Examen Administration des Systèmes et des Réseaux
Durée 2 heures
Documents autorisés
Portables, ordinateurs et téléphones, éteints

J-M Moreno

Mardi 25 mars 2014

Attention

Sauf indication contraire, les questions sont indépendantes. Vous devez expliciter et argumenter vos réponses. Par ailleurs il n'y a pas forcément de « bonne » réponse, ou même de réponse, l'argumentation que vous adosserez à vos commentaires n'en sera que plus importante.

1 On tente ici d'ouvrir une session *FTP*, c'est-à-dire un transfert de fichiers, sur un hôte distant.

```
root@turgescence:~ # ftp amertume
Trying 2001:660:3301:8070::83:21 ...
ftp: Can't connect to '2001:660:3301:8070::83:21': Connection refused
Trying 194.254.199.83:21 ...
ftp: Can't connect to '194.254.199.83:21': Connection refused
ftp: Can't connect to 'amertume:ftp'
ftp> ^D
root@turgescence:~ #
```

Cette tentative échoue, mais ce n'est pas ici l'important, celle-ci n'est là que pour les besoins de l'exercice. Que pouvez vous déduire de cet essai ? Commentez le résultat.

2 On a tracé, à l'aide de l'utilitaire *tcpdump*, l'interface d'où provenait la demande de session *FTP* :

```
root@turgescence:~ # tcpdump -i lagg0 -N -t  port domain
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lagg0, link-type EN10MB (Ethernet), capture size 65535 bytes
IP turgescence.15127 > sweet-smoke.domain:
   63891+ A? amertume.informatique.univ-paris-diderot.fr. (61)
IP sweet-smoke.domain > turgescence.15127:
   63891* 1/3/5 A 194.254.199.83 (266)
IP turgescence.46287 > sweet-smoke.domain:
   63892+ AAAA? amertume.informatique.univ-paris-diderot.fr. (61)
IP sweet-smoke.domain > turgescence.46287:
   63892* 1/3/5 AAAA 2001:660:3301:8070::83 (278)
IP turgescence.40724 > sweet-smoke.domain:
   12552+ PTR? 85.199.254.194.in-addr.arpa. (45)
IP sweet-smoke.domain > turgescence.40724:
   12552* 1/3/5 PTR sweet-smoke.informatique.univ-paris-diderot.fr. (294)
^C
8 packets captured
702 packets received by filter
0 packets dropped by kernel
root@turgescence:~ #
```

Les options *-N* et *-t* sont utilisées pour éliminer une partie de l'affichage et doivent être ignorées ici. Pouvez vous dire à quel service correspond le port 53 ?

La forme de l'affichage obtenu est simple : l'adresse et le port source puis l'adresse et le port de destination, suivis d'une description succincte du contenu de la trame. On ignorera les différents champs purement numériques[1] de la trame, pour se concentrer sur le cœur de celle-ci. En gardant bien à l'esprit qu'il s'agit de la tentative de session *FTP* précédente commentez cette trace. À quoi correspondent les éléments *A*, *AAAA* et *PTR* ?

3 Pour en finir avec les deux point précédents voici le contenu de trois fichiers :

```
root@turgescence:~ # grep amertume /etc/hosts
root@turgescence:~ # grep hosts /etc/nsswitch.conf
hosts: files dns
root@turgescence:~ # cat /etc/resolv.conf
domain informatique.univ-paris-diderot.fr
search informatique.univ-paris-diderot.fr
nameserver 194.254.199.85
root@turgescence:~ #
```

Pourriez-vous dire quels sont les rôles des fichiers */etc/hosts*, */etc/nsswitch.conf* et */etc/resolv.conf* ? Leur contenu vous paraît-il cohérent avec l'affichage obtenu aux deux premières questions ?

4 On a ici un extrait des journaux (*logs*) du routeur d'accès, l'affichage a été un peu élagué afin d'en facilité la compréhension :

```
ramassis# grep 179.184.31.106 /var/adm/syslog/juniper.log | & wc -l
    1515
ramassis# grep 179.184.31.106 /var/adm/syslog/juniper.log | & head -20
Mar 17 09:13:34 SYSLOG: A tcp 179.184.31.106 194.254.199.30 54137 22 (1 packets)
Mar 17 09:13:34 SYSLOG: A tcp 179.184.31.106 194.254.199.27 54137 22 (1 packets)
Mar 17 09:13:34 SYSLOG: D tcp 179.184.31.106 194.254.199.21 54137 22 (1 packets)
Mar 17 09:13:34 SYSLOG: D tcp 179.184.31.106 194.254.199.26 54137 22 (1 packets)
Mar 17 09:13:34 SYSLOG: D tcp 179.184.31.106 194.254.199.72 54137 22 (1 packets)
Mar 17 09:13:34 SYSLOG: D tcp 179.184.31.106 194.254.199.53 54137 22 (1 packets)
Mar 17 09:13:34 SYSLOG: D tcp 179.184.31.106 194.254.199.50 54137 22 (1 packets)
Mar 17 09:13:34 SYSLOG: D tcp 179.184.31.106 194.254.199.96 54137 22 (1 packets)
Mar 17 09:13:35 SYSLOG: D tcp 179.184.31.106 194.254.199.42 54137 22 (1 packets)
Mar 17 09:13:35 SYSLOG: D tcp 179.184.31.106 194.254.199.57 54137 22 (1 packets)
Mar 17 09:13:35 SYSLOG: D tcp 179.184.31.106 194.254.199.92 54137 22 (1 packets)
Mar 17 09:13:35 SYSLOG: D tcp 179.184.31.106 194.254.199.34 54137 22 (1 packets)
Mar 17 09:13:35 SYSLOG: D tcp 179.184.31.106 194.254.199.108 54137 22 (1 packets)
Mar 17 09:13:35 SYSLOG: D tcp 179.184.31.106 194.254.199.25 54137 22 (1 packets)
Mar 17 09:13:35 SYSLOG: D tcp 179.184.31.106 194.254.199.38 54137 22 (1 packets)
Mar 17 09:13:35 SYSLOG: D tcp 179.184.31.106 194.254.199.84 54137 22 (1 packets)
Mar 17 09:13:35 SYSLOG: D tcp 179.184.31.106 194.254.199.80 54137 22 (1 packets)
Mar 17 09:13:35 SYSLOG: D tcp 179.184.31.106 194.254.199.104 54137 22 (1 packets)
Mar 17 09:13:36 SYSLOG: D tcp 179.184.31.106 194.254.199.238 54137 22 (1 packets)
Mar 17 09:13:36 SYSLOG: D tcp 179.184.31.106 194.254.199.76 54137 22 (1 packets)
ramassis# grep 179.184.31.106 /var/adm/syslog/juniper.log | & tail -5
Mar 17 09:38:16 SYSLOG: A tcp 179.184.31.106 194.254.199.27 46052 22 (3 packets)
Mar 17 09:38:16 SYSLOG: A tcp 179.184.31.106 194.254.199.27 46052 22 (1 packets)
Mar 17 09:38:16 SYSLOG: A tcp 179.184.31.106 194.254.199.27 46052 22 (1 packets)
Mar 17 09:38:16 SYSLOG: A tcp 179.184.31.106 194.254.199.27 46052 22 (2 packets)
Mar 17 09:38:16 SYSLOG: A tcp 179.184.31.106 194.254.199.27 46052 22 (1 packets)
ramassis#
```

[1] Par exemple 63891+, 1/3/5, (278)...

L'affichage se lit de la façon suivante : *A* ou *D* indiquent que le paquet à été accepté ou refusé (*Denied*), le protocole (ici *TCP*), viennent ensuite l'adresse source et l'adresse de destination, puis enfin les ports source et destination. Pour mémoire le port 22/tcp est utilisé par le service *ssh*. Le dernier champ est le nombre de paquets, qui nous importe peu ici.

L'utilitaire *grep* recherche une occurrence, tandis que la commande *wc -l* compte le nombre de lignes. Autrement dit l'adresse *179.184.31.106* est apparue 1515 fois dans le journal. Par ailleurs voici à quoi correspond l'adresse en question :

```
ramassis# dig +short -x 179.184.31.106
cedaspy.static.gvt.net.br.
ramassis#
```

Que vous inspire tout ce qui précède ? Que pourriez-vous en tirer comme conclusions *a priori* ? Détaillez vos réflexions.

5 En lien avec la question précédente on dispose d'un extrait choisi des journaux de la machine *ouindose*. Les commandes *head* et *tail* permettent ces extractions et n'ont pas d'importance particulière ici. Sauriez-vous dire de quel journal provient cet affichage ?

```
<ouindose-28-[17:27]>% grep 179.184.31.106 /var/adm/syslog/auth.log \
? | egrep "Invalid|Failed" | head -5
Mar 17 09:34:51 ouindose sshd[7242]: [ID 800047 auth.info] Failed password for
root from 179.184.31.106 port 55972 ssh2
Mar 17 09:34:53 ouindose sshd[7248]: [ID 800047 auth.info] Failed password for
root from 179.184.31.106 port 56856 ssh2
Mar 17 09:34:55 ouindose sshd[7250]: [ID 800047 auth.info] Invalid user db2fenc1
from 179.184.31.106
Mar 17 09:34:56 ouindose sshd[7250]: [ID 800047 auth.info] Failed password for
invalid user db2fenc1 from 179.184.31.106 port 57803 ssh2
Mar 17 09:34:58 ouindose sshd[7252]: [ID 800047 auth.info] Failed password for
oracle from 179.184.31.106 port 58662 ssh2
<ouindose-29-[17:28]>% grep 179.184.31.106 /var/adm/syslog/auth.log \
? | egrep "Invalid|Failed" | tail -5
Mar 17 09:37:40 ouindose sshd[7535]: [ID 800047 auth.info] Failed password for
invalid user iptv from 179.184.31.106 port 43419 ssh2
Mar 17 09:37:42 ouindose sshd[7539]: [ID 800047 auth.info] Failed password for
sshd from 179.184.31.106 port 44351 ssh2
Mar 17 09:37:44 ouindose sshd[7542]: [ID 800047 auth.info] Invalid user ntpd
from 179.184.31.106
Mar 17 09:37:44 ouindose sshd[7542]: [ID 800047 auth.info] Failed password for
invalid user ntpd from 179.184.31.106 port 45131 ssh2
Mar 17 09:37:46 ouindose sshd[7546]: [ID 800047 auth.info] Failed password for
root from 179.184.31.106 port 46052 ssh2
<ouindose-30-[17:28]>%  dig +short -x 194.254.199.27
ouindose.informatique.univ-paris-diderot.fr.
<ouindose-31-[17:29]>%
```

Que s'est-il passé ici selon vous ? Cela vous permet-il de compléter votre réflexion précédente ? Si cela vous paraît intentionné, dans un but bien particulier, quelle en est la méthode suivie d'après vous ?

6 La commande *top* affiche des éléments de configuration du système ainsi que des informations concernant les processus en cours d'exécution. Les différentes options qui sont données ici à *top* (c'est-à-dire *-U jmm*, *-b* et *-n 7*) ne servent simplement qu'à limiter l'affichage. Pourriez-vous donnez quelques précisions sur la configuration ?

```
<gaufre-40-[14:46]>% top -U jmm -b -n 7
load averages:  1.04,  1.04,  0.92;               up 143+05:31:54      14:46:20
428 processes: 426 sleeping, 2 on cpu
CPU states: 95.7% idle,  4.2% user,  0.1% kernel,  0.0% iowait,  0.0% swap
Kernel: 648 ctxsw, 82 trap, 1058 intr, 2397 syscall, 77 flt
Memory: 156G phys mem, 148G free mem, 160G total swap, 160G free swap

   PID USERNAME NLWP PRI NICE  SIZE   RES STATE    TIME    CPU COMMAND
  5756 jmm         1   0    0   75G  732K cpu/18  32:19  4.13% gonflette
  6186 jmm         1  59    0 3804K 2160K cpu/6    0:00  0.02% top
  5669 jmm         1  59    0 3268K 2276K sleep    0:00  0.00% tcsh
  5792 jmm         1  59    0 1756K  736K sleep    0:00  0.00% rikiki
  5805 jmm         1  59    0 1756K  736K sleep    0:00  0.00% rikiki
  5806 jmm         1  59    0 1756K  736K sleep    0:00  0.00% rikiki
  5807 jmm         1  59    0 1756K  736K sleep    0:00  0.00% rikiki

<gaufre-41-[14:46]>%
```

Des processus, aux noms suggestifs (*gonflette* et *rikiki*), sont en cours d'exécution. Pourriez-vous décrire leur impact sur les performances du système ?

7 En rapport avec la question précédente, on trouve ci-dessous le code du programme *rikiki.c*, que vous pouvez commenter :

```
#include <fcntl.h>
main()
{
pause();
}
```

L'affichage ci-après donne le nombre de processus *rikiki*, à savoir 376.

```
<gaufre-43-[15:38]>% ps -eaf |grep rikiki|wc -l
     376
<gaufre-44-[15:39]>%
```

D'après vous quel est l'impact de ces 256 processus sur le système comparé à celui du processus *gonflette* ? S'il y avait 752 ou 900 ? Existe t-il une limite selon vous ?

8 La commande *mkdir* permet de créer un catalogue, mais ce n'est pas l'important ici. Regardez avec beaucoup d'attention l'affichage de commandes qui suit :

```
# whoami
root
# mkdir /var/tmp/essai
# rm -r / var/tmp/essai
```

Que se passera t-il si la commande *rm* est exécutée ? Que pourriez-vous en déduire quant à l'opportunité de travailler en tant qu'utilisateur privilégié ?