinente.

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.

d. Peut-on apprendre des informations sur la nature du matériel en réception et/ou en envoi ? *(1pt)*

4 – Soit le réseau d'entreprise suivant, découpé en 3 sous-réseaux :
5pts
- ▷ Réseaux A « `172.16.200.0/24` » ;
- ▷ Réseaux B « `172.16.100.0/24` » ;
- ▷ Réseaux C « `172.16.300.0/24` ».



et la configuration suivante :

Routeur 1
- ☐ `eth0:192.168.1.10/24` ;
- ☐ `eth1:172.16.200.0/24` ;
- ☐ `eth2:172.16.100.0/24` ;

Routeur 2
- ☐ `eth0:193.50.123.32/24` ;
- ☐ `eth1:172.16.300.0/24` ;
- ☐ `eth2:192.168.1.20/24` ;

Le routeur FAI possède l'adresse IP « `193.50.123.254` ».

Pour votre **migration IPv6**, vous obtenez le préfixe `2003:8b:0c::/56` de la part de votre FAI.
Le routeur du FAI possède l'adresse IPv6 `2003:8b:0c:ff:ff:ff:ff:ff/64`

a. En IPv6, comment le routeur « *Routeur1* » peut découvrir **automatiquement** « *Routeur2* » ? *(1pt)*

b. Est-ce qu'il est nécessaire que le **réseau d'interconnexion** des routeurs disposent d'un préfixe global ? *(1pt)*
Donnez l'adresse IPv6 de type « *SLAAC* » pour l'interface `eth0` de « *Routeur1* » d'adresse MAC `38:60:77:4f:56:eb`.

c. Donnez le **plan d'adressage IPv6** pour les réseaux A, B et C. *(2pts)*

d. Donnez la **table de routage IPv6** de « *Routeur2* ». *(1pts)*