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

J-M Moreno

Mardi 23 mars 2010

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, l'argumentation que vous adosserez à vos commentaires n'en sera que plus importante.

1 La commande est une évolution de disponible sous SOLARIS. Ici elle permet d'afficher 10 processus appartenant à l'utilisateur . Que pouvez vous dire sur le processus en particulier et sur le résultat de la commande en général ?

```
<a e    e-115-[16:37]>%     a  -     -  10 -c 1 1
   PID USERNAME  SIZE   RSS STATE  PRI NICE      TIME  CPU PROCESS/NLWP
  2620          3400K 2560K c  4    59    0   0:00:00 0.0%     a /1
 27455          3700K 1916K   ee    49    0   0:00:00 0.0%  c  /1
  2611          2290M  656K   ee    59    0   0:00:00 0.0%  e   /1
  2613          2290M  656K   ee    59    0   0:00:00 0.0%  e   /1
  2570          2290M  656K   ee    59    0   0:00:00 0.0%  e   /1
  2615          2290M  656K   ee    59    0   0:00:00 0.0%  e   /1
  2503          2290M  656K   ee    59    0   0:00:00 0.0%  e   /1
  2502          2290M  656K   ee    59    0   0:00:00 0.0%  e   /1
 26696          3280K 1212K   ee    59    0   0:00:00 0.0%  c  /1
 27445          6420K 2108K   ee    59    0   0:00:00 0.0%    d/1
T  a : 123    ce  e , 123     ,   ad a e age : 0.04, 0.03, 0.02
<a e    e-116-[16:38]>%    -f       g e   e       c -
          119
<a e    e-117-[16:38]>%
```

Sachant que le nombre de processus est de 119, pourriez-vous affiner votre analyse ? Dans ce qui suit on tente de lancer un nouveau processus qui est immédiatement tué. Pourriez-vous dire pourquoi ? Remarquez que est un *fi* et donc est lié au mécanisme de swap et de mémoire virtuelle.

```
<a e    e-149-[17:47]>% df -   /
F  e    e                e     ed  a a   ca ac     M    ed
  a                    2.0G    72K   2.0G     1%    /
<a e    e-150-[17:47]>% ./ e
K   ed
<a e    e-151-[17:48]>%
```

Pourriez-vous donner une estimation grossière de la taille du catalogue ?

2 Le résultat de la commande ci-après provient de la base définissant la zone sur le serveur primaire. Que représentent les différentes entrées ? Sous quel nom sont elles désignées ? Expliquez et commentez leurs contenu.

```
<sweet-smoke-7-[8:30]>% gsed -n -e '/ouindose /,+5p' /var/named/namedb/db.informatique
ouindose        IN      A       194.254.199.27
                IN      AAAA    2001:660:3301:8070::27
                IN      MX      10      korolev.univ-paris7.fr.
                IN      MX      10      potemkin.univ-paris7.fr.
                IN      MX      30      shiva.jussieu.fr.
master2         IN      CNAME   ouindose
<sweet-smoke-8-[8:57]>%
```

En vous basant sur ce résultat que devraient contenir les entrées correspondant à 194.254.199.27 et 2001 :660 :3301 :8070 : :27 dans les bases inverses ?

3 La commande est l'utilitaire de contrôle du démon , l'option demande le rechargement des bases et la relecture du fichier de configuration. Commentez l'extrait de fichier de donné à la suite.

```
ouindose# ssh sweet-smoke /usr/local/sbin/rndc reload
Enter passphrase for key '/.ssh/id_rsa':
server reload successful
ouindose# dig +short A sweet-smoke.informatique.univ-paris-diderot.fr
194.254.199.85
ouindose# dig +short AAAA sweet-smoke.informatique.univ-paris-diderot.fr
2001:660:3301:8070::85
ouindose# dig +short A ouindose.informatique.univ-paris-diderot.fr
194.254.199.27
ouindose# dig +short AAAA ouindose.informatique.univ-paris-diderot.fr
2001:660:3301:8070::27
ouindose# tail -7 /var/adm/syslog/named.log
Mar 18 16:12:54 ouindose named[12730]: [ID 873579 local4.info] 18-Mar-2010 16:12:54.385
 notify: info: client 194.254.199.85#36424: received notify for zone
 '79.168.192.in-addr.arpa'
Mar 18 16:12:54 ouindose named[12730]: [ID 873579 local4.info] 18-Mar-2010 16:12:54.388
 general: info: zone 79.168.192.in-addr.arpa/IN: Transfer started.
Mar 18 16:12:54 ouindose named[12730]: [ID 873579 local4.info] 18-Mar-2010 16:12:54.389
 xfer-in: info: transfer of '79.168.192.in-addr.arpa/IN' from 2001:660:3301:8070::85#53:
 connected using 2001:660:3 301:8070::27#49008
Mar 18 16:12:54 ouindose named[12730]: [ID 873579 local4.info] 18-Mar-2010 16:12:54.425
 general: info: zone 79.168.192.in-addr.arpa/IN: transferred serial 2010031803
Mar 18 16:12:54 ouindose named[12730]: [ID 873579 local4.info] 18-Mar-2010 16:12:54.426
 xfer-in: info: transfer of '79.168.192.in-addr.arpa/IN' from 2001:660:3301:8070::85#53:
 Transfer completed: 78 mes sages, 78 records, 7696 bytes, 0.036 secs (213777 bytes/sec)
Mar 18 16:12:55 ouindose named[12730]: [ID 873579 local4.info] 18-Mar-2010 16:12:55.405
 notify: info: client 2001:660:3301:8070::85#36425: received notify for zone
 '79.168.192.in-addr.arpa'
Mar 18 16:12:55 ouindose named[12730]: [ID 873579 local4.info] 18-Mar-2010 16:12:55.405
 general: info: zone 79.168.192.in-addr.arpa/IN: notify from 2001:660:3301:8070::85#36425:
 zone is up to date
ouindose#
```

Que pouvez vous en déduire sur les rôles respectifs des machines et et de leurs relations ?

4 La virtualisation de machines est devenu un phénomène répandu et, de fait, incontournable.

a) quels sont d'après vous les avantages considérables, s'il y en a, des machines virtuelles ?

b) quels sont d'après vous les inconvénients considérables, s'il y en a, des machines virtuelles ?

c) si vous avez répondu aux 2 questions que pouvez vous en déduire, en dehors de l'inconstance de l'être humain sur laquelle nous sommes bien sûr d'accord ?

5 **Nous avons ci-dessous un extrait de journal de consignation ( ). Connaissez vous les méthodes, protocole et démon, de consignation ? De quel dispositif proviennent, , ces messages ?**

```
ramassis# grep "22 (" /var/adm/syslog/juniper.log|tail
Mar 15 10:34:39 paella.informatique.univ-paris-diderot.fr fwdd[17929]: PFE_FW_SYSLOG_IP: FW:
 ge-0/0/0.0   D  tcp 118.142.9.236 194.254.199.57 60504    22 (1 packets)
Mar 15 10:34:39 paella.informatique.univ-paris-diderot.fr fwdd[17929]: PFE_FW_SYSLOG_IP: FW:
 ge-0/0/0.0   D  tcp 118.142.9.236 194.254.199.50 47493    22 (1 packets)
Mar 15 10:34:39 paella.informatique.univ-paris-diderot.fr fwdd[17929]: PFE_FW_SYSLOG_IP: FW:
 ge-0/0/0.0   D  tcp 118.142.9.236 194.254.199.59 46963    22 (1 packets)
Mar 15 10:34:39 paella.informatique.univ-paris-diderot.fr fwdd[17929]: PFE_FW_SYSLOG_IP: FW:
 ge-0/0/0.0   D  tcp 118.142.9.236 194.254.199.71 42906    22 (1 packets)
Mar 15 10:34:39 paella.informatique.univ-paris-diderot.fr fwdd[17929]: PFE_FW_SYSLOG_IP: FW:
 ge-0/0/0.0   D  tcp 118.142.9.236 194.254.199.72 50314    22 (1 packets)
Mar 15 10:34:39 paella.informatique.univ-paris-diderot.fr fwdd[17929]: PFE_FW_SYSLOG_IP: FW:
 ge-0/0/0.0   D  tcp 118.142.9.236 194.254.199.70 52621    22 (1 packets)
Mar 15 10:34:39 paella.informatique.univ-paris-diderot.fr fwdd[17929]: PFE_FW_SYSLOG_IP: FW:
 ge-0/0/0.0   D  tcp 118.142.9.236 194.254.199.79 37228    22 (1 packets)
Mar 15 10:34:39 paella.informatique.univ-paris-diderot.fr fwdd[17929]: PFE_FW_SYSLOG_IP: FW:
 ge-0/0/0.0   D  tcp 118.142.9.236 194.254.199.78 36473    22 (1 packets)
Mar 15 10:34:39 paella.informatique.univ-paris-diderot.fr fwdd[17929]: PFE_FW_SYSLOG_IP: FW:
 ge-0/0/0.0   D  tcp 118.142.9.236 194.254.199.75 48260    22 (1 packets)
Mar 15 10:34:40 paella.informatique.univ-paris-diderot.fr fwdd[17929]: PFE_FW_SYSLOG_IP: FW:
 ge-0/0/0.0   D  tcp 118.142.9.236 194.254.199.76 60443    22 (1 packets)
ramassis#
```

Sachant que provient de , que la première adresse est celle de la source et la seconde celle de la destination, suivie par les ports sources et destination, commentez le résultat de l'affichage. Éventuellement commentez la commande .

6 **Voici un autre exemple d'extrait de fichier de consignation. Quelles informations pouvez vous en tirer ? Peut on y voir un lien avec l'extrait affiché à la question précédente ?**

```
ramassis# grep error /var/adm/syslog/auth.info.log | tail
Mar 15 11:52:14 garbanzo.informatique.univ-paris-diderot.fr sshd[8785]: [ID 800047
 auth.error] error: Could not get shadow information for NOUSER
Mar 15 11:52:14 nivose.informatique.univ-paris-diderot.fr sshd[9953]: [ID 800047
 auth.error] error: Could not get shadow information for NOUSER
Mar 15 11:52:16 ouindose.informatique.univ-paris-diderot.fr sshd[26225]: [ID 800047
 auth.error] error: Could not get shadow information for NOUSER
Mar 15 11:52:16 garbanzo.informatique.univ-paris-diderot.fr sshd[8787]: [ID 800047
 auth.error] error: Could not get shadow information for NOUSER
Mar 15 11:52:17 nivose.informatique.univ-paris-diderot.fr sshd[9958]: [ID 800047
 auth.error] error: Could not get shadow information for NOUSER
Mar 15 11:52:18 ouindose.informatique.univ-paris-diderot.fr sshd[26227]: [ID 800047
 auth.error] error: Could not get shadow information for NOUSER
Mar 15 11:52:19 garbanzo.informatique.univ-paris-diderot.fr sshd[8789]: [ID 800047
 auth.error] error: Could not get shadow information for NOUSER
Mar 15 11:52:19 nivose.informatique.univ-paris-diderot.fr sshd[9963]: [ID 800047
 auth.error] error: Could not get shadow information for NOUSER
Mar 15 11:52:22 garbanzo.informatique.univ-paris-diderot.fr sshd[8791]: [ID 800047
 auth.error] error: Could not get shadow information for NOUSER
Mar 15 11:52:24 garbanzo.informatique.univ-paris-diderot.fr sshd[8793]: [ID 800047
 auth.error] error: Could not get shadow information for NOUSER
ramassis#
```

Que pouvez vous dire du rôle dévolu à la machine ?

7 L'utilitaire permet de capturer et de tracer le trafic du réseau. Il est similaire à et mais spécifique à SOLARIS. Nous l'utilisons ici pour tracer la session suivante entre deux machines :

```
<soft-machine-12-[14:24]>% ftp lapin
Connected to lapin.
220 lapin FTP server (Revision 4.0 Version wuftpd-2.6.1 Wed Jun 18 07:11:14 GMT 2008) ready.
Name (lapin:jmm): marcel
331 Password required for marcel.
Password:
230 User marcel logged in.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/var/tmp" is current directory.
ftp> 221-You have transferred 0 bytes in 0 files.
221-Total traffic for this session was 318 bytes in 0 transfers.
221-Thank you for using the FTP service on lapin.
221 Goodbye.
<soft-machine-13-[14:32]>%
```

Il s'agit ici simplement de la connexion, à partir de la machine , de l'utilisateur sur la machine . On ne s'intéresse pas ici directement au protocole mais plutôt au contenu de la session. Que remarquez vous ? Qu'en déduisez vous ? Que préconisez vous ?

```
soft-machine # snoop port ftp
Using device /dev/e1000g0 (promiscuous mode)
soft-machine -> lapin        FTP C port=34860
       lapin -> soft-machine FTP R port=34860
soft-machine -> lapin        FTP C port=34860
       lapin -> soft-machine FTP R port=34860 220 lapin FTP server
soft-machine -> lapin        FTP C port=34860
soft-machine -> lapin        FTP C port=34860 USER marcel\r\n
       lapin -> soft-machine FTP R port=34860 331 Password require
soft-machine -> lapin        FTP C port=34860
soft-machine -> lapin        FTP C port=34860 PASS caramba\r\n
       lapin -> soft-machine FTP R port=34860 230 User marcel logg
soft-machine -> lapin        FTP C port=34860 SYST\r\n
       lapin -> soft-machine FTP R port=34860 215 UNIX Type: L8\r\n
soft-machine -> lapin        FTP C port=34860 TYPE I\r\n
       lapin -> soft-machine FTP R port=34860 200 Type set to I.\r\n
soft-machine -> lapin        FTP C port=34860
soft-machine -> lapin        FTP C port=34860 PWD\r\n
       lapin -> soft-machine FTP R port=34860 257 "/var/tmp" is cu
soft-machine -> lapin        FTP C port=34860
soft-machine -> lapin        FTP C port=34860 QUIT\r\n
       lapin -> soft-machine FTP R port=34860 221-You have transfe
soft-machine -> lapin        FTP C port=34860
       lapin -> soft-machine FTP R port=34860 221-Total traffic fo
soft-machine -> lapin        FTP C port=34860
soft-machine -> lapin        FTP C port=34860
       lapin -> soft-machine FTP R port=34860
^Csoft-machine #
```

Les protocoles et posent des problèmes similaires. Donnez deux raisons qui militent pour l'utilisation de . Pensez vous que celui-ci soit sensible à des attaques de force brute ? Y a-t-il des exemples d'attaque de ce type dans les différents exemples qui sont donnés à travers l'ensemble de ce sujet ? Dans ce cas donnez le ou les numéros des questions où figurent ces exemples.