Université de Limoges | FACULTÉ DES SCIENCES ET TECHNIQUES

Master 1ère année

Réseaux Avancés II

Examen — mai 2015

Durée : 2h — Tous documents autorisés (sauf sur support électronique)

Programmation Python avec Scapy — 7 points

Dans ces exercices vous considérerez que vous pouvez intercepter tout le trafic qui circule dans le réseau.

1 – 7pts On veut réaliser un outil permettant de **détecter** un audit réalisé de manière «silencieuse» par l'outil `nmap` vers une machine quelconque du réseau dans lequel on se trouve.

Soit la trace suivante du lancement de l'outil d'audit `nmap` réalisant un audit silencieux vers la machine `libpfb.so` et à destination du port 2400 :

```
xterm
bob@scapy:~$ sudo nmap -sS libpfb.so -p 2400
```

Soit la capture de trafic suivante, sur la machine qui subit l'audit et sur laquelle un serveur TCP attend sur le port 2400 :

```
xterm
pef@libpfb:/home/pef sudo tcpdump -i eth0 port 2400
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth0, link-type EN10MB (Ethernet), capture size 65535 bytes
17:36:15.051689 IP scapy.unilim.fr.59445 > libpfb.so.2400: ↵
  Flags [S], seq 4280895084, win 1024, options [mss 1416], length 0
17:36:15.051728 IP libpfb.so.2400 > scapy.unilim.fr.59445: ↵
  Flags [S.], seq 2349581930, ack 4280895085, win 29200, options [mss 1460],length 0
17:36:15.184728 IP scapy.unilim.fr.59445 > libpfb.so.2400: ↵
  Flags [R], seq 4280895085, win 0, length 0
```

Questions :

a. Décrivez brièvement le comportement de l'audit silencieux et indiquez comment il est «silencieux». *(1pt)*

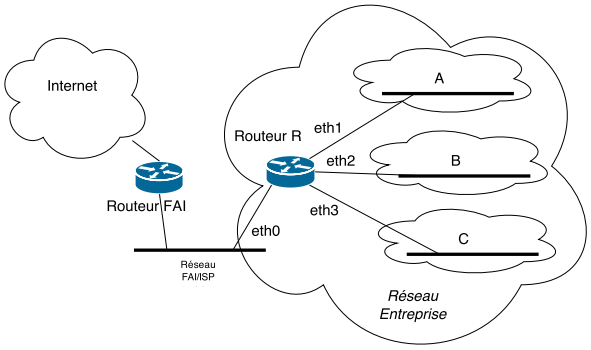
b. Écrivez un programme Python utilisant la bibliothèque Scapy qui intercepte le trafic réseau et détecte ce genre d'échange. *(3pts)*
Vous considérerez n'importe quelle machine cible et pas seulement la machine `libpfb.so` indiquée dans la trace.

c. On veut maintenant rendre «visible» l'audit sur la machine cible qui le subit, afin que les outils de sécurité mis en œuvre sur cette machine cible l'enregistrent dans leurs fichiers de journalisation. *(3pts)*

Ajoutez à votre programme précédent le code Python nécessaire au «rejeu» de la tentative de connexion, en prenant la place originale de l'attaquant et en la rendant «visible».

IPv6 — 9 points

2 – 9pts Une entreprise dispose du réseau suivant :



et des informations suivantes :

- Routeur FAI
  `2608:5200:60:ff:ff:ff:ff:ff`
- Réseau affecté à l'entreprise par le FAI :
  `2608:5200:5c::/48`
- interface eth0 du Routeur R :
  `2608:5200:60:ff:ff:ff:ff:42`
- 3 usages sont répertoriés :
  - «Administration» pour le réseau A ;
  - «Développement» pour le réseau B et pour le réseau C ;
  - «Invité» non encore affecté.

Questions :

a. Donnez une configuration pour chacun des réseaux A, B et C en suivant la méthodologie fournie par le RIPE NCC pour organiser son réseau en bits L, G et B en **privilégiant la localisation**, sachant qu'il y a 3 usages répertoriés : *(1,5pts)*

Réseau	Adresse Réseau	Adresse de l'interface du Routeur R dans le réseau
?	?	?
...	...	...

b. Donnez maintenant une configuration en **privilégiant les usages**, sachant qu'il y a 3 usages répertoriés. *(1,5pts)*

Réseau	Adresse Réseau	Adresse de l'interface du Routeur R dans le réseau
?	?	?
...	...	...

c. Donnez la table de routage du «Routeur R» interne à l'entreprise permettant la communication entre les 3 réseaux en reprenant les informations de votre configuration **privilégiant la localisation** : *(1,5pts)*

Destination	Adresse prochain saut
`default`	?
...	...

Comment les «usages» sont intégrés dans le routage ? Est-il nécessaire d'en tenir compte ?

d. Donnez la table de routage du «Routeur R» interne à l'entreprise permettant la communication entre les 3 réseaux en reprenant les informations de votre configuration **privilégiant les usages** : *(1,5pts)*

Destination	Adresse prochain saut
`default`	?
...	...

Comment les «localisations» sont intégrées dans la configuration ? Est-il nécessaire d'en tenir compte ?

On veux mettre en place une protection à l'aide du firewall NetFilter présent sur le «Routeur R» en utilisant la Policy «DROP» par défaut et en respectant les consignes suivantes :

- Interdire les accès vers le serveur SSH du Routeur R en provenance d'Internet (TCP, port 22) ;
- Autoriser les accès Web depuis Internet vers l'entreprise pour l'usage Administration (TCP, port 80) ;
- Autoriser les accès Web vers Internet pour l'usage Développement, Administration et Invité (TCP, port 80) ;

e. Donnez la configuration du firewall pour la configuration «privilégiant la localisation». *(1,5pts)*

f. Donnez la configuration du firewall pour la configuration «privilégiant les usages». *(1,5pts)*

Analyse de trame — 4 points

3 – 4pts Analysez la trame suivante :

```
0000   33 33 00 00 00 FB 08 00  27 FD CF F7 86 DD 60 00
0010   00 00 00 91 11 FF 20 01  41 D0 FE 2E 07 00 0A 00
0020   27 FF FE FD CF F7 FF 02  00 00 00 00 00 00 00 00
0030   00 00 00 00 00 FB 14 E9  14 E9 00 91 3E 15 00 00
0040   84 00 00 00 00 02 00 00  00 00 01 37 01 66 01 66
0050   01 63 01 64 01 66 01 65  01 66 01 66 01 66 01 37
0060   01 32 01 30 01 30 01 61  01 30 01 30 01 30 01 30
0070   01 30 01 30 01 30 01 30  01 30 01 30 01 30 01 30
0080   01 30 01 30 01 38 01 65  01 66 03 69 70 36 04 61
0090   72 70 61 00 00 0C 80 01  00 00 00 00 00 0D 05 73
00a0   61 6D 75 73 05 6C 6F 63  61 6C 00 C0 60 00 1C 80
00b0   01 00 00 00 00 00 10 FE  80 00 00 00 00 00 00 0A
00c0   00 27 FF FE FD CF F7
```

a. Que contient la trame ?
Vous donnerez une description détaillée et pertinente.

b. Est-elle passée par un routeur ?

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

d. Est-ce que le codage des options de TCP est différent en IPv6 par rapport à IPv4 ?