Dernière mise-à-jour : 2020/01/30 03:27

Gestion de la Sécurité - #3

Autres Risques

Spamming

Le **Spamming** consiste en soit :

- envoyer des messages électroniques indésirables, souvent à des milliers de contacts en utilisant une adresse email *usurpée* de la cible
    - dans ce cas, les retours éventuels des systèmes anti-spam installés sur les serveurs distants peuvent créer un ralentissement important au niveau du MTA de la cible,
- envoyer des milliers de messages vers une boîte au lettre du serveur email de la cible de façon à remplir celle-ci à 100% de sa capacité.

Contre-Mesures

L'utilisation d'un mandataire.

Nuke

Le **Nuke** est une attaque où l'attaquant connait l'adresse IP de sa cible et un **exploit** du système d'exploitation. Ce type d'attaque plante la cible.

Contre-Mesures

Mises à jour de sécurité.

Virus

Les **Virus** sont des codes malicieux. Les virus ne peuvent pas être détectées au niveau IP, mais sont détectables au niveau *application* de part leur signature. Il existe plusieurs types de virus :

Virus de Boot

Un virus de boot s'installe dans un des secteurs de boot d'un périphérique de démarrage. Il a pour seul but de se propager.

Vers

Un ver est un binaire capable de se reproduire sans action externe de la part d'un utilisateur ou de la cible. Son objectif est de :

- créer une liste de cibles possibles,
- trouver les mots de passe des comptes de la cible actuelle,
- rentrer dans les cibles identifiées en se passant pour un utilisateur de la cible actuelle en utilisant une faille dans le protocole *finger*.

Bombes Logiques

Une **Bombe Logique** est action programmée pour déclencher une commande ou un appel système en fonction de la date et heure du système.

Trappes

Une **Trappe** est une porte arrière par laquelle passe l'attaquant afin d'utiliser la cible à des fins néfastes en attaquant d'autre cibles.

Macro-virus

Ce sont des virus écrits dans un langage spécifique à une application comme par exemple Microsoft™ Word.

Contre-Mesures

La mise en place d'un Anti-Virus.

Root Kits

Présentation

Un **rootkit** est un paquet logiciel qui permet à un utilisateur non-autorisé d'obtenir les droits de **root**.

Les rootkits sont essentiellement de deux types, voire un mélange des deux :

- des modules du noyau,
- des paquets logiciels d'un utilisateur qui prennent la place de binaires système.

Les rootkits de type modules du noyau insèrent des modules qui remplacent des appels systèmes et cachent des informations concernant certains processus spécifiques.

Les rootkits de type paquets logiciels remplacement en règle générale des binaires système tels **ps**, **login** etc. Les binaires de remplacement cachent des processus et des répertoires de l'attaquant.

Contre-Mesures

La mise en place de logiciels de vérification.

LAB #19 - Mise en place de Chkrootkit

Importez une machine virtuelle vierge de CentOS 6 pour effectuer les LABS #19 et #20.

Installation

Installez le paquet avec yum :

```
[root@centos6 ~]# yum install chkrootkit
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.in2p3.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package chkrootkit.i686 0:0.49-1.el6.rf set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                                 Arch                                 Version
Repository                              Size
================================================================================
================================================================================
Installing:
```

```
 chkrootkit                                i686                                0.49-1.el6.rf
rpmforge                                 286 k

Transaction Summary
================================================================================
================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 286 k
Installed size: 656 k
Is this ok [y/N]: y
Downloading Packages:
chkrootkit-0.49-1.el6.rf.i686.rpm
| 286 kB     00:00
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : chkrootkit-0.49-1.el6.rf.i686
1/1

Installed:
  chkrootkit.i686 0:0.49-1.el6.rf

Complete!
```

Options de la commande

Les options de cette commande sont :

```
[root@centos6 ~]# chkrootkit --help
Usage: /usr/lib/chkrootkit-0.49/chkrootkit [options] [test ...]
```

```
Options:
        -h               show this help and exit
        -V               show version information and exit
        -l               show available tests and exit
        -d               debug
        -q               quiet mode
        -x               expert mode
        -r dir           use dir as the root directory
        -p dir1:dir2:dirN path for the external commands used by chkrootkit
        -n               skip NFS mounted dirs
```

Utilisation

Lancez **chkrootkit** simplement en appelant son exécutable :

```
[root@centos6 ~]# chkrootkit
ROOTDIR is `/'
Checking `amd'... not found
Checking `basename'... not infected
Checking `biff'... not found
Checking `chfn'... not infected
Checking `chsh'... not infected
Checking `cron'... not infected
Checking `crontab'... not infected
Checking `date'... not infected
Checking `du'... not infected
Checking `dirname'... not infected
Checking `echo'... not infected
Checking `egrep'... not infected
Checking `env'... not infected
Checking `find'... not infected
Checking `fingerd'... not found
Checking `gpm'... not found
```

```
Checking `grep'... not infected
Checking `hdparm'... not infected
Checking `su'... not infected
Checking `ifconfig'... not infected
Checking `inetd'... not found
Checking `inetdconf'... not found
Checking `identd'... not found
Checking `init'... not infected
Checking `killall'... not infected
Checking `ldsopreload'... not infected
Checking `login'... not infected
Checking `ls'... not infected
Checking `lsof'... not infected
Checking `mail'... not infected
Checking `mingetty'... not infected
Checking `netstat'... not infected
Checking `named'... not infected
Checking `passwd'... not infected
Checking `pidof'... not infected
Checking `pop2'... not found
Checking `pop3'... not found
Checking `ps'... not infected
Checking `pstree'... not infected
Checking `rpcinfo'... not infected
Checking `rlogind'... not found
Checking `rshd'... not found
Checking `slogin'... not infected
Checking `sendmail'... not infected
Checking `sshd'... not infected
Checking `syslogd'... not tested
Checking `tar'... not infected
Checking `tcpd'... not infected
Checking `tcpdump'... not infected
Checking `top'... not infected
```

```
Checking `telnetd'... not found
Checking `timed'... not found
Checking `traceroute'... not infected
Checking `vdir'... not infected
Checking `w'... not infected
Checking `write'... not infected
Checking `aliens'... no suspect files
Searching for sniffer's logs, it may take a while... nothing found
Searching for HiDrootkit's default dir... nothing found
Searching for t0rn's default files and dirs... nothing found
Searching for t0rn's v8 defaults... nothing found
Searching for Lion Worm default files and dirs... nothing found
Searching for RSHA's default files and dir... nothing found
Searching for RH-Sharpe's default files... nothing found
Searching for Ambient's rootkit (ark) default files and dirs... nothing found
Searching for suspicious files and dirs, it may take a while...
/usr/lib/.libssl.so.0.9.8e.hmac /usr/lib/.libssl.so.1.0.0.hmac /usr/lib/.libssl.so.10.hmac
/usr/lib/.libfipscheck.so.1.1.0.hmac /usr/lib/.libcrypto.so.1.0.0.hmac /usr/lib/.libssl.so.6.hmac
/usr/lib/.libcrypto.so.0.9.8e.hmac /usr/lib/.libfipscheck.so.1.hmac /usr/lib/.libcrypto.so.10.hmac
/usr/lib/firefox-3.6/.autoreg /usr/lib/.libcrypto.so.6.hmac /lib/.libgcrypt.so.11.hmac

Searching for LPD Worm files and dirs... nothing found
Searching for Ramen Worm files and dirs... nothing found
Searching for Maniac files and dirs... nothing found
Searching for RK17 files and dirs... nothing found
Searching for Ducoci rootkit... nothing found
Searching for Adore Worm... nothing found
Searching for ShitC Worm... nothing found
Searching for Omega Worm... nothing found
Searching for Sadmind/IIS Worm... nothing found
Searching for MonKit... nothing found
Searching for Showtee... nothing found
Searching for OpticKit... nothing found
Searching for T.R.K... nothing found
```

```
Searching for Mithra... nothing found
Searching for LOC rootkit... nothing found
Searching for Romanian rootkit... nothing found
Searching for HKRK rootkit... nothing found
Searching for Suckit rootkit... nothing found
Searching for Volc rootkit... nothing found
Searching for Gold2 rootkit... nothing found
Searching for TC2 Worm default files and dirs... nothing found
Searching for Anonoying rootkit default files and dirs... nothing found
Searching for ZK rootkit default files and dirs... nothing found
Searching for ShKit rootkit default files and dirs... nothing found
Searching for AjaKit rootkit default files and dirs... nothing found
Searching for zaRwT rootkit default files and dirs... nothing found
Searching for Madalin rootkit default files... nothing found
Searching for Fu rootkit default files... nothing found
Searching for ESRK rootkit default files... nothing found
Searching for rootedoor... nothing found
Searching for ENYELKM rootkit default files... nothing found
Searching for common ssh-scanners default files... nothing found
Searching for suspect PHP files... nothing found
Searching for anomalies in shell history files... nothing found
Checking `asp'... not infected
Checking `bindshell'... not infected
Checking `lkm'... chkproc: nothing detected
chkdirs: nothing detected
Checking `rexedcs'... not found
Checking `sniffer'... eth0: PF_PACKET(/usr/sbin/dhcpd, /usr/sbin/snort-plain)
eth0:0: PF_PACKET(/usr/sbin/dhcpd, /usr/sbin/snort-plain)
Checking `w55808'... not infected
Checking `wted'... chkwtmp: nothing deleted
Checking `scalper'... not infected
Checking `slapper'... not infected
Checking `z2'... chklastlog: nothing deleted
Checking `chkutmp'... chkutmp: nothing deleted
```

```
Checking `OSX_RSPLUG'... not infected
```

chkrootkit peut être lancé en mode expert grâce à l'option **-x**. En mode expert, chkrootkit devient très bavard. Cependant, ce mode est utile pour identifier les détails concernant un problème éventuellement décellé, lors du test précédent.

Automatiser chkrootkit

Il convient maintenant d'automatiser cette vérification en utilisant cron. Editez donc le crontab de root ainsi :

```
0 3 * * * /usr/sbin/chkrootkit 2>&1 | mail -s "chkrootkit \ output" root
```

Cette ligne indique à cron d'exécuter chkrootkit tous les jours à 03h00 du matin et d'envoyer un email à root.

LAB #20 - Mise en place de rkhunter

rkhunter est un autre logiciel utilisé pour détecter les rootkits présents sur votre machine. En règle générale il est conseillé d'utiliser rkhunter **et** chkrootkit pour confirmer une alerte réelle et sérieuse ou bien pour détecter une fausse-alerte par un des deux logiciels.

Installation

L'installation de rkhunter se fait simplement en utilisant yum :

```
[root@centos6 ~]# yum install rkhunter
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
 * base: mirror.in2p3.fr
 * extras: mirror.in2p3.fr
```

```
 * rpmforge: fr2.rpmfind.net
 * updates: mirror.in2p3.fr
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package rkhunter.noarch 0:1.4.0-1.el6.rf set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                                 Arch                                 Version
Repository                               Size
================================================================================
================================================================================
Installing:
 rkhunter                                noarch                               1.4.0-1.el6.rf
rpmforge                                158 k

Transaction Summary
================================================================================
================================================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 158 k
Installed size: 688 k
Is this ok [y/N]: y
Downloading Packages:
rkhunter-1.4.0-1.el6.rf.noarch.rpm
| 158 kB     00:00
Running rpm_check_debug
Running Transaction Test
```

```
Transaction Test Succeeded
Running Transaction
  Installing     : rkhunter-1.4.0-1.el6.rf.noarch
1/1

Installed:
  rkhunter.noarch 0:1.4.0-1.el6.rf

Complete!
```

Les options de la commande

Les options de cette commande sont :

```
[root@centos6 ~]# rkhunter --help

Usage: rkhunter {--check | --unlock | --update | --versioncheck |
                 --propupd [{filename | directory | package name},...] |
                 --list [{tests | {lang | languages} | rootkits | perl | propfiles}] |
                 --config-check | --version | --help} [options]

Current options are:
         --append-log                 Append to the logfile, do not overwrite
         --bindir <directory>...      Use the specified command directories
     -c, --check                      Check the local system
     -C, --config-check               Check the configuration file(s), then exit
  --cs2, --color-set2                 Use the second color set for output
         --configfile <file>          Use the specified configuration file
         --cronjob                    Run as a cron job
                                      (implies -c, --sk and --nocolors options)
         --dbdir <directory>          Use the specified database directory
         --debug                      Debug mode
                                      (Do not use unless asked to do so)
```

```
         --disable <test>[,<test>...]  Disable specific tests
                                       (Default is to disable no tests)
         --display-logfile             Display the logfile at the end
         --enable  <test>[,<test>...]  Enable specific tests
                                       (Default is to enable all tests)
         --hash {MD5 | SHA1 | SHA224 | SHA256 | SHA384 | SHA512 |
                NONE | <command>}     Use the specified file hash function
                                       (Default is SHA1, then MD5)
     -h, --help                        Display this help menu, then exit
 --lang, --language <language>         Specify the language to use
                                       (Default is English)
         --list [tests | languages |   List the available test names, languages,
                rootkits | perl |      rootkit names, perl module status
                propfiles]             or file properties database, then exit
     -l, --logfile [file]              Write to a logfile
                                       (Default is /var/log/rkhunter.log)
         --noappend-log                Do not append to the logfile, overwrite it
         --nocf                        Do not use the configuration file entries
                                       for disabled tests (only valid with --disable)
         --nocolors                    Use black and white output
         --nolog                       Do not write to a logfile
--nomow, --no-mail-on-warning          Do not send a message if warnings occur
   --ns, --nosummary                   Do not show the summary of check results
 --novl, --no-verbose-logging          No verbose logging
         --pkgmgr {RPM | DPKG | BSD |  Use the specified package manager to obtain or
                  SOLARIS | NONE}      verify file property values. (Default is NONE)
         --propupd [file | directory | Update the entire file properties database,
                   package]...         or just for the specified entries
     -q, --quiet                       Quiet mode (no output at all)
  --rwo, --report-warnings-only        Show only warning messages
   --sk, --skip-keypress               Don't wait for a keypress after each test
         --summary                     Show the summary of system check results
                                       (This is the default)
         --syslog [facility.priority]  Log the check start and finish times to syslog
```

```
                                    (Default level is authpriv.notice)
        --tmpdir <directory>        Use the specified temporary directory
        --unlock                    Unlock (remove) the lock file
        --update                    Check for updates to database files
   --vl, --verbose-logging          Use verbose logging (on by default)
     -V, --version                  Display the version number, then exit
         --versioncheck             Check for latest version of program
     -x, --autox                    Automatically detect if X is in use
     -X, --no-autox                 Do not automatically detect if X is in use
```

Utilisation

Lancez **rkhunter** simplement en appelant son exécutable. A l'issu de son exécution, vous observerez un résumé :

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

File properties checks...
    Required commands check failed
    Files checked: 138
    Suspect files: 4

Rootkit checks...
    Rootkits checked : 312
    Possible rootkits: 0

Applications checks...
    Applications checked: 5
    Suspect applications: 2

The system checks took: 4 minutes and 31 seconds
```

```
All results have been written to the log file (/var/log/rkhunter.log)

One or more warnings have been found while checking the system.
Please check the log file (/var/log/rkhunter.log)
```

Notez les fausses alertes ! D'où la necessité d'utiliser à la fois rkhunter **et** chkrootkit.

Configuration

rkhunter peut être configuré soit par des options sur la ligne de commande soit par l'édition de son fichier de configuration **/etc/rkhunter.conf**.

Sécurité Applicative

LAB #21 - Mise en place d'Openvas

Importez une machine virtuelle vierge de CentOS 6 pour effectuer les LABs #21 et #22.

Mise en place de SELinux pour sécuriser le serveur

Présentation

Openvas est le successeur libre du scanner **Nessus**, devenu propriétaire. Openvas, tout comme Nessus, est un scanner de vulnérabilité qui balaie un hôte ou une plage d'hôtes pour essayer de détecter des failles de sécurité. Openvas est une application **client-serveur**:

- **openvas-server**
  - le serveur
- **openvas-client**
  - le client graphique

Installation

Installez **openvas-scanner**, **openvas-client**, **openvas-manager**, **openvas-administrator**, **greenbone-security-assistant**, **openvas-cli** en utilisant yum :

```
[root@centos6 ~]# yum install openvas-scanner openvas-client openvas-manager openvas-administrator greenbone-security-assistant openvas-cli
```

Configuration

Les commandes d'Openvas sont les suivantes :

```
[root@centos6 ~]# ls -l /usr/sbin/openvas*
-rwxr-xr-x. 1 root root   75720 24 avril 18:22 /usr/sbin/openvasad
-rwxr-xr-x. 1 root root    7216 10 mai   18:45 /usr/sbin/openvas-adduser
-rwxr-xr-x. 1 root root 1329704 10 mai   18:54 /usr/sbin/openvasmd
-rwxr-xr-x. 1 root root   11993 10 mai   18:45 /usr/sbin/openvas-mkcert
-rwxr-xr-x. 1 root root   13014 10 mai   18:45 /usr/sbin/openvas-mkcert-client
-rwxr-xr-x. 1 root root    8955 10 mai   18:45 /usr/sbin/openvas-nvt-sync
-rwxr-xr-x. 1 root root     839 11 mai    2011 /usr/sbin/openvas-nvt-sync-cron
-rwxr-xr-x. 1 root root    1982 10 mai   18:45 /usr/sbin/openvas-rmuser
-rwxr-xr-x. 1 root root    7699 10 mai   18:54 /usr/sbin/openvas-scapdata-sync
-rwxr-xr-x. 1 root root  124652 10 mai   18:45 /usr/sbin/openvassd
```

- **/usr/sbin/openvas-adduser**,
  - Cette commande permet d'ajouter un utilisateur à Openvas. L'utilisateur n'a pas besoin d'être le même que le compte Linux,
- **/usr/sbin/openvas-mkcert**,

    - Cette commande permet de générer un certificat SSL,
- **/usr/sbin/openvas-nvt-sync**,
    - Cette commande permet la mise à jour des modules d'extensions de Openvas,
- **/usr/sbin/openvas-rmuser**
    - Cette commande permet de supprimer un utilisateur Openvas,
- **/usr/sbin/openvasd**,
    - Cette commande lance le serveur Openvas.

Premièrement, créez un certificat SSL :

```
[root@centos6 ~]# /usr/sbin/openvas-mkcert -f

-------------------------------------------------------------------------------
            Creation of the OpenVAS SSL Certificate
-------------------------------------------------------------------------------

This script will now ask you the relevant information to create the SSL certificate of OpenVAS.
Note that this information will *NOT* be sent to anybody (everything stays local), but anyone with the ability to
connect to your OpenVAS daemon will be able to retrieve this information.


CA certificate life time in days [1460]:
Server certificate life time in days [365]:
Your country (two letter code) [DE]: FR
Your state or province name [none]: VAR
Your location (e.g. town) [Berlin]: Toulon
Your organization [OpenVAS Users United]: FenestrOS

-------------------------------------------------------------------------------
            Creation of the OpenVAS SSL Certificate
-------------------------------------------------------------------------------

Congratulations. Your server certificate was properly created.
```

```
The following files were created:

. Certification authority:
   Certificate = /var/lib/openvas/CA/cacert.pem
   Private key = /var/lib/openvas/private/CA/cakey.pem

. OpenVAS Server :
    Certificate = /var/lib/openvas/CA/servercert.pem
    Private key = /var/lib/openvas/private/CA/serverkey.pem

Press [ENTER] to exit

[Entrée]
```

Ensuite mettez à jour les modules d'extensions de Openvas :

```
[root@centos6 ~]# /usr/sbin/openvas-nvt-sync
```

Les modules d'extensions se trouvent dans le répertoire **/var/lib/openvas/plugins**.

Dernièrement, ajoutez un utilisateur:

```
[root@redhat ~]# openvas-adduser
Using /var/tmp as a temporary file holder.

Add a new openvassd user
--------------------------------


Login : trainee
Authentication (pass/cert) [pass] :
Login password : trainee
Login password (again) : trainee
```

```
User rules
---------------
openvasd has a rules system which allows you to restrict the hosts that fenestros has the right to test.
For instance, you may want him to be able to scan his own host only.

Please see the openvas-adduser(8) man page for the rules syntax.

Enter the rules for this user, and hit ctrl-D once you are done:
(the user can have an empty rules set)
<key>C</key><key>d</key>

Login             : trainee
Password          : ***********

Rules             :


Is that ok? (y/n) [y] y
user added.
```

Dans notre cas, nous souhaitons que notre utilisateur puisse scanner tous les hôtes. Pour cette raison, nous ne mettons pas de règles. La syntaxe des règles se trouve dans le manuel de openvas-adduser.

Ajoutez maintenant l'administrateur de **openvas-administrator** *openvas* en indiquant le mot de passe *fenestros* :

```
[root@centos6 ~]# openvasad -c 'add_user' -n openvas -r Admin
Enter password: fenestros
ad   main:MESSAGE:26337:2012-06-02 16h41.36 CEST: No rules file provided, the new user will have no restrictions.
ad   main:MESSAGE:26337:2012-06-02 16h41.36 CEST: User openvas has been successfully created.
```

Lancez maintenant le service **openvas-scanner** :

```
[root@centos6 ~]# service openvas-scanner start
```

```
All plugins loaded
```

Lancez maintenant le service **openvas-manager** :

```
[root@centos6 ~]# service openvas-manager start
All plugins loaded
```

Lancez maintenant le service **openvas-administrator** :

```
[root@centos6 ~]# service openvas-administrator start
All plugins loaded
```

Lancez maintenant le service **gsad** (Greenbone Security Assistant) :

```
[root@centos6 ~]# service gsad start
All plugins loaded
```

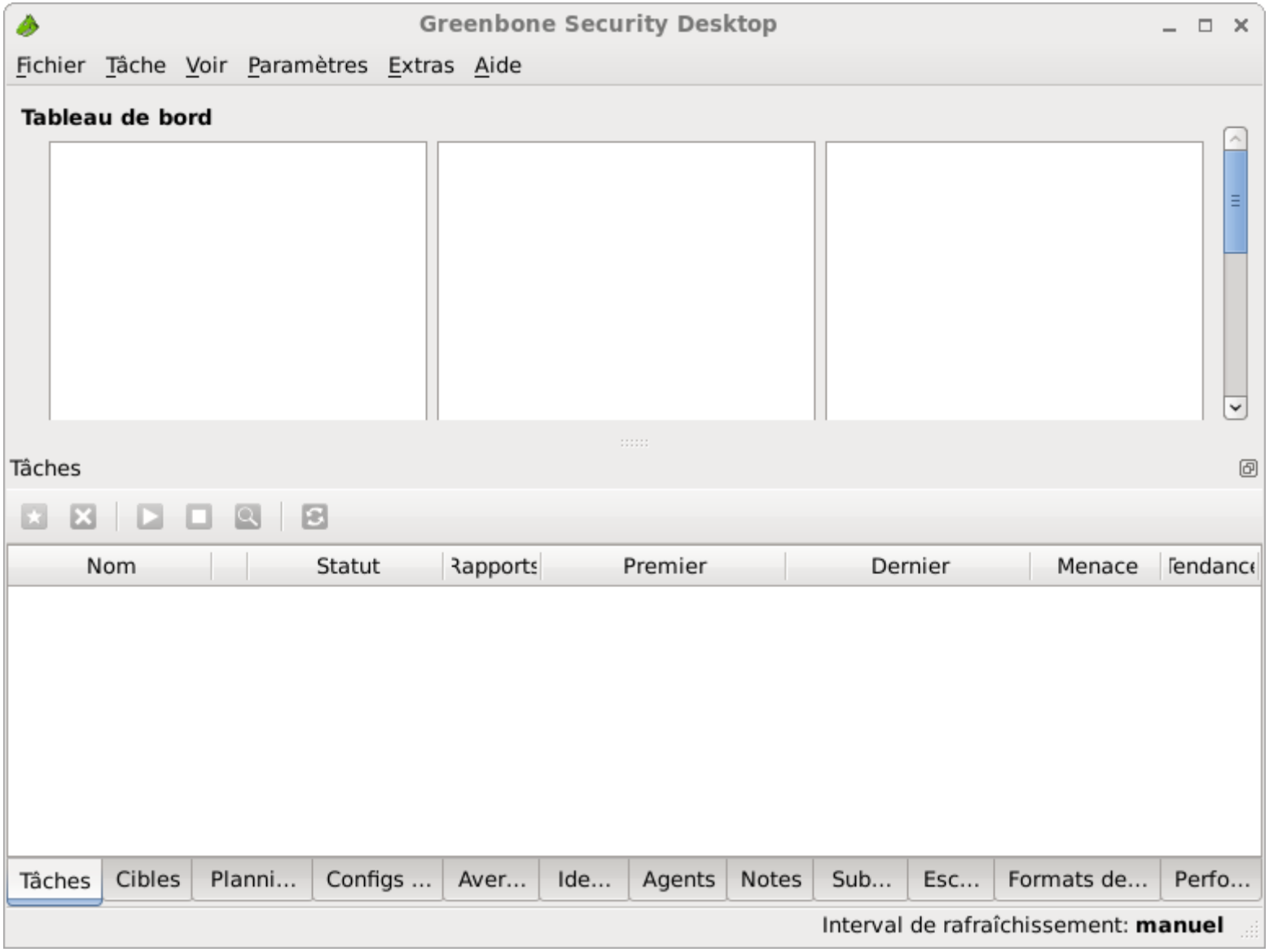
En cas de problèmes (par exemple les services ne démarrent pas), téléchargez le script **openvas-check-setup**, rendez-le exécutable et exécutez-le. Ce script vous informera des erreurs éventuelles liées à votre installation d'Openvas ainsi que les remèdes nécessaires.

Utilisation

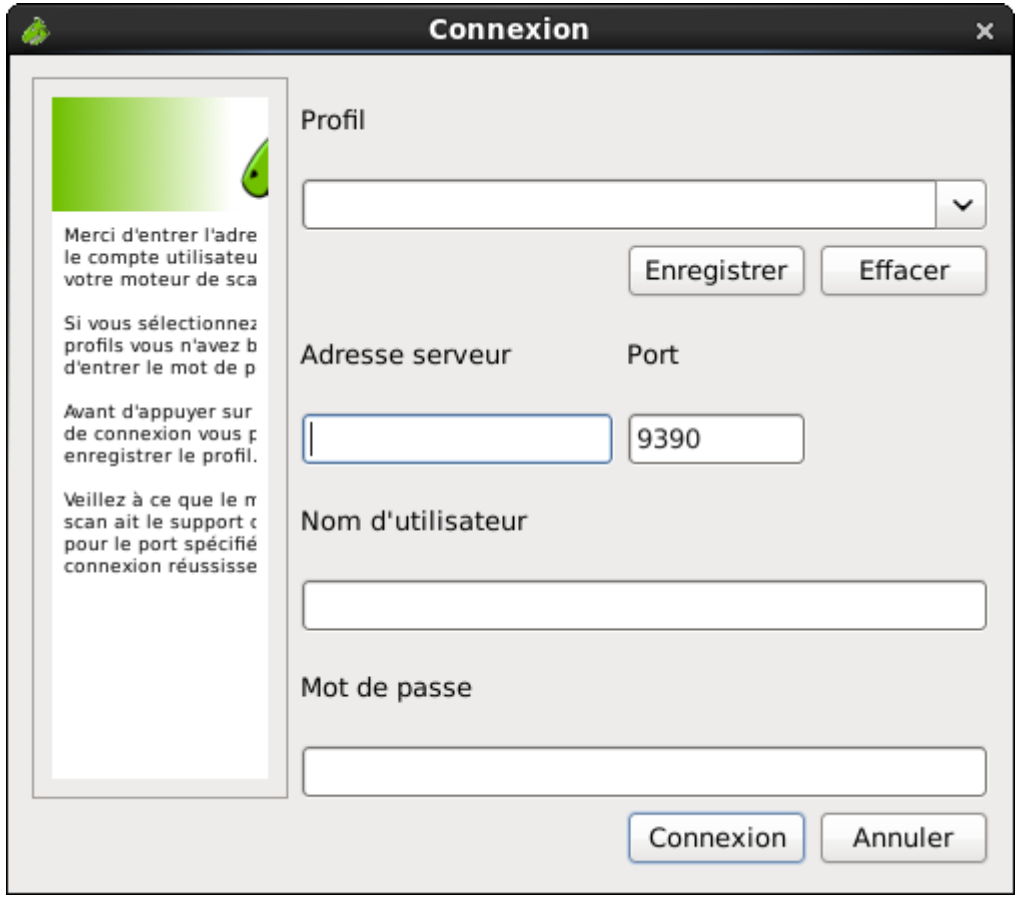
Lancez le client openvas en tant que **trainee** :

```
[trainee@centos6 ~]$ gsd &
[1] 26420
```

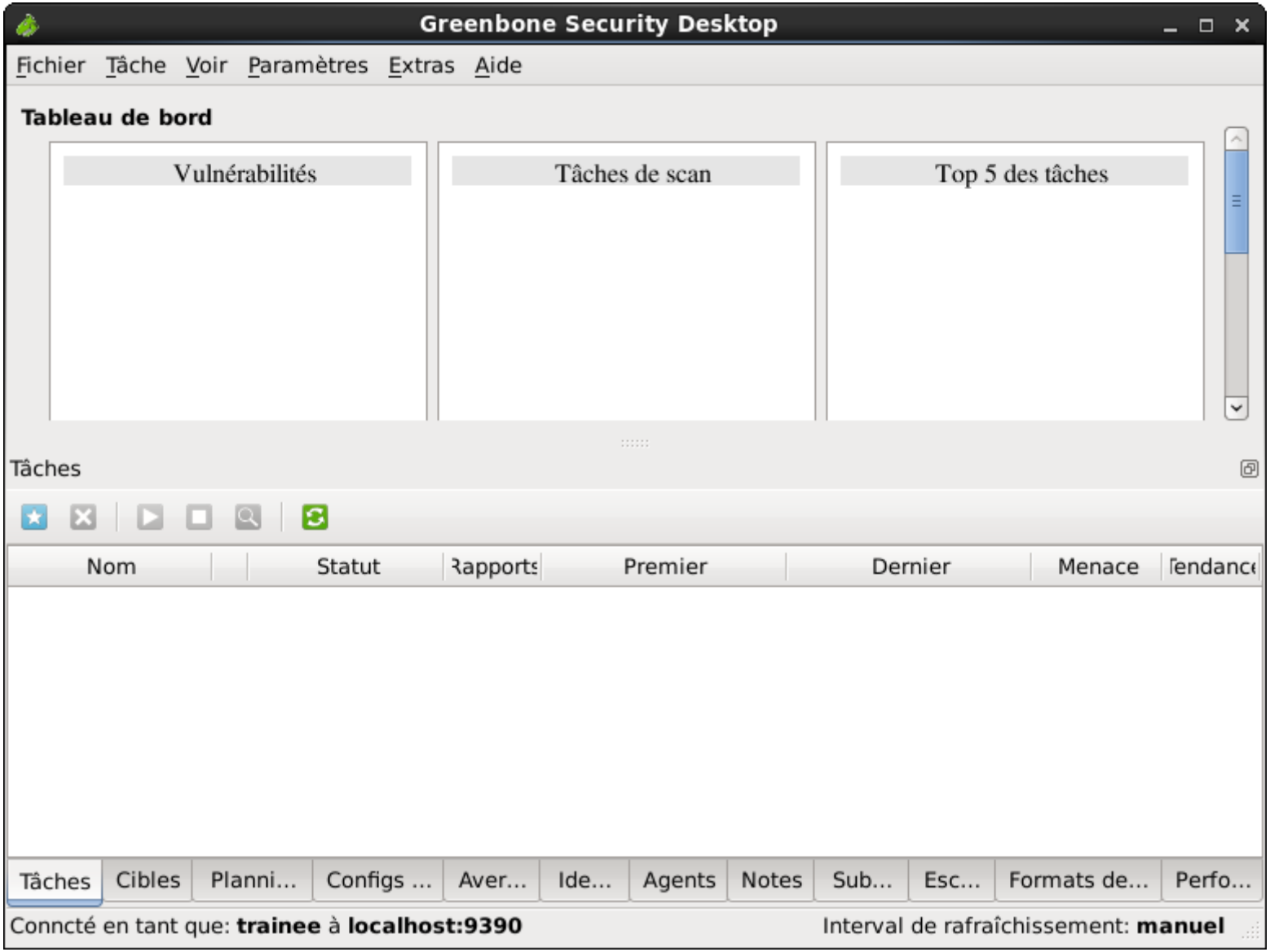
Vous obtiendrez une fenêtre similaire à celle-ci:



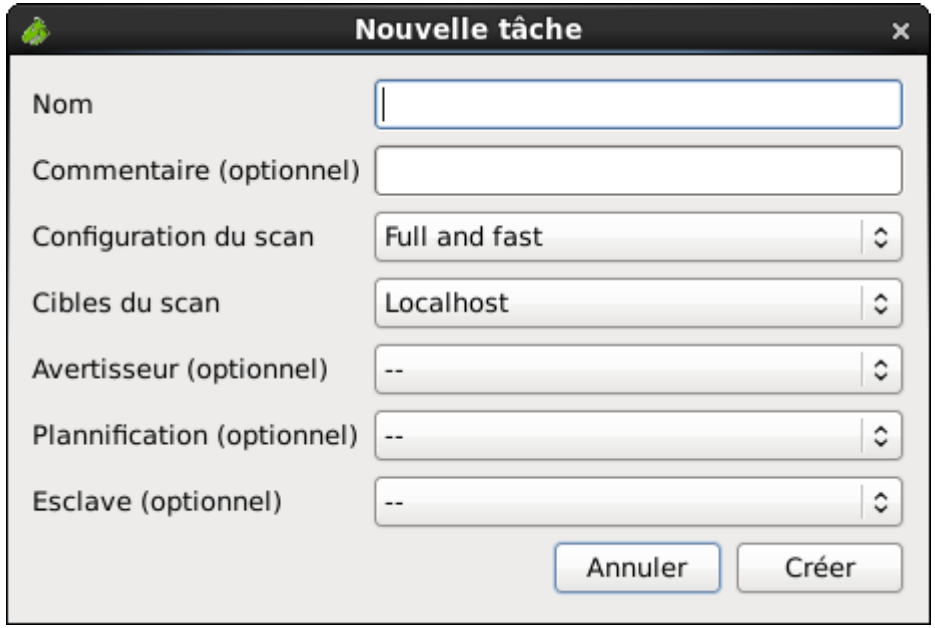
Cliquez sur l'icône **Connecter**, vous obtiendrez une fenêtre similaire à celle-ci:



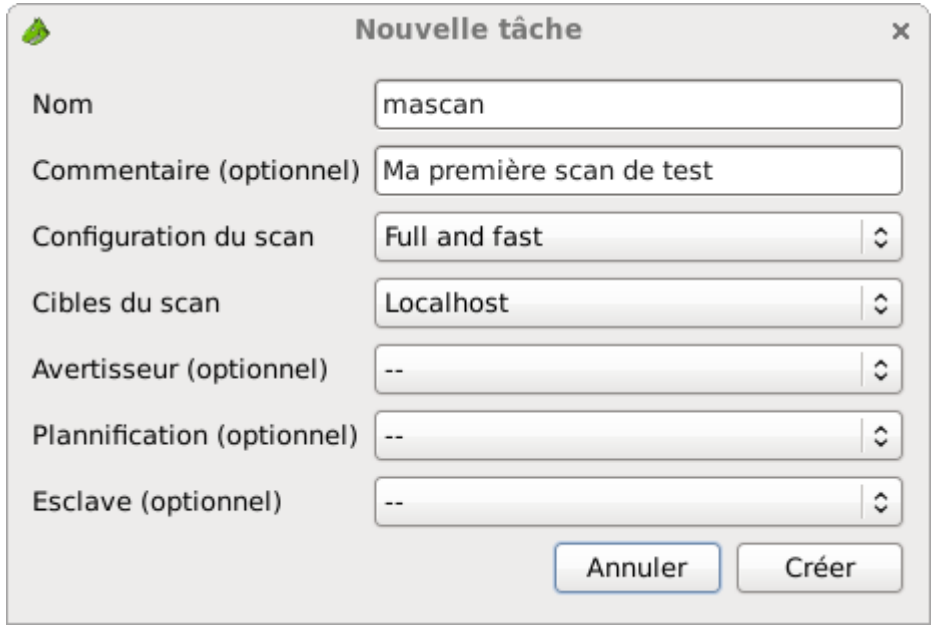
Entrez le nom du serveur **localhost**, le nom de l'utilisateur openvas créé précédemment ainsi que son mot de passe et cliquer sur le bouton **Connexion**. Vous obtiendrez une fenêtre similaire à celle-ci:



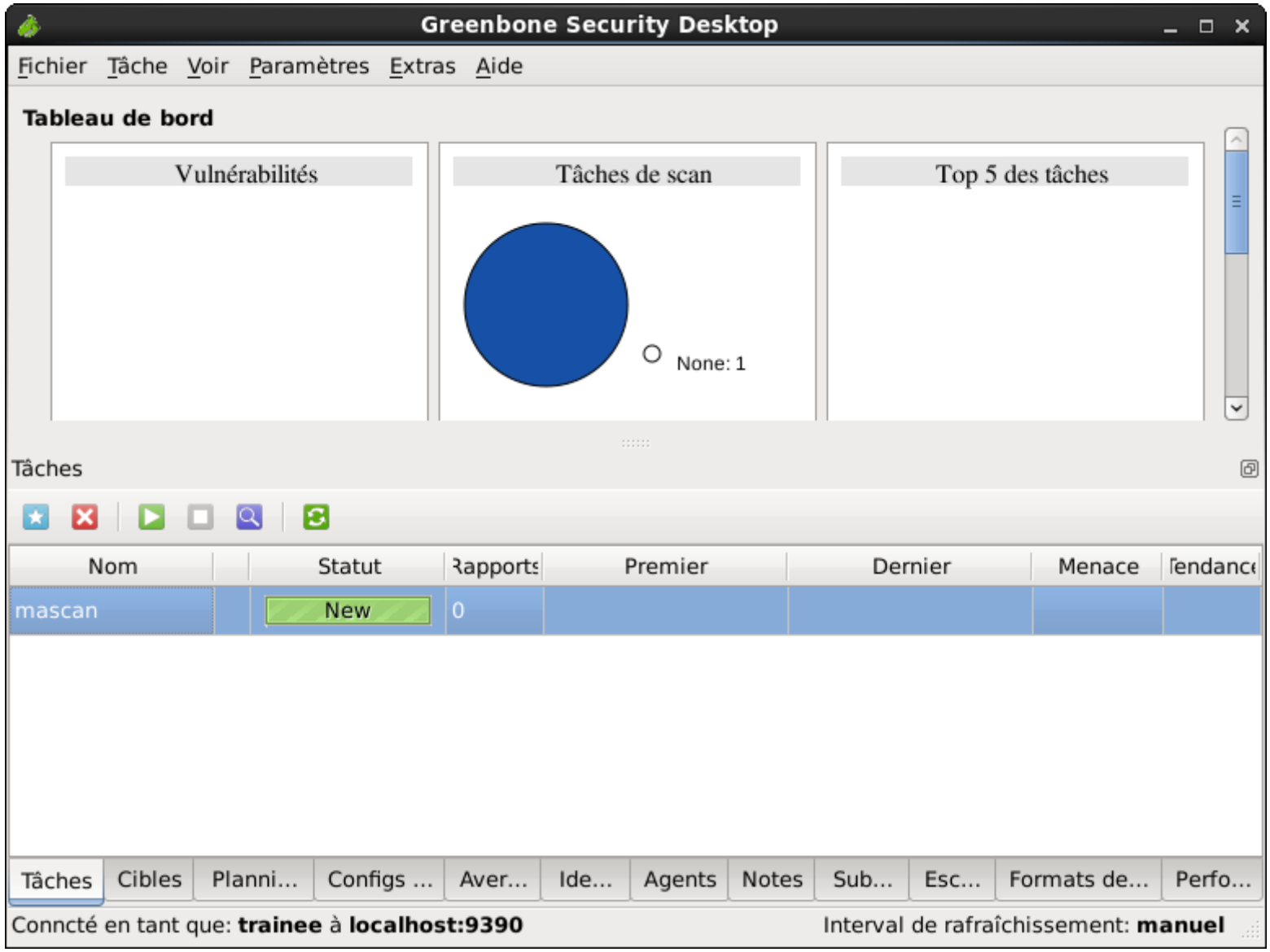
Cliquez maintenant sur **Tâche > Nouveau**. Vous obtiendrez une fenêtre similaire à celle-ci :



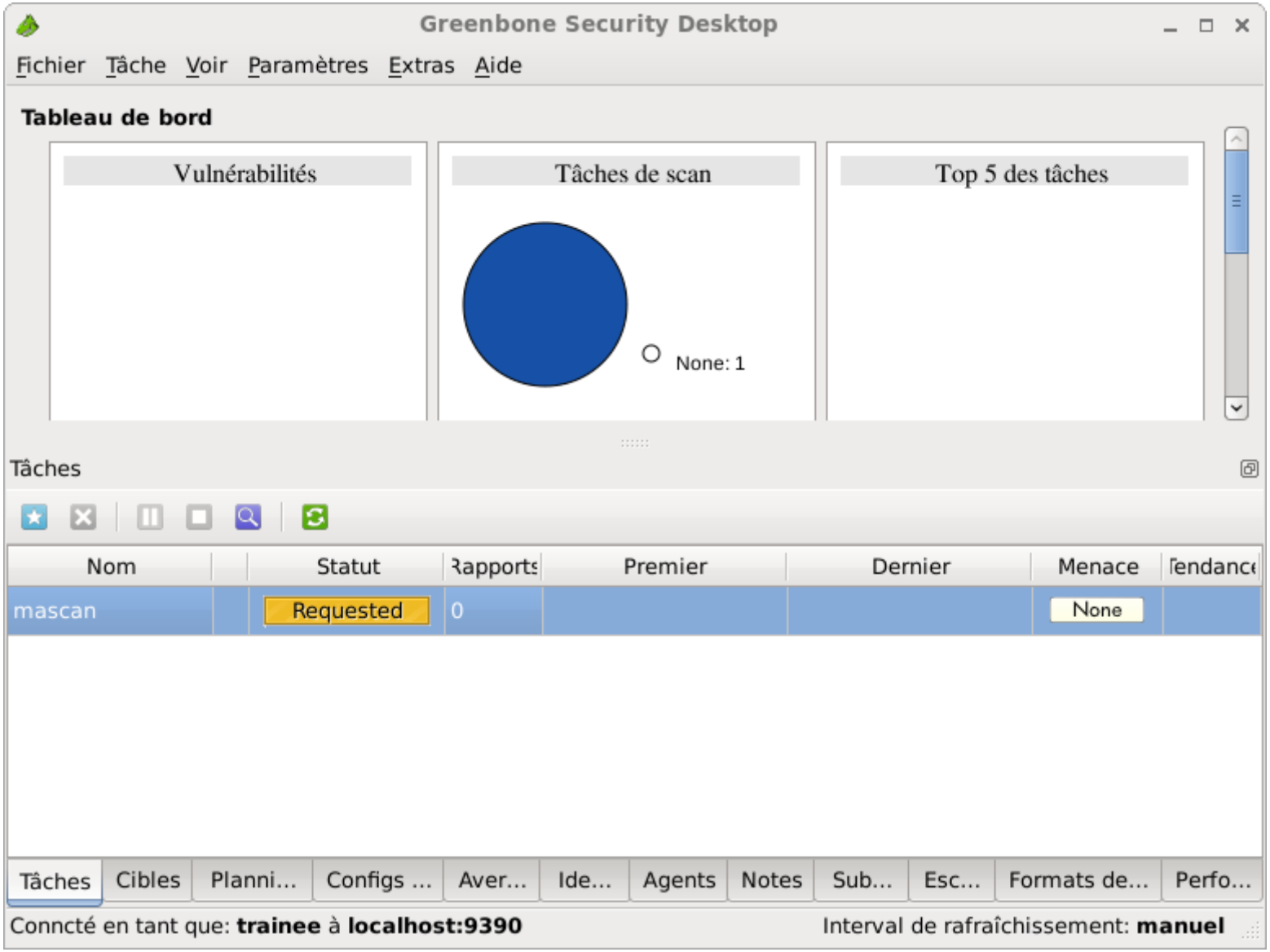
Renseignez un nom pour votre première tâche et cliquez sur le bouton **Créer** :



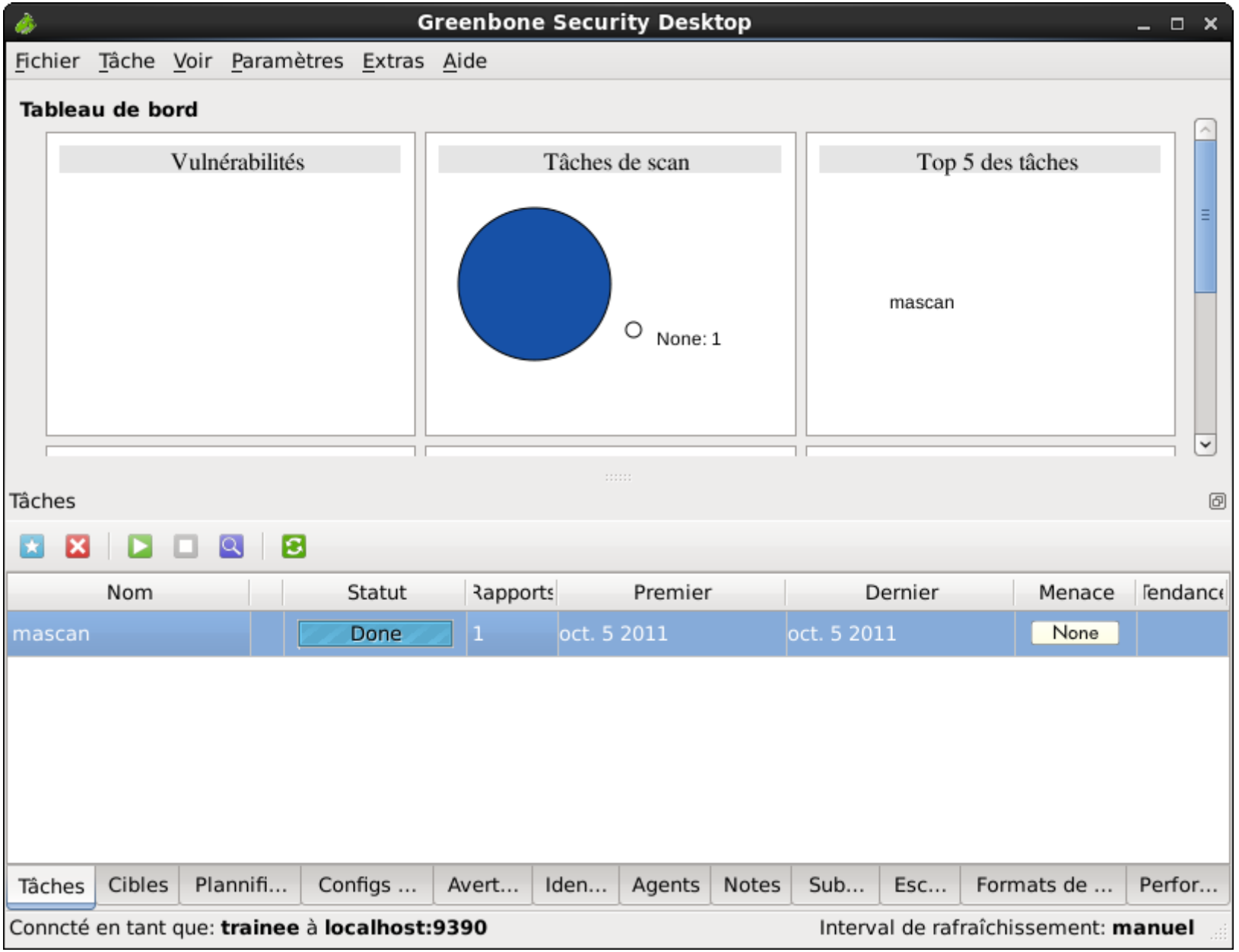
Vous obtiendrez une fenêtre similaire à celle-ci:



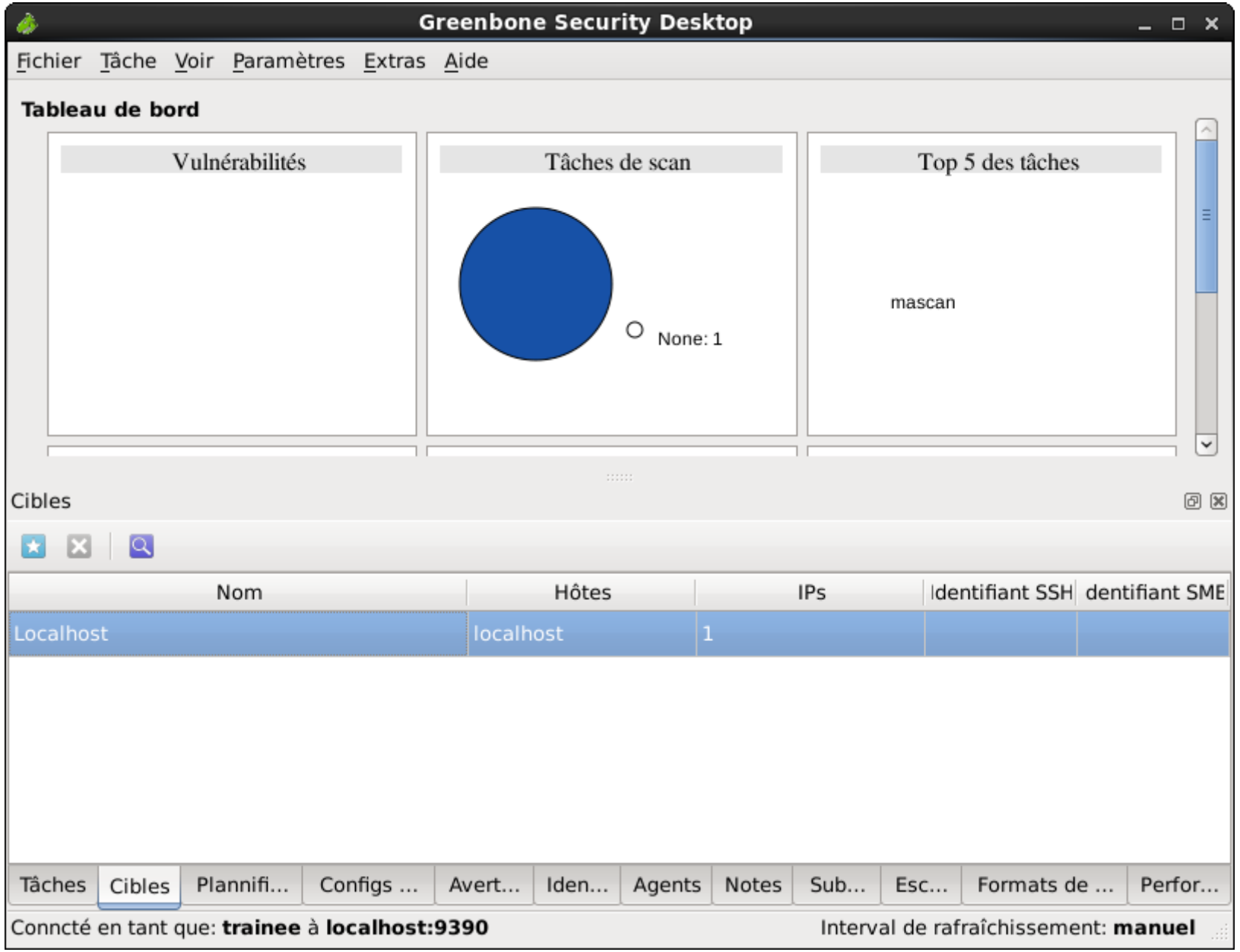
Cliquez sur le bouton démarrer. Vous obtiendrez une fenêtre similaire à celle-ci:



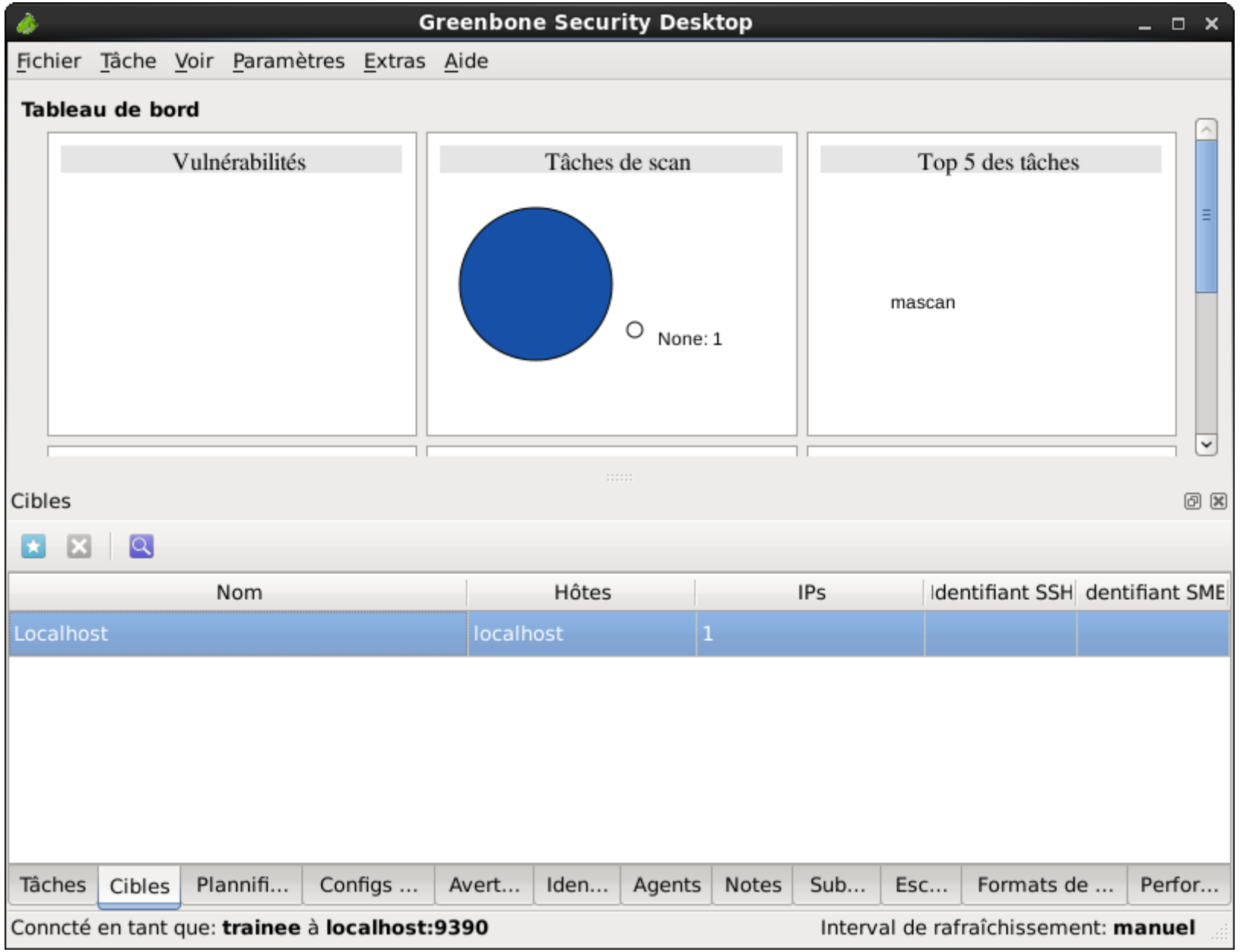
A l'issu de l'analyse, vous obtiendrez une fenêtre similaire à celle-ci:



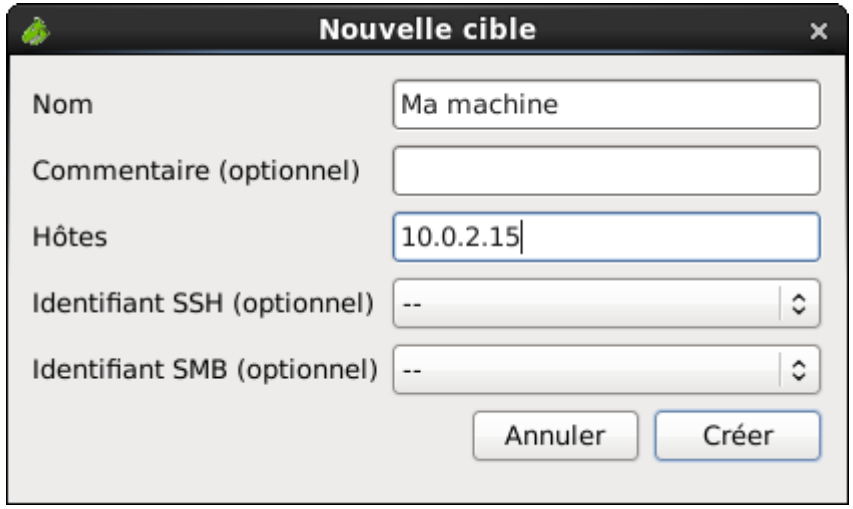
L'analyse précédente a été effectuée sur **localhost** :



Ajoutez maintenant votre propre adresse IP en tant que cible en cliquant sur le bouton en étoile :

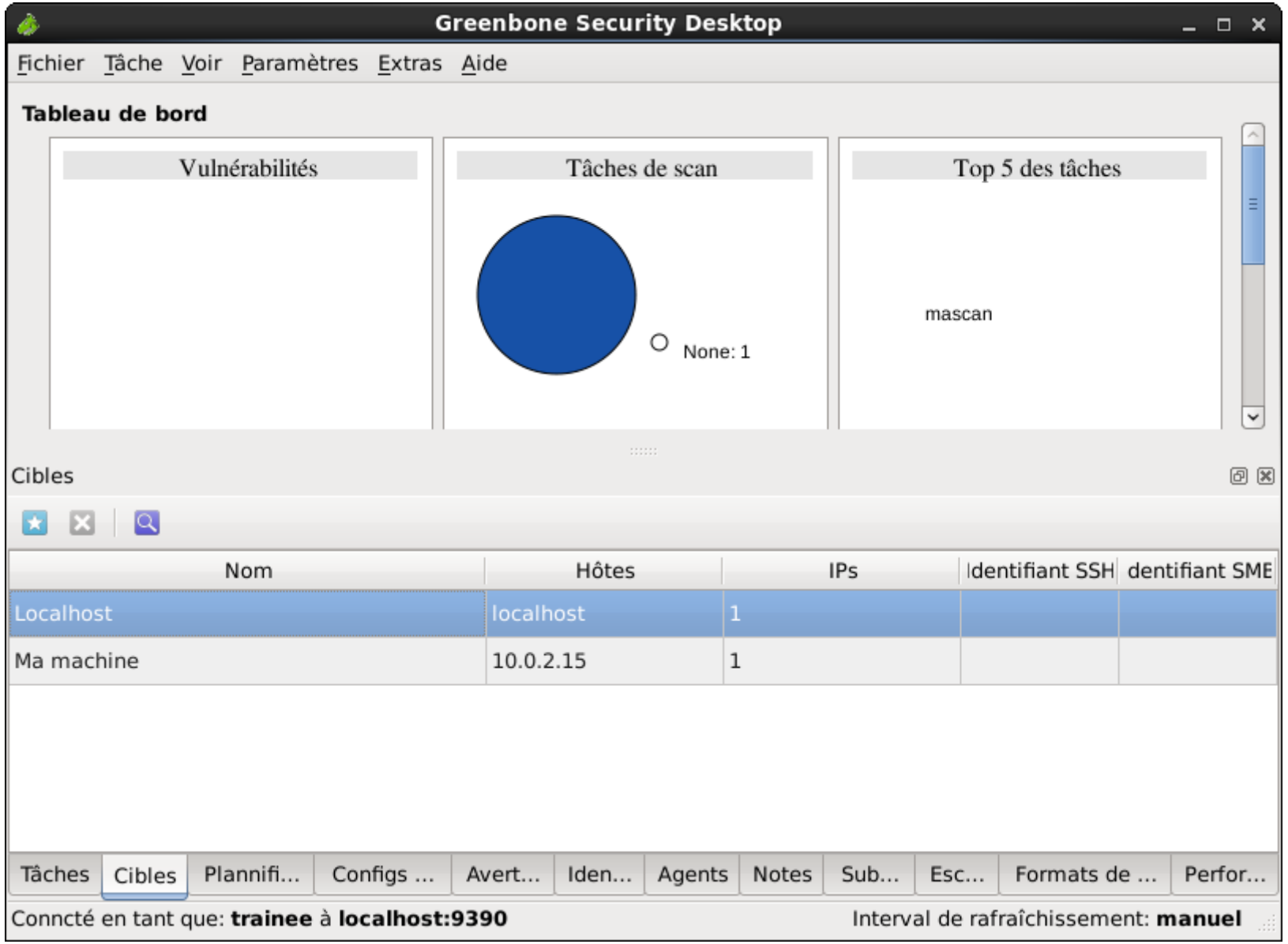


Renseignez les informations comme indiqué ci-après :

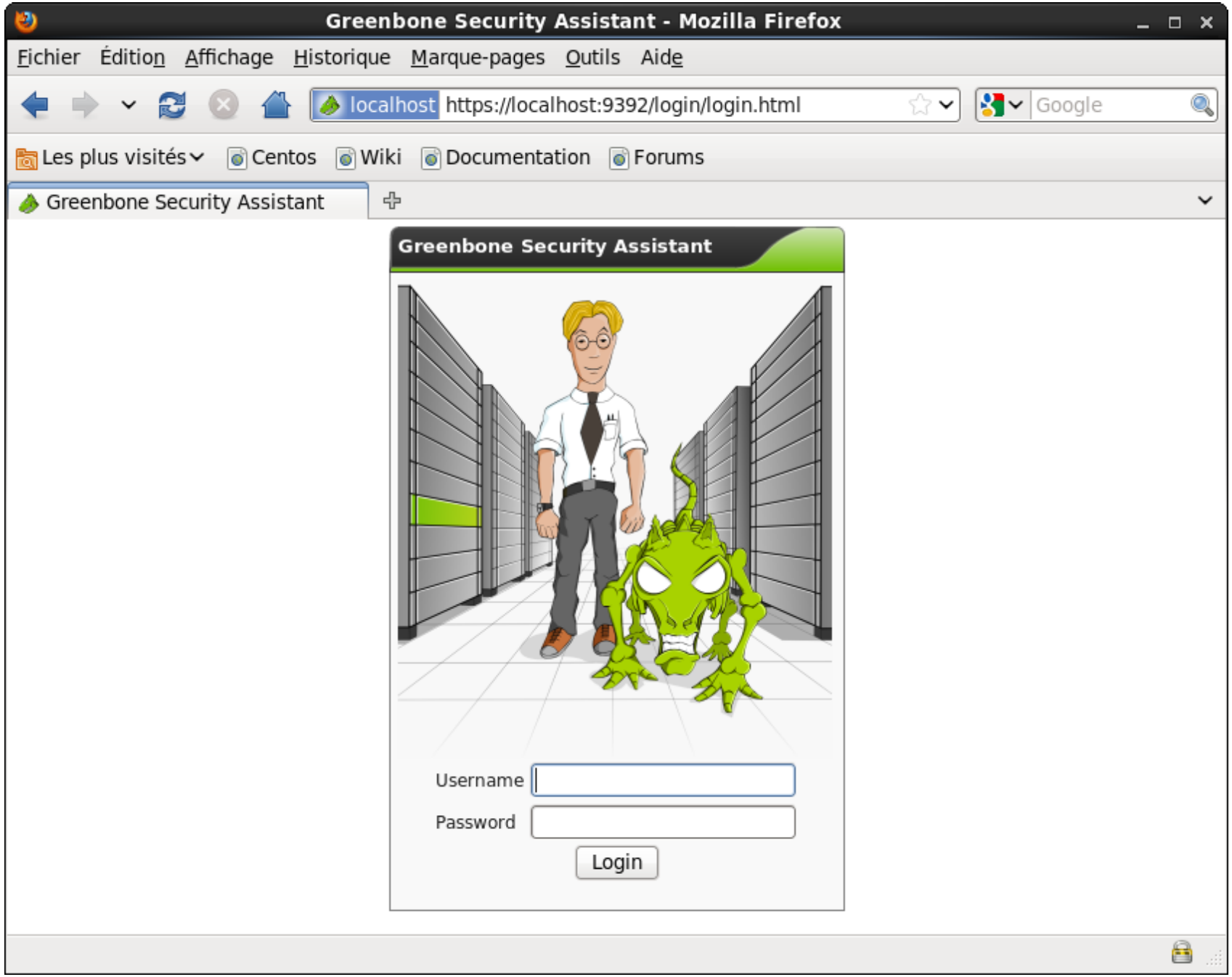


Vous pouvez indiquer un réseau entier de la forme 10.0.2.0/24

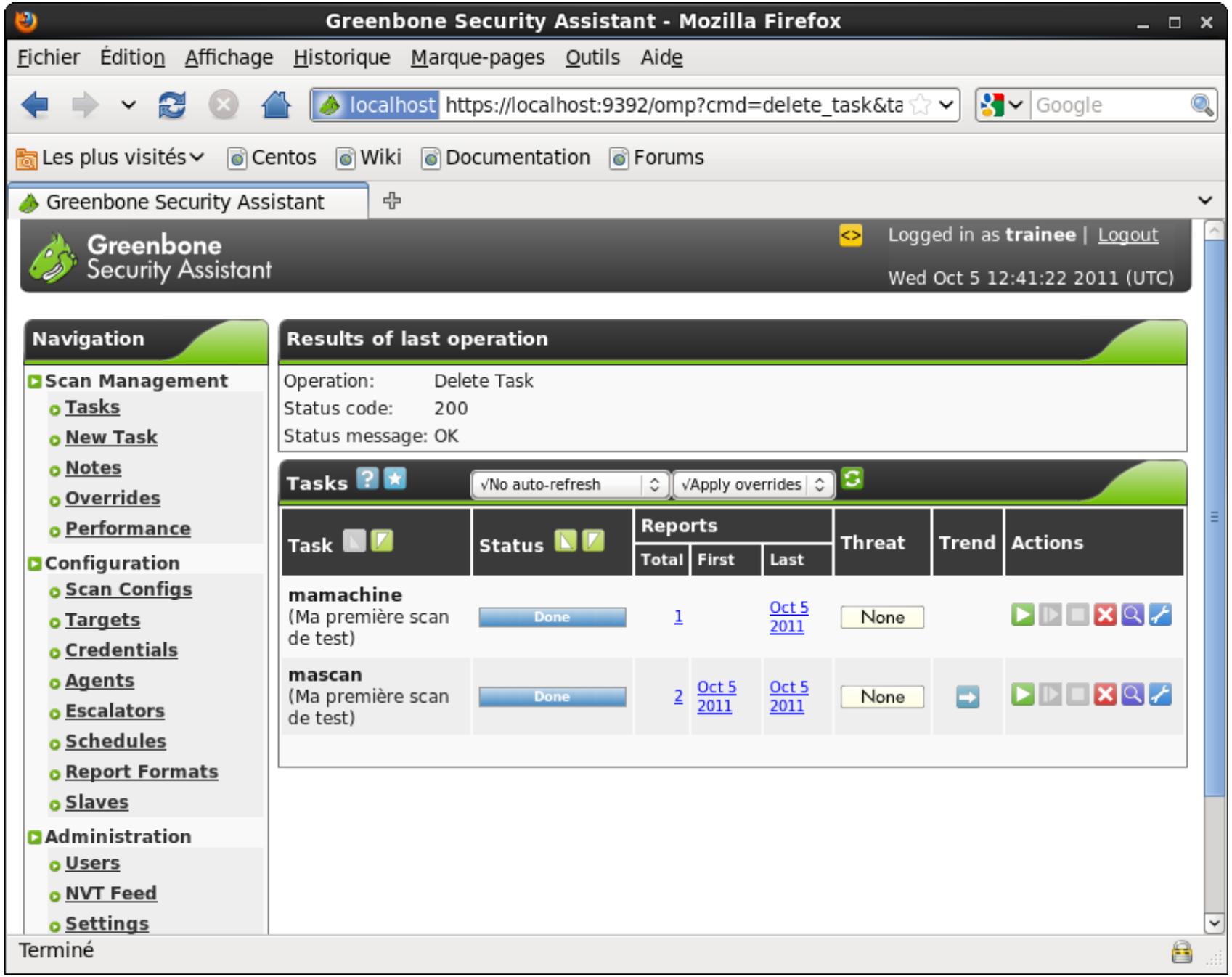
Cliquer sur le bouton **Créer**, vous obtiendrez une fenetre similaire à celle-ci :



Ouvrez maintenant une fenêtre de votre navigateur web et naviguez à la page **https://localhost:9392/**. Vous obtiendrez un résultat similaire à celui-ci :


Greenbone Security Assistant - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils Aide
localhost https://localhost:9392/login/login.html
Google
Les plus visités Centos Wiki Documentation Forums
Greenbone Security Assistant
Greenbone Security Assistant
Username
Password
Login

Entrez votre nom de connexion et votre mot de passe et validez. Vous obtiendrez une fenêtre similaire à celle-ci :

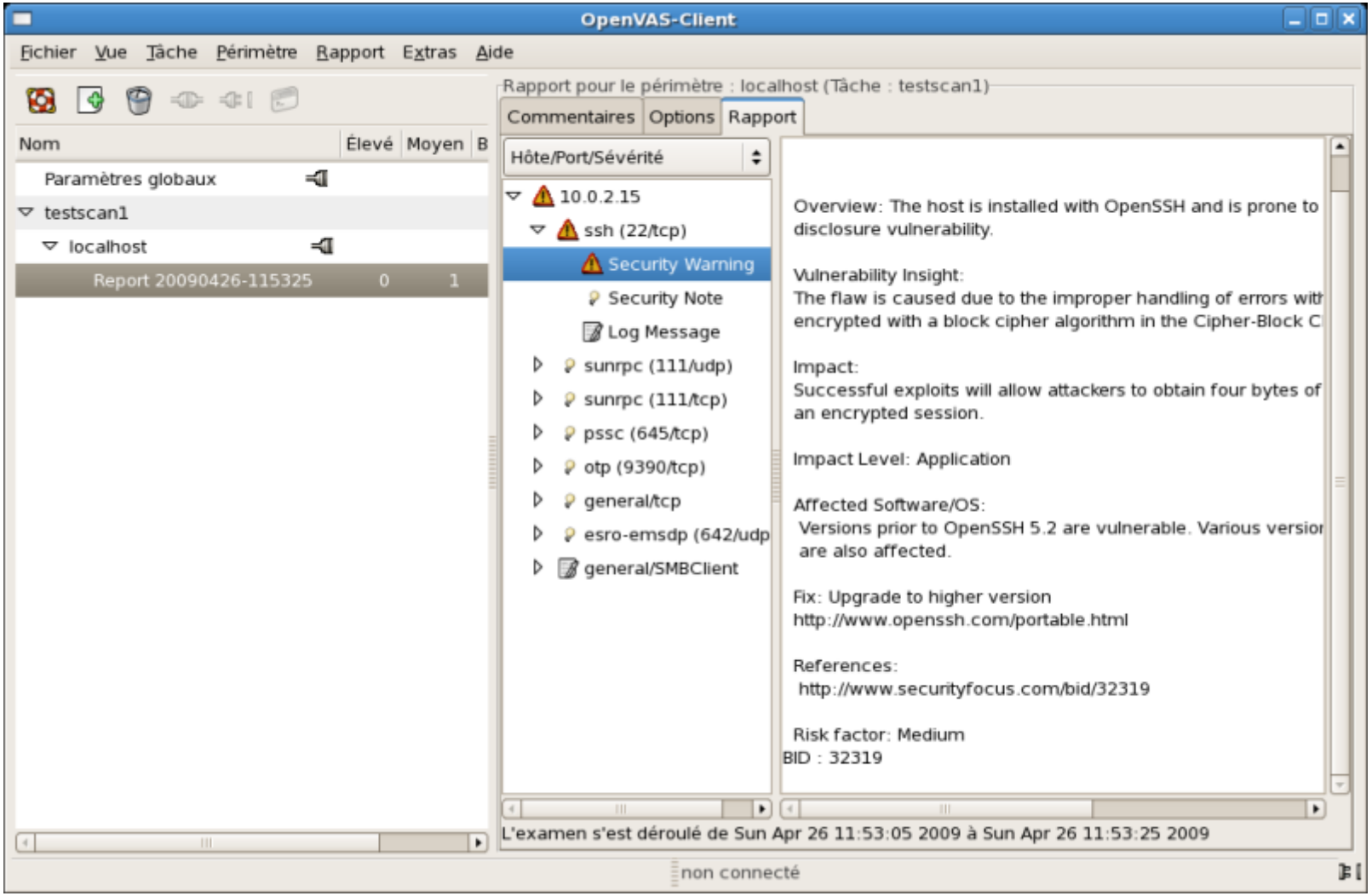

Greenbone Security Assistant - Mozilla Firefox
Fichier Édition Affichage Historique Marque-pages Outils Aide
localhost https://localhost:9392/omp?cmd=delete_task&ta
Google
Les plus visités Centos Wiki Documentation Forums
Greenbone Security Assistant
Greenbone Security Assistant
Logged in as trainee | Logout
Wed Oct 5 12:41:22 2011 (UTC)
Navigation
Scan Management
Tasks
New Task
Notes
Overrides
Performance
Configuration
Scan Configs
Targets
Credentials
Agents
Escalators
Schedules
Report Formats
Slaves
Administration
Users
NVT Feed
Settings
Results of last operation
Operation: Delete Task
Status code: 200
Status message: OK
Tasks
√No auto-refresh
√Apply overrides
Task
Status
Reports
Total
First
Last
Threat
Trend
Actions
mamachine
(Ma première scan de test)
Done
1
Oct 5 2011
None
mascan
(Ma première scan de test)
Done
2
Oct 5 2011
Oct 5 2011
None
Terminé

Analyse des Résultats

Vous apercevrez une liste de ports qui apparaissent dans le cadre de gauche. A côté de chaque port problématique, vous apercevrez une icône :

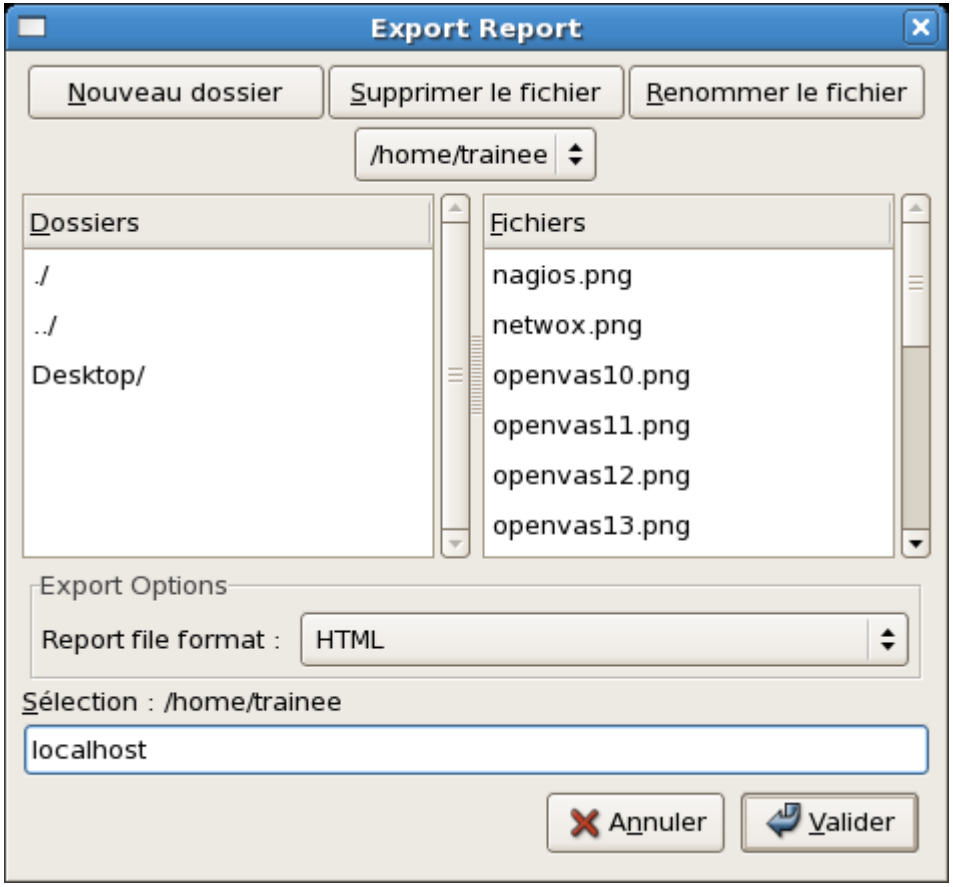
- **L'ampoule** signifie une note indiquant un problème *éventuel*,
- Le panneau **Attention** signifie un avertissement indiquant un problème *probable*,
- Le panneau **Sens Interdit** signifie un trou de sécurité indiquant un problème *existant*.

En cliquant sur une des entrées, vous apercevrez le détail du problème dans le cadre de droite. Vous obtiendrez une fenêtre similaire à celle-ci:

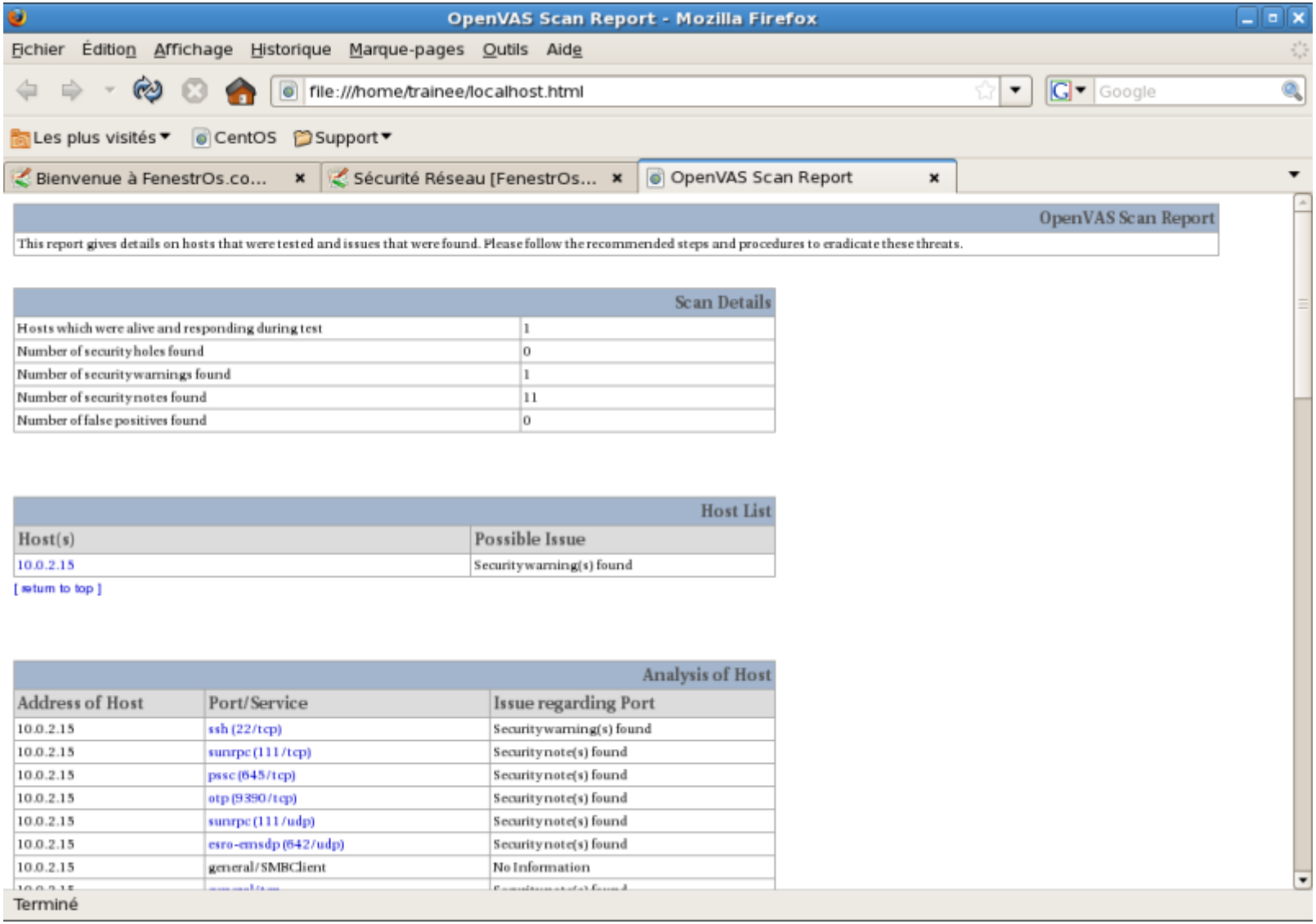


Vous trouverez aussi une **solution** ainsi qu'une évaluation du niveau de risque, **Risk factor**.

A la fin de votre analyse, vous pouvez sauvegarder le rapport sous plusieurs formats différents :



Un des formats le plus intéressant est le format html :



LAB #22 - Mise en place de Netwox

Installation

Netwox s'installe simplement en utilisant yum :

```
[root@centos6 ~]# yum install netwox
Loaded plugins: fastestmirror, refresh-packagekit
Loading mirror speeds from cached hostfile
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package netwox.i686 0:5.35.0-1.el6.rf set to be updated
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
================================================================================
 Package                                Arch                                Version
Repository                                Size
================================================================================
================================================================================
Installing:
 netwox                                 i686                                5.35.0-1.el6.rf
rpmforge                                 536 k

Transaction Summary
================================================================================
================================================================================
Install       1 Package(s)
Upgrade       0 Package(s)

Total download size: 536 k
Installed size: 1.5 M
```

```
Is this ok [y/N]: y
Downloading Packages:
netwox-5.35.0-1.el6.rf.i686.rpm
| 536 kB     00:07
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Installing     : netwox-5.35.0-1.el6.rf.i686
1/1

Installed:
  netwox.i686 0:5.35.0-1.el6.rf

Complete!
```

Utilisation

Le programme **netwox** est un utilitaire puissant de vérification de la sécurité. Au lancement, vous obtiendrez un résultat similaire a celui-ci:

```
[root@centos6 ~]# netwox
Netwox toolbox version 5.35.0. Netwib library version 5.35.0.

######################## MAIN MENU ########################
 0 - leave netwox
 3 - search tools
 4 - display help of one tool
 5 - run a tool selecting parameters on command line
 6 - run a tool selecting parameters from keyboard
 a + information
 b + network protocol
 c + application protocol
 d + sniff (capture network packets)
```

```
 e + spoof (create and send packets)
 f + record (file containing captured packets)
 g + client
 h + server
 i + ping (check if a computer if reachable)
 j + traceroute (obtain list of gateways)
 k + scan (computer and port discovery)
 l + network audit
 m + brute force (check if passwords are weak)
 n + remote administration
 o + tools not related to network
Select a node (key in 03456abcdefghijklmno):
```

L'utilisation de **netwox** en mode interactif se fait a l'aide des menus proposés. Dans notre cas, nous souhaitons utiliser un des outils de la section **network audit**. Il convient donc de choisir le menu **l** :

```
###################### network audit ######################
 0 - leave netwox
 1 - go to main menu
 2 - go to previous menu
 3 - search tools
 4 - display help of one tool
 5 - run a tool selecting parameters on command line
 6 - run a tool selecting parameters from keyboard
 a + network audit using Ethernet
 b + network audit using IP
 c + network audit using TCP
 d + network audit using ICMP
 e + network audit using ARP
Select a node (key in 0123456abcde):
```

Choisissez ensuite le menu **c** :

```
################# network audit using TCP #################
```

```
 0 - leave netwox
 1 - go to main menu
 2 - go to previous menu
 3 - search tools
 4 - display help of one tool
 5 - run a tool selecting parameters on command line
 6 - run a tool selecting parameters from keyboard
 a - 76:Synflood
 b - 77:Check if seqnum are predictible
 c - 78:Reset every TCP packet
 d - 79:Acknowledge every TCP SYN
```

Notre choix de test s'arrête sur un test du type **Synflood** sur un de nos serveurs internes. Nous choisissons donc le menu **a** :

```
################## help for tool number 76 ##################
Title: Synflood
+---------------------------------------------------------------------+
| This tool sends a lot of TCP SYN packets.                           |
| It permits to check how a firewall behaves when receiving packets   |
| which have to be ignored.                                           |
| Parameter --spoofip indicates how to generate link layer for spoofing. |
| Values 'best', 'link' or 'raw' are common choices for --spoofip. Here  |
| is the list of accepted values:                                     |
|  - 'raw' means to spoof at IP4/IP6 level (it uses system IP stack). If |
|    a firewall is installed, or on some systems, this might not work.   |
|  - 'linkf' means to spoof at link level (currently, only Ethernet is   |
|    supported). The 'f' means to Fill source Ethernet address.          |
|    However, if source IP address is spoofed, it might be impossible    |
|    to Fill it. So, linkf will not work: use linkb or linkfb instead.   |
|  - 'linkb' means to spoof at link level. The 'b' means to left a Blank |
|    source Ethernet address (0:0:0:0:0:0, do not try to Fill it).       |
|  - 'linkfb' means to spoof at link level. The 'f' means to try to Fill |
|    source Ethernet address, but if it is not possible, it is left      |
|    Blank.                                                              |
```

```
|  - 'rawlinkf' means to try 'raw', then try 'linkf'                      |
|  - 'rawlinkb' means to try 'raw', then try 'linkb'                      |
|  - 'rawlinkfb' means to try 'raw', then try 'linkfb'                    |
|  - 'linkfraw' means to try 'linkf', then try 'raw'                      |
|  - 'linkbraw' means to try 'linkb', then try 'raw'                      |
|  - 'linkfbraw' means to try 'linkfb', then try 'raw'                    |
|  - 'link' is an alias for 'linkfb'                                      |
|  - 'rawlink' is an alias for 'rawlinkfb'                                |
|  - 'linkraw' is an alias for 'linkfbraw'                                |
|  - 'best' is an alias for 'linkraw'. It should work in all cases.       |
|                                                                         |
| This tool may need to be run with admin privilege in order to spoof.    |
+-------------------------------------------------------------------------+
Usage: netwox 76 -i ip -p port [-s spoofip]
Parameters:
 -i|--dst-ip ip                destination IP address {5.6.7.8}
 -p|--dst-port port            destination port number {80}
 -s|--spoofip spoofip          IP spoof initialization type {linkbraw}
Example: netwox 76 -i "5.6.7.8" -p "80"
Example: netwox 76 --dst-ip "5.6.7.8" --dst-port "80"
Press 'r' or 'k' to run this tool, or any other key to continue
```

Il convient ensuite d'appuyer sur la touche [r] ou [k] pour lancer l'utilitaire.

En utilisant l'exemple fourni, il convient de saisir la ligne suivante :

```
netwox 76 -i "10.0.2.3" -p "80"
```

Il est a noter que **netwox** peut être utilisé sans faire appel au menus interactifs, à condition de connaître le numéro **netwox** du test à lancer:

```
# netwox 76 -i "10.0.2.3" -p "80"
```

Avant de poursuivre, lancez **tcpdump** en arrière plan afin de journaliser le trafic et vérifiez que le job est actif :

```
[root@centos6 ~]# tcpdump -i eth0 -w netwox.dump &
[1] 12388
[root@centos6 ~]# tcpdump: listening on eth0, link-type EN10MB (Ethernet), capture size 96 bytes
[^C]
[root@centos6 ~]# jobs
[1]+  Running                 tcpdump -i eth0 -w netwox.dump &
```

Lancez maintenant votre attaque et attendez **10s** avant de saisir [^C] :

```
[root@centos6 ~]# netwox 76 -i "10.0.2.3" -p "80"
[^C]
```

Vérifiez la présence du fichier **netwox.dump** :

```
[root@redhat ~]# ls -l netwox.dump
-rw-r--r-- 1 root root 37474304 mar 17 09:58 netwox.dump
```

Ouvrez ensuite le fichier **netwox.dump** avec **wireshark** :

Notez la présence des mauvais paquets !

Avertissement important

netwox est un outil puissant. Il convient de noter que:

- il ne doit pas être installé sur un serveur de production mais sur le poste de l'administrateur,
- netwox existe aussi en version Windows™,
- l'utilisation de netwox à des fins autres que de test est interdite.

LAB #23 - La commande chroot

Importez une machine virtuelle vierge de CentOS 6 pour effectuer le LAB #23.

Le chrootage permet de séparer un utilisateur du système.

Sous RHEL/CentOS 6 le binaire chroot est installé par défaut :

```
[root@centos6 ~]# whereis chroot
chroot: /usr/sbin/chroot /usr/share/man/man2/chroot.2.gz /usr/share/man/man1/chroot.1.gz
```

Commencez par créer un répertoire pour l'utilisateur qui sera emprisonné :

```
[root@centos6 ~]# mkdir /home/prison
```

Le binaire **/usr/sbin/chroot** doit prendre le SUID bit :

```
[root@centos6 ~]# ls -l /usr/sbin/chroot
-rwxr-xr-x. 1 root root 30644 30 mai   18:50 /usr/sbin/chroot
[root@centos6 ~]# chmod +s /usr/sbin/chroot
[root@centos6 ~]# ls -l /usr/sbin/chroot
-rwsr-sr-x. 1 root root 30644 30 mai   18:50 /usr/sbin/chroot
```

Créez maintenant un script de connexion générique pour que l'utilisateur **prison** puisse se connecter :

```
[root@centos6 ~]# vi /bin/chroot
```

Éditez-le ainsi :

```
#!/bin/bash
```

```
exec -c /usr/sbin/chroot /home/$USER /bin/bash
```

Rendez ce script exécutable :

```
[root@centos6 ~]# chmod +x /bin/chroot
```

Il est maintenant nécessaire de copier toutes les commandes dont l'utilisateur **prison** aura besoin. Dans cet exemple, nous allons nous contenter de copier **/bin/bash** et **/bin/ls** ainsi que les bibliothèques associées :

```
[root@centos6 ~]# mkdir /home/prison/bin
[root@centos6 ~]# cp /bin/bash /home/prison/bin/
[root@centos6 ~]# ldd /bin/bash
    linux-gate.so.1 =>  (0x00948000)
    libtinfo.so.5 => /lib/libtinfo.so.5 (0x00101000)
    libdl.so.2 => /lib/libdl.so.2 (0x00582000)
    libc.so.6 => /lib/libc.so.6 (0x003f4000)
    /lib/ld-linux.so.2 (0x003d2000)
[root@centos6 ~]# mkdir /home/prison/lib
[root@centos6 ~]# cp /lib/libtinfo.so.5 /home/prison/lib
[root@centos6 ~]# cp /lib/libdl.so.2 /home/prison/lib
[root@centos6 ~]# cp /lib/libc.so.6 /home/prison/lib
[root@centos6 ~]# cp /lib/ld-linux.so.2 /home/prison/lib
[root@centos6 ~]# cp /bin/ls /home/prison/bin/
[root@centos6 ~]# ldd /bin/ls
    linux-gate.so.1 =>  (0x00b58000)
    libselinux.so.1 => /lib/libselinux.so.1 (0x006c8000)
    librt.so.1 => /lib/librt.so.1 (0x005d2000)
    libcap.so.2 => /lib/libcap.so.2 (0x00ddc000)
    libacl.so.1 => /lib/libacl.so.1 (0x00df4000)
    libc.so.6 => /lib/libc.so.6 (0x003f4000)
    libdl.so.2 => /lib/libdl.so.2 (0x00582000)
    /lib/ld-linux.so.2 (0x003d2000)
    libpthread.so.0 => /lib/libpthread.so.0 (0x00589000)
    libattr.so.1 => /lib/libattr.so.1 (0x0520b000)
```

```
[root@centos6 ~]# cp /lib/libselinux.so.1 /home/prison/lib
[root@centos6 ~]# cp /lib/librt /home/prison/lib
[root@centos6 ~]# cp /lib/librt.so.1 /home/prison/lib
[root@centos6 ~]# cp /lib/libcap.so.2 /home/prison/lib
[root@centos6 ~]# cp /lib/libacl.so.1 /home/prison/lib
[root@centos6 ~]# cp /lib/libpthread.so.0 /home/prison/lib
[root@centos6 ~]# cp /lib/libattr.so.1 /home/prison/lib
```

Créez maintenant le groupe chroot :

```
[root@centos6 ~]# groupadd chroot
[root@centos6 ~]# cat /etc/group | grep chroot
chroot:x:502:
```

Créez maintenant l'utilisateur **prison** :

```
[root@centos6 ~]# useradd prison -c chroot_user -d /home/prison -g chroot -s /bin/chroot
useradd : attention, le répertoire personnel existe déjà.
Aucun fichier du répertoire « skels » n'y sera copié.
[root@centos6 ~]# cp /etc/skel/.* /home/prison
cp: omission du répertoire « /etc/skel/. »
cp: omission du répertoire « /etc/skel/.. »
cp: omission du répertoire « /etc/skel/.gnome2 »
cp: omission du répertoire « /etc/skel/.mozilla »
[root@centos6 ~]# cp -pfR /etc/skel/.m* /home/prison
[root@centos6 ~]# cp -pfR /etc/skel/.g* /home/prison
[root@centos6 ~]# passwd prison
Changement de mot de passe pour l'utilisateur prison.
Nouveau mot de passe :
MOT DE PASSE INCORRECT : basé sur un mot du dictionnaire
MOT DE PASSE INCORRECT : est trop simple
Retapez le nouveau mot de passe :
passwd : mise à jour réussie de tous les jetons d'authentification.
```

Dernièrement, modifiez le propriétaire et le groupe du répertoire **/home/prison** :

```
[root@centos6 ~]# chown -R prison:chroot /home/prison
```

Essayez maintenant de vous connecter en tant que prison :

```
[root@centos6 ~]# su - prison
bash-4.1$ pwd
/
bash-4.1$ ls -la
total 40
drwxr-xr-x. 6 501 502 4096 Oct  3 16:21 .
drwxr-xr-x. 6 501 502 4096 Oct  3 16:21 ..
-rw-------. 1 501 502   21 Oct  3 16:23 .bash_history
-rw-r--r--. 1 501 502   18 Oct  3 16:10 .bash_logout
-rw-r--r--. 1 501 502  176 Oct  3 16:10 .bash_profile
-rw-r--r--. 1 501 502  124 Oct  3 16:10 .bashrc
drwxr-xr-x. 2 501 502 4096 Nov 12  2010 .gnome2
drwxr-xr-x. 4 501 502 4096 Jul 28 12:19 .mozilla
drwxr-xr-x. 2 501 502 4096 Oct  3 16:22 bin
drwxr-xr-x. 2 501 502 4096 Oct  3 16:20 lib
bash-4.1$ exit
exit
[root@centos6 ~]#
```

Notez que l'utilisateur **prison** est *chrooté*.

LAB #24 - Sécuriser Apache

Importez une machine virtuelle vierge de CentOS 6 pour effectuer les LABs #24 et #25.

Apache est capable de gérer de multiples sites hébergés sur la même machine. Ceci est rendu possible par un fichier de configuration spécifique appelé: **/etc/httpd/conf/vhosts.d/Vhosts.conf**. Le répertoire **/etc/httpd/conf/vhosts.d/** n'existant pas, créez-le:

```
[root@centos ~]# mkdir /etc/httpd/conf/vhosts.d/
```

Créez ensuite le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** :

```
[root@centos ~]# touch /etc/httpd/conf/vhosts.d/Vhosts.conf
```

Le contenu de fichier est inclus à l'intérieur de la configuration d'apache grâce à la directive suivante du fichier **httpd.conf**:

```
Include conf/vhosts.d/*.conf
```

Ajoutez donc cette ligne au fichier **/etc/httpd/conf/httpd.conf**.

Il existe deux façons de créer des sites (hôtes) virtuels :

- Hôte Virtuel par adresse IP
- Hôte Virtuel par nom

Créez un répertoire **/www/site1** à la racine de votre arborescence pour héberger notre premier hôte virtuel :

```
[root@centos ~]# mkdir -p /www/site1
```

Créez ensuite le fichier **index.html** du répertoire **/www/site1**:

```
[root@centos ~]# vi /www/site1/index.html
```

Editez-le ainsi :

index.html

```
<html>
<head>
```

```
<title>Page de Test</title>
<body>
<center>Accueil du site 1</center>
</body>
</html>
```

Hôte virtuel par nom

Nous allons d'abord considérer les sites virtuels par nom. Editez donc le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** en suivant l'exemple ci-dessous :

Vhosts.conf

```
################## Named VirtualHosts
NameVirtualHost *:80
###################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
</VirtualHost>
###################www.vhostnom.com
<VirtualHost *:80>
ServerName www.vhostnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
<Directory /www/site1>
Order allow,deny
Allow from all
</Directory>
</VirtualHost>
```

Notez qu'apache servira toujours le **contenu da la première section** des sites virtuels par défaut, sauf précision de la part de l'internaute. Il est donc impératif d'ajouter une section **VirtualHost** pour votre site par défaut.

Redémarrez ensuite le serveur Apache :

```
[root@centos ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Avant de pouvoir consulter le site virtuel, il faut renseigner votre fichier **hosts** :

```
10.0.2.15            www.homeland.net
10.0.2.15            www.vhostnom.com
```

Sauvegardez votre fichier hosts et installez le navigateur web en mode texte **lynx** :

```
# yum install lynx
```

Testez votre configuration avec **lynx** :

```
[root@centos ~]# lynx --dump http://www.vhostnom.com
                              Accueil du site 1
```

Afin de mieux comprendre les visites à notre site virtuel, nous avons besoin d'un fichier log ainsi qu'un fichier de log des erreurs. Ouvrez donc le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf** et ajoutez les deux lignes suivantes:

```
Customlog /www/logs/site1/vhostnom.log combined
Errorlog /www/logs/site1/error.log
```

Vous obtiendrez une fenêtre similaire à celle-ci :

Vhosts.conf

```
################## Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
</VirtualHost>
##################www.vhostnom.com
<VirtualHost *:80>
ServerName www.vhostnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
Customlog /www/logs/site1/vhostnom.log combined
Errorlog /www/logs/site1/error.log
<Directory /www/site1>
Order allow,deny
Allow from all
</Directory>
</VirtualHost>
```

Créez ensuite le répertoire /www/logs/site1 :

```
[root@centos ~]# mkdir -p /www/logs/site1
```

Redémarrez le serveur Apache :

```
[root@centos ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Saisissez maintenant l'adresse http://www.vhostnom.com dans la barre d'adresses de votre navigateur.

Contrôlez maintenant le contenu du répertoire **/www/logs/site1**. Vous devez y retrouver deux fichiers :

```
[root@centos ~]# ls -l /www/logs/site1/
total 8
-rw-r--r--. 1 root root  98 15 juil. 10:36 error.log
-rw-r--r--. 1 root root 365 15 juil. 10:36 vhostnom.log
```

Ces deux fichiers **vhostnom.log** et **error.log** sont créés automatiquement par Apache.

En contrôlant le contenu du fichier **/www/logs/site1/vhostnom.log** nous constatons que le log a été généré :

```
[root@centos ~]# cat /www/logs/site1/vhostnom.log
10.0.2.15 - - [15/Jul/2013:10:36:43 +0200] "GET / HTTP/1.1" 200 100 "-" "Mozilla/5.0 (X11; Linux i686)
AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.63 Safari/537.31"
10.0.2.15 - - [15/Jul/2013:10:36:43 +0200] "GET /favicon.ico HTTP/1.1" 404 291 "-" "Mozilla/5.0 (X11; Linux i686)
AppleWebKit/537.31 (KHTML, like Gecko) Chrome/26.0.1410.63 Safari/537.31"
```

Hôte virtuel par adresse IP

Vous allez maintenant procéder à la création d'un site (hôte) virtuel par adresse IP. Normalement, votre serveur serait muni de deux cartes réseaux permettant ainsi d'attribuer un site ou hôte virtuel par numéro IP. Cependant, dans le cas suivant vous allez tout simplement affecté deux numéros IP à la même carte afin de procéder aux tests. Pour faire ceci, vous devez associer une deuxième adresse IP à votre carte réseau eth0. Saisissez donc la commande suivante dans une fenêtre de console en tant que root :

```
[root@centos ~]# ifconfig eth0 add 192.168.1.99
```

Vérifiez ensuite avec la commande **ifconfig**:

```
[root@centos ~]# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:48:7D:7F
          inet adr:10.0.2.15  Bcast:10.0.2.255  Masque:255.255.255.0
          adr inet6: fe80::a00:27ff:fe48:7d7f/64 Scope:Lien
```

```
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:100259 errors:0 dropped:0 overruns:0 frame:0
          TX packets:78865 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:1000
          RX bytes:67227829 (64.1 MiB)  TX bytes:5964812 (5.6 MiB)

eth0:0    Link encap:Ethernet  HWaddr 08:00:27:48:7D:7F
          inet adr:192.168.1.99  Bcast:10.0.2.255  Masque:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1

lo        Link encap:Boucle locale
          inet adr:127.0.0.1  Masque:255.0.0.0
          adr inet6: ::1/128 Scope:Hôte
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:350 errors:0 dropped:0 overruns:0 frame:0
          TX packets:350 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 lg file transmission:0
          RX bytes:80682 (78.7 KiB)  TX bytes:80682 (78.7 KiB)
```

Créez maintenant le répertoire pour notre site2 :

```
[root@centos ~]# mkdir /www/site2
```

Créez la page d'accueil :

```
[root@centos ~]# vi /www/site2/index.html
```

Editez notre page d'accueil :

index.html

```
<html>
<body>
<center>Accueil du site 2</center>
```

```
</body>
</html>
```

Créez ensuite le répertoire /www/logs/site2 :

```
[root@centos ~]# mkdir /www/logs/site2
```

Editez maintenant le fichier **/etc/httpd/conf/vhosts.d/Vhosts.conf**:

Vhosts.conf

```
################## IP-based Virtual Hosts
<VirtualHost 192.168.1.99>
DocumentRoot /www/site2
ServerName www.vhostip.com
DirectoryIndex index.html
Customlog /www/logs/site2/vhostip.log combined
Errorlog /www/logs/site2/error.log
<Directory /www/site2>
Order allow,deny
Allow from all
</Directory>
</VirtualHost>
################## Named VirtualHosts
NameVirtualHost *:80
##################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
</VirtualHost>
##################www.vhostnom.com
<VirtualHost *:80>
ServerName www.vhostnom.com
```

```
DirectoryIndex index.html
DocumentRoot /www/site1
Customlog /www/logs/site1/vhostnom.log combined
Errorlog /www/logs/site1/error.log
<Directory /www/site1>
Order allow,deny
Allow from all
</Directory>
</VirtualHost>
```

Editez ensuite le fichier **/etc/hosts** et ajoutez la ligne suivante:

```
192.168.1.99            www.vhostip.com
```

Redémarrez votre serveur Apache :

```
[root@centos ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Testez votre configuration avec **lynx** :

```
[root@centos ~]# lynx --dump http://www.vhostip.com
                            Accueil du site 2
```

Consultez maintenant le répertoire **/www/logs/site2**. Vous constaterez l'apparition d'un fichier log pour le site www.vhostip.com :

```
[root@centos ~]# ls -l /www/logs/site2/
total 4
-rw-r--r--. 1 root root   0 15 juil. 10:40 error.log
-rw-r--r--. 1 root root 139 15 juil. 10:40 vhostip.log
```

mod_auth_basic

La sécurité sous Apache se gère grâce à deux fichiers :

- **.htaccess**
  - Ce fichier contient les droits d'accès au répertoire dans lequel est situé le fichier
- **.htpasswd**
  - Ce fichier contient les noms d'utilisateurs et les mots de passe des personnes autorisées à accéder au répertoire protégé par le fichier .htaccess.

Pour activer la sécurité sous apache 2.2, les trois modules **mod_auth_basic**, **mod_authn_file** et **mod_authz_host** doivent être chargées. Vérifiez donc que les trois lignes suivantes ne sont **pas** en commentaires dans le fichier **httpd.conf**:

```
[root@centos ~]# cat /etc/httpd/conf/httpd.conf | grep auth_basic
LoadModule auth_basic_module modules/mod_auth_basic.so
[root@centos ~]# cat /etc/httpd/conf/httpd.conf | grep authn_file
LoadModule authn_file_module modules/mod_authn_file.so
[root@centos ~]# cat /etc/httpd/conf/httpd.conf | grep authz_host_module
LoadModule authz_host_module modules/mod_authz_host.so
```

Configuration de la sécurité avec .htaccess

Dans le cas de notre serveur, nous souhaitons mettre en place un répertoire privé appelé ***secret***. Ce répertoire ne doit être accessible qu'au **webmaster**. Pour le faire, procédez ainsi :

Créez le répertoire secret dans le répertoire **/www/site1** :

```
[root@centos ~]# mkdir /www/site1/secret/
```

Créez le fichier **/www/site1/secret/.htaccess**:

```
[root@centos ~]# vi /www/site1/secret/.htaccess
```

Editez-le en suivant l'exemple ci-dessous :

.htaccess

```
AuthUserFile /www/passwords/site1/.htpasswd
AuthName "Secret du Site1"
AuthType Basic
<Limit GET>
require valid-user
</Limit>
```

Sauvegardez votre fichier.

Mise en place d'un fichier de mots de passe

Ensuite créez maintenant le répertoire /www/passwords/site1 :

```
[root@centos ~]# mkdir -p /www/passwords/site1
```

Créez maintenant le fichier **.htpasswd** avec une entrée pour le **webmaster** grâce à la commande **htpasswd** :

```
[root@centos ~]# htpasswd -c /www/passwords/site1/.htpasswd webmaster
New password: fenestros
Re-type new password: fenestros
Adding password for user webmaster
```

Vérifiez le contenu du fichier **/www/passwords/site1/.htpasswd** grâce à la commande **cat** :

```
[root@centos ~]# cat /www/passwords/site1/.htpasswd
```

```
webmaster:Xa2SvtJUBz.g.
```

Créez maintenant une page html dans le répertoire secret :

```
[root@centos ~]# vi /www/site1/secret/index.html
```

Maintenant, éditez-le ainsi :

index.html

```
<html>
<body>
<center>Si vous voyez ce message, vous avez decouvert mon secret !</center>
</body>
</html>
```

Finalement, pour que la sécurité par **.htaccess** soit prise en compte pour le répertoire secret, il faut rajouter une directive à la section de l'hôte virtuel par nom dans le fichier **Vhosts.conf** :

Vhosts.conf

```
################## IP-based Virtual Hosts
<VirtualHost 192.168.1.99>
DocumentRoot /www/site2
ServerName www.vhostip.com
DirectoryIndex index.html
Customlog /www/logs/site2/vhostip.log combined
Errorlog /www/logs/site2/error.log
<Directory /www/site2>
Order allow,deny
Allow from all
</Directory>
</VirtualHost>
```

```
################## Named VirtualHosts
NameVirtualHost *:80
###################Default Site Virtual Host
<VirtualHost *:80>
DocumentRoot /var/www/html
ServerName www.homeland.net
</VirtualHost>
###################www.vhostnom.com
<VirtualHost *:80>
ServerName www.vhostnom.com
DirectoryIndex index.html
DocumentRoot /www/site1
Customlog /www/logs/site1/vhostnom.log combined
Errorlog /www/logs/site1/error.log
<Directory /www/site1>
Order allow,deny
Allow from all
</Directory>
<Directory /www/site1/secret>
AllowOverride AuthConfig
</Directory>
</VirtualHost>
```

Sauvegardez votre fichier et puis redémarrez votre serveur Apache :

```
[root@centos ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Testez ensuite votre section privée en tapant http://www.vhostnom.com/secret/index.html dans la barre d'adresses de votre navigateur. Vous constaterez qu'une boîte de dialogue apparaît en vous demandant de renseigner le nom d'utilisateur ainsi que le mot de passe pour pouvoir avoir accès à la section « Secret du Site1 ».

mod_auth_mysql

Vous devez utiliser **mod_auth_mysql** pour protéger l'accès à un répertoire **secret2** dans votre site virtuel www.vhostnom.com.

Installation

Installez le module **mod_auth_mysql** et le serveur mysql :

```
[root@centos ~]# yum install mysql-server mod_auth_mysql
```

Configuration de MySQL

Il est maintenant nécessaire de préparer une base de données MySQL pour être compatible avec **mod_auth_mysql**. Démarrez donc le service **mysqld** :

```
[root@centos ~]# service mysqld start
Initialisation de la base de données MySQL :  WARNING: The host 'centos.fenestros.loc' could not be looked up
with resolveip.
This probably means that your libc libraries are not 100 % compatible
with this binary MySQL version. The MySQL daemon, mysqld, should work
normally with the exception that host name resolving will not work.
This means that you should use IP addresses instead of hostnames
when specifying MySQL privileges !
Installing MySQL system tables...
130715 10:56:43 [Note] libgovernor.so not found
OK
Filling help tables...
130715 10:56:43 [Note] libgovernor.so not found
OK
```

```
To start mysqld at boot time you have to copy
support-files/mysql.server to the right place for your system

PLEASE REMEMBER TO SET A PASSWORD FOR THE MySQL root USER !
To do so, start the server, then issue the following commands:

/usr/bin/mysqladmin -u root password 'new-password'
/usr/bin/mysqladmin -u root -h centos.fenestros.loc password 'new-password'

Alternatively you can run:
/usr/bin/mysql_secure_installation

which will also give you the option of removing the test
databases and anonymous user created by default.  This is
strongly recommended for production servers.

See the manual for more instructions.

You can start the MySQL daemon with:
cd /usr ; /usr/bin/mysqld_safe &

You can test the MySQL daemon with mysql-test-run.pl
cd /usr/mysql-test ; perl mysql-test-run.pl

Please report any problems with the /usr/bin/mysqlbug script!

                                                           [  OK  ]
Démarrage de mysqld :
```

Connectez-vous à mysql :

```
[root@centos ~]# mysql
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2
```

```
Server version: 5.5.32-cll-lve MySQL Community Server (GPL) by Atomicorp

Copyright (c) 2000, 2013, Oracle and/or its affiliates. All rights reserved.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql>
```

Puis saisissez les commandes MySQL suivantes :

```
CREATE DATABASE auth;

USE auth;

CREATE TABLE users (
user_name CHAR(30) NOT NULL,
user_passwd CHAR(20) NOT NULL,
PRIMARY KEY (user_name)
);

GRANT SELECT
ON auth.users
TO authuser@localhost
IDENTIFIED BY 'PaSsW0Rd';

INSERT INTO users VALUES ('testuser', ENCRYPT('testpass'));
```

Configuration d'Apache

Quittez mysql :

```
mysql> exit;
Bye
[root@centos ~]#
```

Créez ensuite le répertoire **/www/site1/secret2** :

```
[root@centos ~]# mkdir /www/site1/secret2
```

Créez maintenant une page **index.html** dans le répertoire **secret2** et éditez-le ainsi :

index.html

```
<html>
<body>
<center>Si vous voyez ce message, vous connaissez mon secret MySQL !</center>
</body>
</html>
```

Ouvrez ensuite le fichier de configuration de mod_auth_mysql **/etc/httpd/conf.d/auth_mysql.conf** et ôtez les **#** devant chacunes des lignes suivantes :

```
<Directory /var/www>
    AuthName "MySQL authenticated zone"
    AuthType Basic

    AuthMYSQLEnable on
    AuthMySQLUser authuser
    AuthMySQLPassword PaSsW0Rd
```

```
    AuthMySQLDB auth
    AuthMySQLUserTable users
    AuthMySQLNameField user_name
    AuthMySQLPasswordField user_passwd

    require valid-user
</Directory>
```

Modifiez ensuite la ligne suivante :

```
<Directory /var/www>
```

en

```
<Directory /www/site1/secret2>
```

Afin que les modifications soient prises en charge par apache, redémarrez le service :

```
[root@centos ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

En utilisant votre navigateur, ouvrez le site http://www.vhostnom.com/secret2/index.html, renseignez l'utilisateur **testuser** et le mot de passe **testpass** puis cliquez sur le bouton **OK**.

Vous devrez découvert le secret MySQL !

mod_ssl

Présentation de SSL

SSL (*Secure Sockets Layers*) est utilisé pour sécuriser des transactions effectuées sur le Web et a été mis au point par :

- Netscape
- MasterCard
- Bank of America
- MCI
- Silicon Graphics

SSL est indépendant du protocole utilisé et agit en tant que couche supplémentaire entre la couche Application et la couche Transport. Il peut être utilisé avec :

- HTTP
- FTP
- POP
- IMAP

Fonctionnement de SSL

Le fonctionnement de SSL suit la procédure suivante :

- Le navigateur demande une page web sécurisée en https,
- Le serveur web émet sa clé publique et son certificat,
- Le navigateur vérifie que le certificat a été émis par une autorité fiable, qu'il est valide et qu'il fait référence au site consulté,
- Le navigateur utilise la clé publique du serveur pour chiffrer une clé symétrique aléatoire, une clé de session, et l'envoie au serveur avec l'URL demandé ainsi que des données HTTP chiffrées,
- Le serveur déchiffre la clé symétrique avec sa clé privée et l'utilise pour récupérer l'URL demandé et les données HTTP,
- Le serveur renvoie le document référencé par l'URL ainsi que les données HTTP chiffrées avec la clé symétrique,
- Le navigateur déchiffre le tout avec la clé symétrique et affiche les informations.

Quand on parle de **SSL**, on parle de **cryptologie**.

Configuration de SSL

Dans le cas où vous souhaitez générer vos propres clés, vous devez d'abord générer une clé privée, nécessaire pour la création d'un **Certificate**

Signing Request. Le CSR doit alors être envoyé à une des sociétés faisant autorité en la matière afin que celle-ci puisse vous retourner votre certificat définitif. Ce service est payant. C'est ce certificat définitif qui est utilisé pour des connexions sécurisées.

Saisissez donc la commande suivante pour générer votre clé privée :

```
[root@centos ~]# openssl genrsa -out www.homeland.net.key 1024
Generating RSA private key, 1024 bit long modulus
.....................................++++++
.............++++++
e is 65537 (0x10001)
```

Générer maintenant votre CSR :

```
[root@centos ~]# openssl req -new -key www.homeland.net.key -out www.homeland.net.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:VAR
Locality Name (eg, city) [Default City]:Toulon
Organization Name (eg, company) [Default Company Ltd]:Linux E-Learning
Organizational Unit Name (eg, section) []:Training
Common Name (eg, your name or your server's hostname) []:centos.fenestros.loc
Email Address []:root@localhost

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

et répondez aux questions qui vous sont posées. Notez bien la réponse à la question **Common Name**. Si vous ne donnez pas votre FQDN, certains navigateurs ne gèreront pas votre certificat correctement. Vous pouvez maintenant envoyé votre CSR à la société que vous avez choisie. Quand votre clé **.crt** vous est retournée, copiez-la, ainsi que votre clé privée dans le répertoire **/etc/pki/tls/certs/**.

Sans passer par un prestataire externe, vous pouvez signer votre CSR avec votre propre clé afin de générer votre certificat :

```
[root@centos ~]# openssl x509 -req -days 365 -in www.homeland.net.csr -signkey www.homeland.net.key -out
www.homeland.net.crt
Signature ok
subject=/C=FR/ST=VAR/L=Toulon/O=Linux E-Learning/OU=Training/CN=centos.fenestros.loc/emailAddress=root@localhost
Getting Private key
```

Cette procédure va générer trois fichiers dont votre clé privée et un certificat – une clé ayant une extension **.crt**.

Il convient ensuite de copier ces deux fichiers dans l'arborescence **/etc/pki/tls** :

```
[root@centos ~]# cp /root/www.homeland.net.key /etc/pki/tls/private/
```

```
[root@centos ~]# cp /root/www.homeland.net.crt /etc/pki/tls/certs/
```

Mise en place des paramètres de sécurité SSL

Créez maintenant le répertoire qui va contenir le site sécurisé :

```
# mkdir /www/ssl
```

Créez le fichier **index.html** pour notre site sécurisé :

```
# vi /www/ssl/index.html
```

Editez le fichier **index.html** ainsi :

index.html

```
<html>
<body>
<center>Accueil du site SSL</center>
</body>
</html>
```

En consultant le contenu du répertoire **/etc/httpd/conf.d**, vous constaterez un fichier **ssl.conf**.

Ouvrez ce fichier et modifiez la ligne suivante :

```
#DocumentRoot "/var/www/html"
```

en :

```
DocumentRoot "/www/ssl"
```

Cette directive indique que la racine du site sécurisé sera **/www/ssl**.

Définissez ensuite les droits d'accès à ce site en ajoutant la section suivante à l'emplacement indiqué :

```
<Files ~ "\.(cgi|shtml|phtml|php3?)$">
    SSLOptions +StdEnvVars
</Files>
# Ajoutez la section suivante
<Directory "/www/ssl">
Order allow,deny
Allow from all
</Directory>
# Fin
<Directory "/var/www/cgi-bin">
    SSLOptions +StdEnvVars
```

```
</Directory>
```

Dernièrement modifiez les deux lignes suivantes :

```
SSLCertificateFile /etc/pki/tls/certs/localhost.crt
SSLCertificateKeyFile /etc/pki/tls/private/localhost.key
```

en :

```
SSLCertificateFile /etc/pki/tls/certs/www.homeland.net.crt
SSLCertificateKeyFile /etc/pki/tls/private/www.homeland.net.key
```

respectivement.

Sauvegardez votre fichier et redémarrez votre serveur apache :

```
[root@centos ~]# service httpd restart
Arrêt de httpd :                                           [  OK  ]
Démarrage de httpd :                                       [  OK  ]
```

Passez en revue les **directives** contenues dans le fichier **ssl.conf** en utilisant le **Manuel en ligne d'Apache**.

Tester Votre Configuration

Pour tester votre serveur apache en mode SSL saisissez la commande suivante :

```
[root@centos ~]# openssl s_client -connect www.homeland.net:443
CONNECTED(00000003)
depth=0 C = FR, ST = VAR, L = Toulon, O = Linux E-Learning, OU = Training, CN = centos.fenestros.loc,
```

```
emailAddress = root@localhost
verify error:num=18:self signed certificate
verify return:1
depth=0 C = FR, ST = VAR, L = Toulon, O = Linux E-Learning, OU = Training, CN = centos.fenestros.loc,
emailAddress = root@localhost
verify return:1
---
Certificate chain
 0 s:/C=FR/ST=VAR/L=Toulon/O=Linux E-Learning/OU=Training/CN=centos.fenestros.loc/emailAddress=root@localhost
   i:/C=FR/ST=VAR/L=Toulon/O=Linux E-Learning/OU=Training/CN=centos.fenestros.loc/emailAddress=root@localhost
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICqTCCAhICCQD2dnaBu4RrlTANBgkqhkiG9w0BAQUFADCBmDELMAkGA1UEBhMC
RlIxDDAKBgNVBAgMA1ZBUjEPMA0GA1UEBwwGVG91bG9uMRkwFwYDVQQKDBBMaW51
eCBFLUxlYXJuaW5nMREwDwYDVQQLDAhUcmFpbmluZzEdMBsGA1UEAwwUY2VudG9z
LmZlbmVzdHJvcy5sb2MxHTAbBgkqhkiG9w0BCQEWDnJvb3RAbG9jYWxob3N0MB4X
DTEzMDcxNTA5MDUzMloXDTE0MDcxNTA5MDUzMlowgZgxCzAJBgNVBAYTAkZSMQww
CgYDVQQIDANWQVIxDzANBgNVBAcMBlRvdWxvbjEZMBcGA1UECgwQTGludXggRS1M
ZWFybmluZzERMA8GA1UECwwIVHJhaW5pbmcxHTAbBgNVBAMMFGNlbnRvcy5mZW5l
c3Ryb3MubG9jMR0wGwYJKoZIhvcNAQkBFg5yb290QGxvY2FsaG9zdDCBnzANBgkq
hkiG9w0BAQEFAAOBjQAwgYkCgYEAsgGH/CeTmW6E+3O2SRf4tVmPAcKKL5MAC3nl
iZvKGE9+QSA1uD9QSxhtTkSaoQbgxfSxTxoZ533eRdwNFgeLbeUqhx8yhOwfzSV5
cNKE3ai4reIOcCMNxjxBWTFj1AH75NHlVH//S7u82GG+pWu+dhC29k+AasxHt2SD
xA9wUv8CAwEAATANBgkqhkiG9w0BAQUFAAOBgQCdy/bJKFYCS9LFvEvqcUNizRjj
GJaCqzjDdaC/rpYSDJgFIdt/UWu+DwGVylpSUsQBuG3ASmGblto3JbX2FXdjRj7N
lcxAwtsna9bAoznc2pmRsoRaUKrohiT5iciK2r67uhNfrfgiCWTTpW7L+NZq0s1I
O5dJLH16BMPaTkTRjg==
-----END CERTIFICATE-----
subject=/C=FR/ST=VAR/L=Toulon/O=Linux E-Learning/OU=Training/CN=centos.fenestros.loc/emailAddress=root@localhost
issuer=/C=FR/ST=VAR/L=Toulon/O=Linux E-Learning/OU=Training/CN=centos.fenestros.loc/emailAddress=root@localhost
---
No client certificate CA names sent
---
```

```
SSL handshake has read 1435 bytes and written 310 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-SHA
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1
    Cipher    : DHE-RSA-AES256-SHA
    Session-ID: 213134CCEB89F17051CDB476CAFB6EDE6173CB0CF74ED4FF219DECC27E1C8B60
    Session-ID-ctx:
    Master-Key: 6A097818500070788FCFC4E9986966628D40F662B8448D24F83FCF1208FF205798D372E5FC6D7754A7C648841668134E
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    TLS session ticket:
    0000 - ab 27 98 fc 21 1c 09 d6-92 b9 b8 0c 52 7c ef 69   .'..!.......R|.i
    0010 - 9a cf df f1 40 46 12 89-60 18 ea 42 72 c9 fa 20   ....@F..`..Br..
    0020 - 2d 91 96 66 b3 3a dc 11-da 3d 8c 11 fc 02 f9 d7   -..f.:...=......
    0030 - e3 96 cd 6f 61 69 e2 01-b0 ab c2 03 a4 e7 65 93   ...oai........e.
    0040 - 5b da 38 dc 66 ad 7c 72-db 55 a4 47 30 c4 eb 91   [.8.f.|r.U.G0...
    0050 - 8d 7e 56 d8 91 ad af 51-59 53 ef 62 3d 52 5c f4   .~V....QYS.b=R\.
    0060 - 4a 96 01 b0 f2 32 08 8b-2d ae b3 9c bf 41 a3 83   J....2..-....A..
    0070 - 96 6b a4 37 f4 f6 4e 9d-43 01 ae 5c 08 01 c3 c0   .k.7..N.C..\....
    0080 - 85 31 ca d5 10 9f 4a 93-96 7a 87 aa 0e aa e7 1c   .1....J..z......
    0090 - b4 e2 65 34 21 19 d9 58-9b 01 f8 b7 06 3c a9 fb   ..e4!..X.....<..
    00a0 - d6 ae 6f 70 8b 23 de 19-e3 c2 88 53 3e 56 a6 19   ..op.#.....S>V..
    00b0 - 89 1d 62 a4 37 e6 d7 9f-d0 b2 08 e0 4a d1 f2 df   ..b.7.......J...

    Start Time: 1373879544
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
```

```
---
```

A la suite de l'affichage, saisissez la ligne suivante :

```
GET / HTTP/1.0 [Entrée] [Entrée]
```

Vous obtiendrez un résultat similaire à celle-ci :

```
GET / HTTP/1.0

HTTP/1.1 200 OK
Date: Mon, 15 Jul 2013 09:13:16 GMT
Server: Apache/2.2.15 (CentOS)
Last-Modified: Mon, 15 Jul 2013 09:08:02 GMT
ETag: "7576-43-4e1893297286c"
Accept-Ranges: bytes
Content-Length: 67
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
<body>
<center>Accueil du site SSL</center>
</body>
</html>
closed
```

Notez qu'il y a génération d'erreurs. Ceci est normal.

Procédez maintenant au test en utilisant votre navigateur en saisissant l'adresse :

```
https://www.homeland.net
```

Il est normal que la vérification échoue car dans ce cas il s'agit du certificat de test.

LAB #25 - Sécuriser Postfix

Cyrus SASL

Présentation

Cyrus SASL (**S**imple **A**uthentification and **S**ecurity **L**ayer) est l'implentation **SASL** de l'**Université de Carnegie Mellon**. SASL est un **Framework** d'authentification décrit dans la **RFC 2222**.

SASL est organisé en trois couches - **l'interface d'authentification**, **le mécanisme** et **la méthode** :

- l'**interface d'authentification** concerne la phase de communication entre le client et le serveur,
  - le client se connecte au serveur,
  - les serveur annonce ses fonctionnalités,
  - le client détecte l'option d'authentification et la liste des mécanismes possibles,
  - le client choisit un **mécanisme** et génère une chaine de caractères en fonction du mécanisme choisi :
    - **anonyme** - accès anonymes,
    - **texte en clair** - de type **PLAIN** ou **LOGIN**, il fonctionne en encodant le nom d'utilisateur et le mot de passe en **base64**. La version LOGIN est utilisée pour des clients de messagerie non conformes à la RFC tels Outlook™ et Outlook Express™. Le codage **base64** n'est pas chiffré et necéssite l'utilisation de **TLS** (**T**ransport **L**ayer **S**ecurity).,
    - **secret partagé** - il fonctionne selon le principe de secret partagé en utilisant **CRAM-MD5** ou **DIGEST-MD5**,
  - le client envoie la chaîne au serveur en tant que reqûete d'authentification,
  - le serveur transmet la reqûete à SASL,
  - SASL utilise une **méthode** pour contacter la base d'authentification en fonction du **mécanisme** en utilisant :

        - **rimap** - SASL se connecte à un serveur IMAP en utilisant coordonnées de l'utilisateur. Si la connexion aboutit SASL valide l'authentification,
        - **ldap** - SASL se connecte à un serveur LDAP en utilisant coordonnées de l'utilisateur. Si la connexion aboutit SASL valide l'authentification,
        - **kerberos** - vérifie le ticker kerberos du client pour vérifier l'authentification,
        - **getpwent/shadow** - accède à /etc/passwd pour vérifier l'authentification,
        - **pam** - utilise un module PAM pour vérifier l'authentification,
        - **sasldb** - consulte la base de données **saslbd2** pour vérifier l'authentification,
        - **sql** - utilise une reqûete SQL auprès de MySQL, SQLite ou PostgreSQL pour vérifier l'authentification,
    - si l'authentification est correcte SASL informe le serveur qui permet la demande du client,.
    - si l'authentification est incorrecte SASL informe le serveur qui informe le client et refuse la demande du client.

SASL propose trois services pour effectuer les procédures décrites ci-dessus :

- **saslauthd** - un service autonome exécuté sous l'identité de root qui peut utiliser le mécanisme texte en clair (PLAIN et LOGIN),
- **auxprop** - un service faisant partie de l'architecture de Cyrus capable d'utiliser les mécanismes texte en clair (PLAIN et LOGIN) et secret partagé (CRAM-MD5 et DIGEST-MD5,
- **authdaemond** - un service écrit pour utiliser le daemon authdaemond du serveur **Courier** qui peut utiliser le mécanisme texte en clair (PLAIN et LOGIN).

Passez en revue la **totalité** des liens ci-dessus. Lisez chaque article/page attentivement.

La configuration de SASL se trouve dans le fichier **/etc/sasl/smtpd.conf** :

```
[root@mail ~]# cat /etc/sasl2/smtpd.conf
pwcheck_method: saslauthd
mech_list: plain login
```

A part le nom du service de vérification du mot de passe et les mécanismes à utiliser, il est aussi possible de trouver la directive **log_level**. Cette directive prend comme valeur un chiffre :

Chiffre	Description
0	Aucune journalisation
1	Journalisation des erreurs inhabituelles
2	Journalisation des échecs d'authentification
3	Journalisation des avertissements inhabituelles
4	Niveau 3 en vv
5	Niveau 3 en vvv
6	Journalisation des événements concernant des protocoles internes de SASL
7	Journalisation des événements concernant des protocoles internes de SASL et mots de passe

La valeur par défaut de la directive **log_level** est de **1**.

La configuration de saslauthd se trouve dans le fichier **/etc/sysconfig/saslauthd** :

/etc/sysconfig/saslauthd

```
# Directory in which to place saslauthd's listening socket, pid file, and so
# on.  This directory must already exist.
SOCKETDIR=/var/run/saslauthd

# Mechanism to use when checking passwords.  Run "saslauthd -v" to get a list
# of which mechanism your installation was compiled with the ablity to use.
MECH=pam

# Options sent to the saslauthd. If the MECH is other than "pam" uncomment the next line.
# DAEMONOPTS=--user saslauth

# Additional flags to pass to saslauthd on the command line.  See saslauthd(8)
# for the list of accepted flags.
FLAGS=
```

Les méchanisms de vérification des mots de passe supportés par saslauthd peuvent être visualisés en utilisant l'option **-v** de la commande **saslauthd** :

```
[root@mail ~]# saslauthd -v
saslauthd 2.1.23
authentication mechanisms: getpwent kerberos5 pam rimap shadow ldap
```

Configuration de Postfix

Vérifiez que Cyrus-sasl est installé :

```
[root@mail ~]# rpm -qa | grep sasl
cyrus-sasl-gssapi-2.1.23-13.el6_3.1.i686
cyrus-sasl-plain-2.1.23-13.el6_3.1.i686
cyrus-sasl-lib-2.1.23-13.el6_3.1.i686
cyrus-sasl-2.1.23-13.el6_3.1.i686
```

Sachez que plusieurs paquets supplémentaies sont disponibles en fonction de la méthode :

```
[root@mail ~]# yum search cyrus-sasl
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * atomic: atomic.mirror.uber.com.au
 * base: centos.mirror.crcrepairs.com
 * epel: epel.mirrors.ovh.net
 * extras: centos.mirror.crcrepairs.com
 * rpmforge: apt.sw.be
 * updates: centos.crazyfrogs.org
ox-backend
| 1.3 kB     00:00
ox-frontend
| 1.3 kB     00:00
ox-usm
```

```
| 1.2 kB     00:00
================================================================================ N/S Matched: cyrus-sasl
================================================================================
cyrus-sasl.i686 : The Cyrus SASL library
cyrus-sasl-devel.i686 : Files needed for developing applications with Cyrus SASL
cyrus-sasl-gssapi.i686 : GSSAPI authentication support for Cyrus SASL
cyrus-sasl-ldap.i686 : LDAP auxprop support for Cyrus SASL
cyrus-sasl-lib.i686 : Shared libraries needed by applications which use Cyrus SASL
cyrus-sasl-md5.i686 : CRAM-MD5 and DIGEST-MD5 authentication support for Cyrus SASL
cyrus-sasl-ntlm.i686 : NTLM authentication support for Cyrus SASL
cyrus-sasl-plain.i686 : PLAIN and LOGIN authentication support for Cyrus SASL
cyrus-sasl-sql.i686 : SQL auxprop support for Cyrus SASL

  Name and summary matches only, use "search all" for everything.
```

Dans le cas de Postfix, le serveur qui prend en charge les reqûetes d'authentification est **smtpd** avec la fonction **SMTP AUTH**. Vérifiez que postfix a été installé avec le support pour **SMTP AUTH** :

```
[root@mail ~]# ldd /usr/libexec/postfix/smtpd | grep libsasl
    libsasl2.so.2 => /usr/lib/libsasl2.so.2 (0x00b11000)
```

La présence de la bibliothèque **libsasl2** indique que postfix a été installé avec le support pour SASL.

Ajoutez ensuite les lignes suivantes au fichier **/etc/postfix/main.cf** :

```
...
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
```

```
                                    reject_non_fqdn_hostname,
                                    reject_non_fqdn_sender,
                                    reject_non_fqdn_recipient,
                                    reject_unknown_sender_domain,
                                    reject_unknown_recipient_domain,
                                    reject_unauth_pipelining,
                                    reject_rbl_client zen.spamhaus.org,
                                    reject_rbl_client bl.spamcop.net,
                                    reject_rbl_client dnsbl.njabl.org,
                                    reject_rbl_client dnsbl.sorbs.net,
                                    permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = linuxelearning.info
smtpd_helo_required = yes
```

Pour plus d'informations concernant les directives, consultez **cette page**.

Vous obtiendrez le résultat suivant :

/etc/postfix/main.cf

```
myhostname = mail.linuxelearning.info
mydomain= linuxelearning.info
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mail_spool_directory = /var/spool/mail
mailbox_command = /usr/bin/procmail -Y -a $DOMAIN
```

```
smtpd_banner = $myhostname ESMTP $mail_name ($mail_version)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
relayhost = smtp.bbox.fr
mail_owner = postfix
inet_interfaces = all
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
#unknown_local_recipient_reject_code = 550
unknown_local_recipient_reject_code = 450
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
         xxgdb $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
setgid_group = postdrop
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.6.6/samples
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
                                  reject_non_fqdn_hostname,
                                  reject_non_fqdn_sender,
                                  reject_non_fqdn_recipient,
                                  reject_unknown_sender_domain,
```

```
                                    reject_unknown_recipient_domain,
                                    reject_unauth_pipelining,
                                    reject_rbl_client zen.spamhaus.org,
                                    reject_rbl_client bl.spamcop.net,
                                    reject_rbl_client dnsbl.njabl.org,
                                    reject_rbl_client dnsbl.sorbs.net,
                                    permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = linuxelearning.info
smtpd_helo_required = yes
```

Les directives ajoutées dans l'exemple ci-dessus sont :

Directive	**Description**
smtpd_sasl_application_name	Nom de l'application utilisée pour l'initialisation du serveur SASL. Ceci contrôle le nom du fichier de configuration SASL.
smtpd_recipient_restrictions	Restrictions d'accès que le serveur SMTP de Postfix applique dans le contexte d'une commande RCPT TO.
smtpd_client_restrictions	Restrictions d'accès optionelles du serveur SMTP pour les requêtes de connexion au service SMTP.
smtp_sasl_mechanism_filter	La version spécifique LMTP du paramètre smtp_sasl_mechanism_filter.
smtpd_sasl_auth_enable	Active l'authentification SASL dans le serveur SMTP de Postfix.
smtpd_sasl_security_options	Options de sécurité SASL.
broken_sasl_auth_clients	Active l'interoperabilité avec les clients SMTP qui implémentent une version obsolete de la commande AUTH.
smtpd_sasl_local_domain	Nom de royaume d'authentification SASL local.
smtpd_helo_required	Impose au client SMTP de démarrer la session SMTP par une commande HELO ou EHLO.

smtpd_recipient_restrictions

Restriction	**Description**
permit_sasl_authenticated	Autorise la requête lorsque le client est authentifié avec succès via le protocole AUTH.

Restriction	Description
permit_mynetworks	Autorise la requête si l'adresse IP du client correspond à l'une des adresses ou l'un des réseaux listé dans $mynetworks.
reject_invalid_hostname	Rejette les requêtes lorsque la syntaxe du nom de machine passé avec HELO ou EHLO est invalide.
reject_non_fqdn_hostname	Rejette la requête lorsque le nom de domaine n'est pas sous la forme pleinement qualifiée requise par la RFC.
reject_non_fqdn_sender	Rejette la requête lorsque l'adresse MAIL FROM n'est pas sous la forme pleinement qualifiée requise par la RFC.
reject_non_fqdn_recipient	Rejette la requête lorsque l'adresse RCPT TO n'est pas de forme pleinement qualifiée.
reject_unknown_sender_domain	Rejette la requête lorsque Postfix n'est pas la destination finale de l'adresse d'expédition et que l'adresse MAIL FROM n'a pas d'enregistrement DNS A ou MX correspondant, ou lorsque cet enregistrement MX est malformé comme un nom MX de longueur nulle.
reject_unknown_recipient_domain	Rejette la requête lorsque l'adresse RCPT TO ne correspond à aucun enregistrement DNS de type A ou MX et Postfix n'est pas la destination finale de l'adresse de destination.
reject_unauth_pipelining	Rejette la requête lorsque le client envoie des commandes SMTP en dehors des moments où il y est autorisé ou lorsque le client envoie des commandes SMTP avant de savoir que Postfix supporte la canalisation des commandes SMTP (pipelining).
reject_rbl_client	Rejette la requête lorsque la résolution inverse de l'adresse réseau du client correspond à un enregistrement de type A du domaine zen.spamhaus.org, bl.spamcop.net, dnsbl.njabl.org ou dnsbl.sorbs.net.
permit	Autorise la requête. C'est la politique par défaut.

smtpd_client_restrictions

Restriction	Description
permit_sasl_authenticated	Autorise la requête lorsque le client est authentifié avec succès via le protocole AUTH.
permit_mynetworks	Autorise la requête si l'adresse IP du client correspond à l'une des adresses ou l'un des réseaux listé dans $mynetworks.
reject_unauth_destination	Rejette la requête sauf si Postfix transfert le message ou Postfix est la destination finale.

smtpd_sasl_security_options

Option	Description
noplaintext	Interdit les méthodes utilisant les mots de passe en clair.
noactive	Interdit les méthodes sujettes à une attaque active (sans dictionnaire).
nodictionary	Interdit les méthodes sujettes à une attaque passive (par dictionnaire).
noanonymous	Interdit les méthodes qui autorisent l'authentification anonyme.

Option	Description
mutual_auth	N'autorise que les méthodes fournissant une authentification mutuelle.

Rechargez la configuration de postfix :

```
[root@centos6 ~]# service postfix reload
Rechargement de postfix :                                  [  OK  ]
```

Pour tester l'authentification, vous devez envoyer un nom d'utilisateur et un mot de passe encodés en **base64**. Créez donc une chaîne de caractères encodés en base64 grâce à Perl en utilisant le format **utilisateur\0utilisateur\0motdepasse** :

```
[root@mail ~]# perl -MMIME::Base64 -e 'print encode_base64("trainee\0trainee\0trainee");'
dHJhaW5lZQB0cmFpbmVlAHRyYWluZWU=
```

Notez que les caractères **\0** séparent les champs et que le nom d'utilisateur est repété deux fois.

Activez le service **saslauthd** :

```
[root@mail ~]# chkconfig --list saslauthd
saslauthd       0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
[root@mail ~]# chkconfig --level 2345 saslauthd on
[root@mail ~]# chkconfig --list saslauthd
saslauthd       0:arrêt    1:arrêt    2:marche    3:marche    4:marche    5:marche    6:arrêt
```

Démarrez maintenant le service **saslauthd** :

```
[root@mail ~]# service saslauthd start
Démarrage de saslauthd :                                   [  OK  ]
```

Connectez-vous maintenant au serveur postfix sur le port 25 :

```
[root@mail ~]# telnet localhost 25
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.linuxelearning.info ESMTP Postfix (2.6.6)
EHLO me
250-mail.linuxelearning.info
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH PLAIN dHJhaW5lZQB0cmFpbmVlAHRyYWluZWU=
235 2.7.0 Authentication successful
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

Notez l'utilisation de la commande **EHLO**. EHLO est la version *Enhanced* (ESMTP) de **HELO**. Le serveur répond ensuite avec les extensions ESMTP supportées. Dans le cas de l'exemple ci-dessus, on peut noter la présence des deux lignes **250-AUTH LOGIN PLAIN** et **250-AUTH=LOGIN PLAIN** qui indique que le serveur supporte le mécanisme AUTH. Notez aussi l'utilisation de la commande AUTH PLAIN qui informe le serveur que les coordonnées de connexion vont être transmises sous forme d'un couple nom d'utilisateur/mot de passe encodés en **base64**.

Les autres extensions supportées dans l'exemple ci-dessus sont :

Extension	**Description**
250-PIPELINING	Service qui permet au client d'envoyer une nouvelle requête sans attendre la réponse à la requête précédente.
250-SIZE 10240000	La taille maximale en octets d'un message

Extension	Description
250-VRFY	Service qui permet d'interroger directement le serveur SMTP pour savoir si une adresse existe.
250-ETRN	Service qui permet au serveur mail de demander au serveur mail du FAI de livrer ses messages.
250-ENHANCEDSTATUSCODES	Compatible **Enhanced Status Codes Registry**
250-8BITMIME	Service 8bit-MIMEtransport.
250 DSN	Service Delivery Status Notification (Accusés de réception).

TLS

Rappel : le codage **base64** n'est pas chiffré et necéssite l'utilisation de **TLS** (**T**ransport **L**ayer **S**ecurity).

Commencez par exécuter le script CA qui se trouve dans **/etc/pki/tls/misc** :

```
[root@mail ~]# cd /etc/pki/tls/misc
[root@mail misc]# ls -l
total 24
-rwxr-xr-x. 1 root root 5178  8 avril 04:36 CA
-rwxr-xr-x. 1 root root  119  8 avril 04:36 c_hash
-rwxr-xr-x. 1 root root  152  8 avril 04:36 c_info
-rwxr-xr-x. 1 root root  112  8 avril 04:36 c_issuer
-rwxr-xr-x. 1 root root  110  8 avril 04:36 c_name
[root@mail misc]# ./CA -newca
CA certificate filename (or enter to create)

Making CA certificate ...
Generating a 2048 bit RSA private key
.....................................................................................+++
..+++
writing new private key to '/etc/pki/CA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:fenestros
```

```
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:VAR
Locality Name (eg, city) [Default City]:Toulon
Organization Name (eg, company) [Default Company Ltd]:Linux E-Learning
Organizational Unit Name (eg, section) []:Formation
Common Name (eg, your name or your server's hostname) []:linuxelearning.info
Email Address []:infos@linuxelearning.info

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:secret
An optional company name []:
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/./cakey.pem:fenestros
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            d3:df:b4:68:69:a8:15:27
        Validity
            Not Before: May  8 10:30:15 2014 GMT
            Not After : May  7 10:30:15 2017 GMT
        Subject:
            countryName               = FR
            stateOrProvinceName       = VAR
            organizationName          = Linux E-Learning
```

```
            organizationalUnitName    = Formation
            commonName                = linuxelearning.info
            emailAddress              = infos@linuxelearning.info
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                9E:CB:4E:E8:8F:43:72:ED:F4:54:8C:4A:F3:5B:5B:CC:A1:26:4F:CD
            X509v3 Authority Key Identifier:
                keyid:9E:CB:4E:E8:8F:43:72:ED:F4:54:8C:4A:F3:5B:5B:CC:A1:26:4F:CD

            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until May  7 10:30:15 2017 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
```

Vous obtiendrez donc deux fichiers - **cacert.pem** et **cakey.pem** :

```
[root@mail misc]# ls /etc/pki/CA
cacert.pem  careq.pem  certs  crl  index.txt  index.txt.attr  index.txt.old  newcerts  private  serial
[root@mail misc]# ls /etc/pki/CA/private
cakey.pem
```

Vous devez générer maintenant une clef privée ainsi qu'un **Certificate Signing Request** pour le serveur mail. Le **CSR (Certificate Signing Request)** doit alors être envoyé à une des sociétés faisant autorité en la matière afin que celle-ci puisse vous retourner votre certificat définitif. Ce service est payant. C'est ce certificat définitif qui est utilisé pour des connexions sécurisées.

```
[root@mail misc]# openssl req -new -nodes -keyout lel_clef.pem -out lel_req.pem
Generating a 2048 bit RSA private key
....+++
.....................................................................+++
writing new private key to 'lel_clef.pem'
-----
You are about to be asked to enter information that will be incorporated
```

```
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:FR
State or Province Name (full name) []:VAR
Locality Name (eg, city) [Default City]:Toulon
Organization Name (eg, company) [Default Company Ltd]:Linux E-Learning
Organizational Unit Name (eg, section) []:Formation
Common Name (eg, your name or your server's hostname) []:mail.linuxelearning.info
Email Address []:infos@linuxelearning.info

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Vous obtiendrez deux fichiers - **lel_clef.pem** et **lel_req.pem** :

```
[root@mail misc]# ls
CA  c_hash  c_info  c_issuer  c_name  lel_clef.pem  lel_req.pem
```

Vous pouvez maintenant envoyé votre **CSR (Certificate Signing Request)**, **lel_req.pem**, à la société que vous avez choisie. Quand votre certificat **.crt** vous est retourné, copiez-le, ainsi que votre clé privée dans le répertoire **/etc/postfix/ssl**.

Sans passer par un prestataire externe, vous pouvez signer votre **CSR (Certificate Signing Request)** avec votre propre clef afin de générer votre certificat :

```
[root@mail misc]# openssl ca -out lel_cert.pem -infiles lel_req.pem
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for /etc/pki/CA/private/cakey.pem:
Check that the request matches the signature
```

```
Signature ok
Certificate Details:
        Serial Number:
            d3:df:b4:68:69:a8:15:28
        Validity
            Not Before: May  8 10:48:31 2014 GMT
            Not After : May  8 10:48:31 2015 GMT
        Subject:
            countryName               = FR
            stateOrProvinceName       = VAR
            organizationName          = Linux E-Learning
            organizationalUnitName    = Formation
            commonName                = mail.linuxelearning.info
            emailAddress              = infos@linuxelearning.info
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                84:8E:5F:F1:C3:21:78:E3:FB:12:CD:5B:DE:5C:56:77:28:9E:FA:31
            X509v3 Authority Key Identifier:
                keyid:9E:CB:4E:E8:8F:43:72:ED:F4:54:8C:4A:F3:5B:5B:CC:A1:26:4F:CD

Certificate is to be certified until May  8 10:48:31 2015 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Notez que le **commonName** est différent ! Dans le cas contraire la base de données ne sera pas mise à jour et une erreur sera jetée.

Il convient ensuite de copier les fichiers lel_cert.pem, lel_clef.pem et cacert.pem dans le répertoire **/etc/postfix** puis de modifier les permissions :

```
[root@mail misc]# cp lel_cert.pem lel_clef.pem /etc/postfix
[root@mail misc]# cp /etc/pki/CA/cacert.pem /etc/postfix
[root@mail misc]# chmod 644 /etc/postfix/lel_cert.pem /etc/postfix/cacert.pem
[root@mail misc]# chmod 400 /etc/postfix/lel_clef.pem
```

Pour activer **TLS** vous allez modifier votre fichier **/etc/postfix/main.cf** en y ajoutant les lignes suivantes :

```
...
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_tls_sesson_cache
smtp_tls_security_level = may
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_sesson_cache
smtpd_tls_cert_file = /etc/postfix/lel_cert.pem
smtpd_tls_key_file = /etc/postfix/lel_clef.pem
smtpd_tls_received_header = yes
tls_random_source = dev:/dev/urandom
smtpd_tls_security_level = may
smtpd_tls_loglevel = 2
smtpd_use_tls = no
smtpd_tls_ask_ccert = no
```

Vous obtiendrez un résultat similaire à celui-ci :

/etc/postfix/main.cf

```
myhostname = mail.linuxelearning.info
mydomain= linuxelearning.info
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mail_spool_directory = /var/spool/mail
mailbox_command = /usr/bin/procmail -Y -a $DOMAIN
```

```
smtpd_banner = $myhostname ESMTP $mail_name ($mail_version)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
relayhost = smtp.bbox.fr
mail_owner = postfix
#inet_interfaces = localhost
inet_interfaces = all
#mydestination = $myhostname, localhost.$mydomain, localhost
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
#unknown_local_recipient_reject_code = 550
unknown_local_recipient_reject_code = 450
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
debug_peer_level = 2
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
         xxgdb $daemon_directory/$process_name $process_id & sleep 5
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
setgid_group = postdrop
html_directory = no
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.6.6/samples
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
queue_directory = /var/spool/postfix
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
```

```
                                    reject_non_fqdn_hostname,
                                    reject_non_fqdn_sender,
                                    reject_non_fqdn_recipient,
                                    reject_unknown_sender_domain,
                                    reject_unknown_recipient_domain,
                                    reject_unauth_pipelining,
                                    reject_rbl_client zen.spamhaus.org,
                                    reject_rbl_client bl.spamcop.net,
                                    reject_rbl_client dnsbl.njabl.org,
                                    reject_rbl_client dnsbl.sorbs.net,
                                    permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = linuxelearning.info
smtpd_helo_required             = yes
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_tls_sesson_cache
smtp_tls_security_level = may
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_sesson_cache
smtpd_tls_cert_file = /etc/postfix/lel_cert.pem
smtpd_tls_key_file = /etc/postfix/lel_clef.pem
smtpd_tls_received_header = yes
tls_random_source = dev:/dev/urandom
smtpd_tls_security_level = may
smtpd_tls_loglevel = 2
smtpd_tls_ask_ccert = no
```

Les directives ajoutées dans l'exemple ci-dessus sont :

Directive	Description
smtpd_tls_CAfile	Fichier contenant le certificat de l'autorité de certification de laquelle est issu le certificat du serveur SMTP de Postfix.
smtpd_tls_session_cache_database	Nom du fichier contenant le cache optionnel des sessions TLS du serveur SMTP de Postfix.
smtpd_tls_cert_file	Fichier contenant le certificat RSA du serveur SMTP de Postfix au format PEM.
smtpd_tls_key_file	Fichier contenat la clef privée RSA du serveur SMTP de Postfix au format PEM.
smtpd_tls_received_header	Requiert que le serveur SMTP de Postfix produise des en-têtes de message Received: qui incluent les informations à propos du protocole et du chiffrement utilisé ainsi que les champs CommonName des certificats client et de l'autorité dont il est issu.
tls_random_source	Source externe d'entropie pour le gestionnaire tlsmgr(8) du pool de générateurs en mémoire de nombres peudo-aléatoires (pseudo random number generator PRNG).
smtpd_tls_loglevel	Active l'enregistrement additionnel de l'activité TLS du serveur SMTP de Postfix. La valeur de deux enregistre les informations concernant la négociation et les certificats ainsi que les niveaux durant la négociation TLS.
smtpd_tls_ask_ccert	Demande au client SMTP distant un certificat client.

Pour plus d'informations concernant les directives **smtp_tls_security_level** et **smtpd_tls_security_level**, consultez **cette page**.

Rechargez la configuration de postfix :

```
[root@mail ~]# service postfix reload
Rechargement de postfix :                                  [  OK  ]
```

Testez maintenant le serveur postfix afin de savoir si celui-ci a pris en compte **TLS** :

```
[root@mail misc]# cd ~
[root@mail ~]# openssl s_client -starttls smtp -connect mail.linuxelearning.info:25
CONNECTED(00000003)
depth=1 C = FR, ST = VAR, O = Linux E-Learning, OU = Formation, CN = linuxelearning.info, emailAddress =
infos@linuxelearning.info
verify error:num=19:self signed certificate in certificate chain
verify return:0
```

```
---
Certificate chain
 0 s:/C=FR/ST=VAR/O=Linux E-
Learning/OU=Formation/CN=mail.linuxelearning.info/emailAddress=infos@linuxelearning.info
   i:/C=FR/ST=VAR/O=Linux E-Learning/OU=Formation/CN=linuxelearning.info/emailAddress=infos@linuxelearning.info
 1 s:/C=FR/ST=VAR/O=Linux E-Learning/OU=Formation/CN=linuxelearning.info/emailAddress=infos@linuxelearning.info
   i:/C=FR/ST=VAR/O=Linux E-Learning/OU=Formation/CN=linuxelearning.info/emailAddress=infos@linuxelearning.info
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIEKTCCAxGgAwIBAgIJANPftGhpqBUoMA0GCSqGSIb3DQEBBQUAMIGSMQswCQYD
VQQGEwJGUjEMMAoGA1UECAwDVkFSMRkwFwYDVQQKDBBMaW51eCBFLUxlYXJuaW5n
MRIwEAYDVQQLDAlGb3JtYXRpb24xHDAaBgNVBAMME2xpbnV4ZWxlYXJuaW5nLmlu
Zm8xKDAmBgkqhkiG9w0BCQEWGWluZm9zQGxpbnV4ZWxlYXJuaW5nLmluZm8wHhcN
MTQwNTA4MTA0ODMxWhcNMTUwNTA4MTA0ODMxWjCBlzELMAkGA1UEBhMCRlIxDDAK
BgNVBAgMA1ZBUjEZMBcGA1UECgwQTGludXggRS1MZWFybmluZzESMBAGA1UECwwJ
Rm9ybWF0aW9uMSEwHwYDVQQDDBhtYWlsLmxpbnV4ZWxlYXJuaW5nLmluZm8xKDAm
BgkqhkiG9w0BCQEWGWluZm9zQGxpbnV4ZWxlYXJuaW5nLmluZm8wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDB0/IU1NdxcCAOPodxDpcK/vpOBAsrcPWB
6KHXhbz5VtCfWdVm4nbQlidhTQQRFygj9udpxe0/OG//MeV+/wKYwHlLH+57jCRX
GQ/ge+5h6UzkOGGZ16ABvBNEHTloPGZsWObkYuwzYPV55fpt2OYsT58F6WQNxhU5
UWNKcA3uAWJ5GwGLh5emihSzo6g07LkZe65qCDsCt0Gk/Icruo8EgVn+OGQCCGRI
Kapxo9lC3bhVKLKc4Ui6IMoAB7EGcdMRlurpooImDu4aNAJKEQgSj691jerJe1KS
2a2rjbtkzpuOzbnRy1D0w5DJTSizDPfYJkrVqW33xt5yH7zzgL6VAgMBAAGjezB5
MAkGA1UdEwQCMAAwLAYJYIZIAYb4QgENBB8WHU9wZW5TU0wgR2VuZXJhdGVkIENl
cnRpZmljYXRlMB0GA1UdDgQWBBSEjl/xwyF44/sSzVveXFZ3KJ76MTAfBgNVHSME
GDAWgBSey07oj0Ny7fRUjErzW1vMoSZPzTANBgkqhkiG9w0BAQUFAAOCAQEAbzRa
vUpUCoyEDUxeWjwUURPvmoH2fC7isU8t28xFyDm3QtC8Od3bhedkAtEWGPmSL7W8
79Spwl479X33bF44iVAFTH6S6915Wnq8Brg0jvc2xGAhPIyrYy+t3zyq2A5xH89I
OFtQg+qVvi+ZVuOI+B6UT1W2fRCysSH08t/3RgQYdJ/icA7oDHApz0HahZ0PGNTH
pAhy2VscSzlNrRFucecs8FvqE6SnihNCwybdIfxHTc8btLEZZ+BhtMoDxb9YcLhv
vBKYtldZGMrs+eXyM+RLyxIngJQGm9yNvqADgcJUNTOKVlVOoSbURkj0I5e7qWDt
UCtwuI+HEIj1HcbwlQ==
-----END CERTIFICATE-----
```

```
subject=/C=FR/ST=VAR/O=Linux E-
Learning/OU=Formation/CN=mail.linuxelearning.info/emailAddress=infos@linuxelearning.info
issuer=/C=FR/ST=VAR/O=Linux E-Learning/OU=Formation/CN=linuxelearning.info/emailAddress=infos@linuxelearning.info
---
No client certificate CA names sent
---
SSL handshake has read 3211 bytes and written 488 bytes
---
New, TLSv1/SSLv3, Cipher is DHE-RSA-AES256-GCM-SHA384
Server public key is 2048 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : DHE-RSA-AES256-GCM-SHA384
    Session-ID: 07A10D85C1196942C4B5B458BD45D4FE181A7AA3F4C40E5CC2DF886F0796936F
    Session-ID-ctx:
    Master-Key: 38C5167EE3BD3D4C5A9E207B07A7DC8A71BDB283263FBB71E3141873EAC9887590840BAEEA529D3C32AA5E2B6FD0CCC3
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    TLS session ticket lifetime hint: 3600 (seconds)
    TLS session ticket:
    0000 - ef 1e fc 1f 64 6d 57 01-d3 1f 77 8a 46 5b 21 32   ....dmW...w.F[!2
    0010 - ff ab 97 c9 9f 7b 53 fd-24 50 b2 66 e5 2b af f0   .....{S.$P.f.+..
    0020 - 6c 0f 68 b3 a3 a4 16 a4-c3 d7 86 5c 67 dc ec 5e   l.h........\g..^
    0030 - 56 95 69 d1 7c 62 6a 77-9a 0d 67 cb 3b a5 36 48   V.i.|bjw..g.;.6H
    0040 - ee 35 10 34 ac 01 66 b2-82 a1 24 23 0a 47 a0 d2   .5.4..f...$#.G..
    0050 - a8 9b 4a 8a 21 e2 f5 c8-79 62 bd 81 ae c1 27 ba   ..J.!...yb....'.
    0060 - 2f 10 c5 c8 67 06 16 57-f7 35 a2 c7 ff 7b 75 16   /...g..W.5...{u.
    0070 - 08 8a ae 95 da 92 ba da-2a 83 b1 8a 56 10 64 a3   ........*...V.d.
    0080 - 20 6a 5a c6 40 ce 28 ad-16 c7 78 5c 2b 24 92 00    jZ.@.(...x\+$..
```

```
    0090 - 04 95 5d 69 be 39 50 8d-6b 37 f4 ba 6a ff ce 5b   ..]i.9P.k7..j..[

    Start Time: 1399546992
    Timeout   : 300 (sec)
    Verify return code: 19 (self signed certificate in certificate chain)
---
250 DSN
QUIT
DONE
```

Notez la présence de l'erreur 19 (self signed certificate in certificate chain).

Afin de configurer Postfix pour écouter sur les ports **tcp/465** et **tcp/587**, il convient d'ajouter les deux ligne suivantes au fichier **/etc/postfix/master.cf** :

```
...
# Port 465 pour SSL
465     inet    n       -       n       -       -       smtpd
# Port 587 pour TLS
587     inet    n       -       n       -       -       smtpd
...
```

Vous obtiendrez donc le résultat suivant :

/etc/postfix/master.cf

```
#
# Postfix master process configuration file.  For details on the format
# of the file, see the master(5) manual page (command: "man 5 master").
#
# Do not forget to execute "postfix reload" after editing this file.
```

```
#
# ==========================================================================
# service type  private unpriv  chroot  wakeup  maxproc command + args
#               (yes)   (yes)   (yes)   (never) (100)
# ==========================================================================
smtp      inet  n       -       n       -       -       smtpd
# Port 465 pour SSL
465 inet    n    -    n    -    -    smtpd
# Port 587 pour TLS
587 inet    n    -    n    -    -    smtpd
#submission inet n       -       n       -       -       smtpd
#  -o smtpd_tls_security_level=encrypt
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#smtps     inet  n       -       n       -       -       smtpd
#  -o smtpd_tls_wrappermode=yes
#  -o smtpd_sasl_auth_enable=yes
#  -o smtpd_client_restrictions=permit_sasl_authenticated,reject
#  -o milter_macro_daemon_name=ORIGINATING
#628      inet  n       -       n       -       -       qmqpd
pickup    fifo  n       -       n       60      1       pickup
cleanup   unix  n       -       n       -       0       cleanup
qmgr      fifo  n       -       n       300     1       qmgr
#qmgr     fifo  n       -       n       300     1       oqmgr
tlsmgr    unix  -       -       n       1000?   1       tlsmgr
rewrite   unix  -       -       n       -       -       trivial-rewrite
bounce    unix  -       -       n       -       0       bounce
defer     unix  -       -       n       -       0       bounce
trace     unix  -       -       n       -       0       bounce
verify    unix  -       -       n       -       1       verify
flush     unix  n       -       n       1000?   0       flush
proxymap  unix  -       -       n       -       -       proxymap
proxywrite unix -       -       n       -       1       proxymap
```

```
smtp      unix  -       -       n       -       -       smtp
# When relaying mail as backup MX, disable fallback_relay to avoid MX loops
relay     unix  -       -       n       -       -       smtp
    -o smtp_fallback_relay=
#       -o smtp_helo_timeout=5 -o smtp_connect_timeout=5
showq     unix  n       -       n       -       -       showq
error     unix  -       -       n       -       -       error
retry     unix  -       -       n       -       -       error
discard   unix  -       -       n       -       -       discard
local     unix  -       n       n       -       -       local
virtual   unix  -       n       n       -       -       virtual
lmtp      unix  -       -       n       -       -       lmtp
anvil     unix  -       -       n       -       1       anvil
scache    unix  -       -       n       -       1       scache
#
# ====================================================================
# Interfaces to non-Postfix software. Be sure to examine the manual
# pages of the non-Postfix software to find out what options it wants.
#
# Many of the following services use the Postfix pipe(8) delivery
# agent.  See the pipe(8) man page for information about ${recipient}
# and other message envelope options.
# ====================================================================
#
# maildrop. See the Postfix MAILDROP_README file for details.
# Also specify in main.cf: maildrop_destination_recipient_limit=1
#
#maildrop  unix  -       n       n       -       -       pipe
#  flags=DRhu user=vmail argv=/usr/local/bin/maildrop -d ${recipient}
#
# ====================================================================
#
# The Cyrus deliver program has changed incompatibly, multiple times.
#
```

```
#old-cyrus unix  -       n       n       -       -       pipe
#  flags=R user=cyrus argv=/usr/lib/cyrus-imapd/deliver -e -m ${extension} ${user}
#
# ====================================================================
#
# Cyrus 2.1.5 (Amos Gouaux)
# Also specify in main.cf: cyrus_destination_recipient_limit=1
#
# cyrus     unix  -       n       n       -       -       pipe
#  user=cyrus argv=/usr/lib/cyrus-imapd/deliver -e -r ${sender} -m ${extension} ${user}
#
# ====================================================================
#
# See the Postfix UUCP_README file for configuration details.
#
#uucp      unix  -       n       n       -       -       pipe
#  flags=Fqhu user=uucp argv=uux -r -n -z -a$sender - $nexthop!rmail ($recipient)
#
# ====================================================================
#
# Other external delivery methods.
#
#ifmail    unix  -       n       n       -       -       pipe
#  flags=F user=ftn argv=/usr/lib/ifmail/ifmail -r $nexthop ($recipient)
#
#bsmtp     unix  -       n       n       -       -       pipe
#  flags=Fq. user=bsmtp argv=/usr/local/sbin/bsmtp -f $sender $nexthop $recipient
#
#scalemail-backend unix -       n       n       -       2       pipe
#  flags=R user=scalemail argv=/usr/lib/scalemail/bin/scalemail-store
#  ${nexthop} ${user} ${extension}
#
#mailman   unix  -       n       n       -       -       pipe
#  flags=FR user=list argv=/usr/lib/mailman/bin/postfix-to-mailman.py
```

```
#  ${nexthop} ${user}
```

Rechargez les fichiers de configuration de Postfix :

```
[root@mail ~]# service postfix reload
Rechargement de postfix :                                  [  OK  ]
```

Utilisez la commande **netstat** pour vérifier que les ports soient à l'écoute :

```
[root@mail ~]# netstat -ln | more
Connexions Internet actives (seulement serveurs)
Proto Recv-Q Send-Q Local Address               Foreign Address             State
tcp        0      0 0.0.0.0:993                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:995                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:3306                0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:587                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:110                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:143                 0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:783               0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:111                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:465                 0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:22                  0.0.0.0:*                   LISTEN
tcp        0      0 127.0.0.1:631               0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:25                  0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:53689               0.0.0.0:*                   LISTEN
tcp        0      0 0.0.0.0:4190                0.0.0.0:*                   LISTEN
tcp        0      0 :::993                      :::*                        LISTEN
tcp        0      0 :::995                      :::*                        LISTEN
tcp        0      0 ::ffff:127.0.0.1:5701       :::*                        LISTEN
tcp        0      0 ::ffff:127.0.0.1:8009       :::*                        LISTEN
tcp        0      0 ::ffff:127.0.0.1:1099       :::*                        LISTEN
tcp        0      0 :::110                      :::*                        LISTEN
tcp        0      0 ::ffff:127.0.0.1:9999       :::*                        LISTEN
```

```
tcp        0      0 :::143                      :::*                        LISTEN
tcp        0      0 :::111                      :::*                        LISTEN
tcp        0      0 :::80                       :::*                        LISTEN
tcp        0      0 :::22                       :::*                        LISTEN
tcp        0      0 :::42294                    :::*                        LISTEN
tcp        0      0 :::55255                    :::*                        LISTEN
tcp        0      0 ::1:631                     :::*                        LISTEN
tcp        0      0 :::4190                     :::*                        LISTEN
udp        0      0 0.0.0.0:42118               0.0.0.0:*
--Plus--
```

Antispam et Antivirus

SpamAssassin

SpamAssassin est une **extension** pour postfix permettant de vérifier chaque message entrant afin d'identifier les messages **SPAM** en passant tous les messages par des tests. En fonction du résultat de ces tests, il attribue un score au message, chaque test rajoutant des points au score.

Installez SpamAssassin en utilisant yum :

```
[root@mail ~]# yum install spamassassin
```

Ouvrez le fichier de configuration de SpamAssassin, **/etc/mail/spamassassin/local.cf** :

```
[root@mail ~]# vi /etc/mail/spamassassin/local.cf
```

/etc/mail/spamassassin/local.cf

```
# These values can be overridden by editing ~/.spamassassin/user_prefs.cf
# (see spamassassin(1) for details)

# These should be safe assumptions and allow for simple visual sifting
```

```
# without risking lost emails.

required_hits 5
report_safe 0
rewrite_header Subject [SPAM]
```

Notez que les messages suspects seront marqués avec la chaine **[SPAM]** au début de l'objet du message.

Insérez la ligne **trusted_networks 10.0.2.** pour que celle-ci reflète l'adressage de votre propre réseau.

Insérez la ligne **ok_languages all**. Cette ligne indique les langues que vous acceptez de recevoir. Vous pouvez également mettre ici **fr** et/ou **en** pour ne recevoir que des messages en français et/ou en anglais.

Modifiez la ligne **required_hits 5** à **required_hits 3**. Cette ligne définit le score au delà duquel les mails sont considérés comme du spam.

Vous obtiendrez un résutat similaire à celui-ci :

/etc/mail/spamassassin/local.cf

```
# These values can be overridden by editing ~/.spamassassin/user_prefs.cf
# (see spamassassin(1) for details)

# These should be safe assumptions and allow for simple visual sifting
# without risking lost emails.

required_hits 3
report_safe 0
rewrite_header Subject [SPAM]
trusted_networks 10.0.2.
ok_languages all
```

Consultez le manuel de spamassassin pour connaître la signification de la directive **report_safe**.

Le service spamassissin n'est pas activé. Activez-le :

```
[root@mail ~]# chkconfig --list spamassassin
spamassassin    0:arrêt    1:arrêt    2:arrêt    3:arrêt    4:arrêt    5:arrêt    6:arrêt
[root@mail ~]# chkconfig --level 345 spamassassin on
[root@mail ~]# chkconfig --list spamassassin
spamassassin    0:arrêt    1:arrêt    2:arrêt    3:marche    4:marche    5:marche    6:arrêt
```

Démarrez le service spamassassin :

```
[root@mail ~]# service spamassassin start
Démarrage de spamd :                                       [  OK  ]
```

ClamAV

ClamAV est un antivirus pour Linux.

Installation

Installez clamav en utilisant la commande **yum** :

```
[root@mail ~]# yum install clamav clamd
```

Ouvrez le fichier **/etc/freshclam.conf** et éditez-le selon l'exemple ci-dessous :

```
##
## Example config file for freshclam
## Please read the freshclam.conf(5) manual before editing this file.
##
```

```
# Comment or remove the line below.
# Example

# Path to the database directory.
# WARNING: It must match clamd.conf's directive!
# Default: hardcoded (depends on installation options)
#DatabaseDirectory /var/lib/clamav

# Path to the log file (make sure it has proper permissions)
# Default: disabled
UpdateLogFile /var/log/freshclam.log

# Maximum size of the log file.
# Value of 0 disables the limit.
# You may use 'M' or 'm' for megabytes (1M = 1m = 1048576 bytes)
# and 'K' or 'k' for kilobytes (1K = 1k = 1024 bytes).
# in bytes just don't use modifiers. If LogFileMaxSize is enabled,
# log rotation (the LogRotate option) will always be enabled.
# Default: 1M
LogFileMaxSize 2M

# Log time with each message.
# Default: no
LogTime yes

# Enable verbose logging.
# Default: no
#LogVerbose yes

# Use system logger (can work together with UpdateLogFile).
# Default: no
#LogSyslog yes

# Specify the type of syslog messages - please refer to 'man syslog'
```

```
# for facility names.
# Default: LOG_LOCAL6
#LogFacility LOG_MAIL

# Enable log rotation. Always enabled when LogFileMaxSize is enabled.
# Default: no
LogRotate yes

# This option allows you to save the process identifier of the daemon
# Default: disabled
#PidFile /var/run/freshclam.pid

# By default when started freshclam drops privileges and switches to the
# "clamav" user. This directive allows you to change the database owner.
# Default: clamav (may depend on installation options)
#DatabaseOwner clamav

# Initialize supplementary group access (freshclam must be started by root).
# Default: no
#AllowSupplementaryGroups yes

# Use DNS to verify virus database version. Freshclam uses DNS TXT records
# to verify database and software versions. With this directive you can change
# the database verification domain.
# WARNING: Do not touch it unless you're configuring freshclam to use your
# own database verification domain.
# Default: current.cvd.clamav.net
#DNSDatabaseInfo current.cvd.clamav.net

# Uncomment the following line and replace XY with your country
# code. See http://www.iana.org/cctld/cctld-whois.htm for the full list.
# You can use db.XY.ipv6.clamav.net for IPv6 connections.
#DatabaseMirror db.XY.clamav.net
```

```
# database.clamav.net is a round-robin record which points to our most
# reliable mirrors. It's used as a fall back in case db.XY.clamav.net is
# not working. DO NOT TOUCH the following line unless you know what you
# are doing.
DatabaseMirror db.fr.clamav.net
DatabaseMirror db.local.clamav.net

# How many attempts to make before giving up.
# Default: 3 (per mirror)
MaxAttempts 5

# With this option you can control scripted updates. It's highly recommended
# to keep it enabled.
# Default: yes
#ScriptedUpdates yes

# By default freshclam will keep the local databases (.cld) uncompressed to
# make their handling faster. With this option you can enable the compression;
# the change will take effect with the next database update.
# Default: no
#CompressLocalDatabase no

# With this option you can provide custom sources (http:// or file://) for
# database files. This option can be used multiple times.
# Default: no custom URLs
#DatabaseCustomURL http://myserver.com/mysigs.ndb
#DatabaseCustomURL file:///mnt/nfs/local.hdb

# This option allows you to easily point freshclam to private mirrors.
# If PrivateMirror is set, freshclam does not attempt to use DNS
# to determine whether its databases are out-of-date, instead it will
# use the If-Modified-Since request or directly check the headers of the
# remote database files. For each database, freshclam first attempts
# to download the CLD file. If that fails, it tries to download the
```

```
# CVD file. This option overrides DatabaseMirror, DNSDatabaseInfo
# and ScriptedUpdates. It can be used multiple times to provide
# fall-back mirrors.
# Default: disabled
#PrivateMirror mirror1.mynetwork.com
#PrivateMirror mirror2.mynetwork.com

# Number of database checks per day.
# Default: 12 (every two hours)
#Checks 24

# Proxy settings
# Default: disabled
#HTTPProxyServer myproxy.com
#HTTPProxyPort 1234
#HTTPProxyUsername myusername
#HTTPProxyPassword mypass

# If your servers are behind a firewall/proxy which applies User-Agent
# filtering you can use this option to force the use of a different
# User-Agent header.
# Default: clamav/version_number
#HTTPUserAgent SomeUserAgentIdString

# Use aaa.bbb.ccc.ddd as client address for downloading databases. Useful for
# multi-homed systems.
# Default: Use OS'es default outgoing IP address.
#LocalIPAddress aaa.bbb.ccc.ddd

# Send the RELOAD command to clamd.
# Default: no
#NotifyClamd /path/to/clamd.conf

# Run command after successful database update.
```

```
# Default: disabled
#OnUpdateExecute command

# Run command when database update process fails.
# Default: disabled
#OnErrorExecute command

# Run command when freshclam reports outdated version.
# In the command string %v will be replaced by the new version number.
# Default: disabled
#OnOutdatedExecute command

# Don't fork into background.
# Default: no
#Foreground yes

# Enable debug messages in libclamav.
# Default: no
#Debug yes

# Timeout in seconds when connecting to database server.
# Default: 30
#ConnectTimeout 60

# Timeout in seconds when reading from database server.
# Default: 30
#ReceiveTimeout 60

# With this option enabled, freshclam will attempt to load new
# databases into memory to make sure they are properly handled
# by libclamav before replacing the old ones.
# Default: yes
#TestDatabases yes
```

```
# When enabled freshclam will submit statistics to the ClamAV Project about
# the latest virus detections in your environment. The ClamAV maintainers
# will then use this data to determine what types of malware are the most
# detected in the field and in what geographic area they are.
# Freshclam will connect to clamd in order to get recent statistics.
# Default: no
#SubmitDetectionStats /path/to/clamd.conf

# Country of origin of malware/detection statistics (for statistical
# purposes only). The statistics collector at ClamAV.net will look up
# your IP address to determine the geographical origin of the malware
# reported by your installation. If this installation is mainly used to
# scan data which comes from a different location, please enable this
# option and enter a two-letter code (see http://www.iana.org/domains/root/db/)
# of the country of origin.
# Default: disabled
#DetectionStatsCountry country-code

# This option enables support for our "Personal Statistics" service.
# When this option is enabled, the information on malware detected by
# your clamd installation is made available to you through our website.
# To get your HostID, log on http://www.stats.clamav.net and add a new
# host to your host list. Once you have the HostID, uncomment this option
# and paste the HostID here. As soon as your freshclam starts submitting
# information to our stats collecting service, you will be able to view
# the statistics of this clamd installation by logging into
# http://www.stats.clamav.net with the same credentials you used to
# generate the HostID. For more information refer to:
# http://www.clamav.net/support/faq/faq-cctts/
# This feature requires SubmitDetectionStats to be enabled.
# Default: disabled
#DetectionStatsHostID unique-id

# This option enables support for Google Safe Browsing. When activated for
```

```
# the first time, freshclam will download a new database file (safebrowsing.cvd)
# which will be automatically loaded by clamd and clamscan during the next
# reload, provided that the heuristic phishing detection is turned on. This
# database includes information about websites that may be phishing sites or
# possible sources of malware. When using this option, it's mandatory to run
# freshclam at least every 30 minutes.
# Freshclam uses the ClamAV's mirror infrastructure to distribute the
# database and its updates but all the contents are provided under Google's
# terms of use. See http://code.google.com/support/bin/answer.py?answer=70015
# and http://safebrowsing.clamav.net for more information.
# Default: disabled
#SafeBrowsing yes

# This option enables downloading of bytecode.cvd, which includes additional
# detection mechanisms and improvements to the ClamAV engine.
# Default: enabled
#Bytecode yes

# Download an additional 3rd party signature database distributed through
# the ClamAV mirrors. Here you can find a list of available databases:
# http://www.clamav.net/download/cvd/3rdparty
# This option can be used multiple times.
#ExtraDatabase dbname1
#ExtraDatabase dbname2
```

Creéz ensuite le fichier de journalisation de freshclam :

```
[root@mail ~]# touch /var/log/freshclam.log
[root@mail ~]# chown clamav:clamav /var/log/freshclam.log
```

Mettez à jour les définitions des virus :

```
[root@mail ~]# freshclam
ClamAV update process started at Sun May  4 15:07:04 2014
```

```
Downloading main.cvd [100%]
main.cvd updated (version: 55, sigs: 2424225, f-level: 60, builder: neo)
Downloading daily.cvd [100%]
daily.cvd updated (version: 18919, sigs: 928169, f-level: 63, builder: neo)
Downloading bytecode.cvd [100%]
bytecode.cvd updated (version: 236, sigs: 43, f-level: 63, builder: dgoddard)
Database updated (3352437 signatures) from db.fr.clamav.net (IP: 193.43.215.41)
```

Le Mandataire MailScanner

MailScanner est un mandataire qui est muni d'un système anti-spam et qui est capable d'utiliser la plupart des logiciels anti-virus.

MailScanner est utilisé dans plus de 225 pays et a été téléchargé plus de 1.3 millions de fois.

Préparation à l'Installation

Le paquet **rpm-build** est requis par le script d'installation de MailScanner :

```
[root@mail ~]# yum install rpm-build
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * atomic: mirrors.neusoft.edu.cn
 * base: centos.mirror.fr.planethoster.net
 * epel: fedora.aau.at
 * extras: centos.crazyfrogs.org
 * rpmforge: mirror.datacenter.mn
 * updates: centos.mirror.crcrepairs.com
ox-backend
```

```
| 1.3 kB     00:00
ox-frontend
| 1.3 kB     00:00
ox-usm
| 1.2 kB     00:00
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package rpm-build.i686 0:4.8.0-37.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
================================================
 Package                                  Arch                                  Version
Repository                               Size
================================================================================================================
================================================
Installing:
 rpm-build                                i686                                  4.8.0-37.el6
base                                    128 k

Transaction Summary
================================================================================================================
================================================
Install       1 Package(s)

Total download size: 128 k
Installed size: 306 k
Is this ok [y/N]: y
```

Installez les dépendances de MailScanner :

```
[root@mail ~]# yum install perl-Filesys-Df perl-DBD-SQLite
Loaded plugins: fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * atomic: www8.atomicorp.com
 * base: centos.mirror.fr.planethoster.net
 * epel: epel.mirrors.ovh.net
 * extras: centos.crazyfrogs.org
 * rpmforge: merlin.fit.vutbr.cz
 * updates: centos.mirror.crcrepairs.com
ox-backend
| 1.3 kB     00:00
ox-frontend
| 1.3 kB     00:00
ox-usm
| 1.2 kB     00:00
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package perl-DBD-SQLite.i686 0:1.27-3.el6 will be installed
---> Package perl-Filesys-Df.i686 0:0.92-5.el6 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
================================================
 Package                                    Arch                                Version
Repository                          Size
================================================================================================================
================================================
Installing:
 perl-DBD-SQLite                            i686                                1.27-3.el6
base                                83 k
 perl-Filesys-Df                            i686                                0.92-5.el6
```

```
epel                                    17 k

Transaction Summary
================================================================================
================================================
Install       2 Package(s)

Total download size: 100 k
Installed size: 246 k
Is this ok [y/N]: y
```

Installation

Téléchargez le fichier **MailScanner-4.84.6-1.rpm.tar.gz** :

```
[root@mail ~]# wget http://www.mailscanner.info/files/4/rpm/MailScanner-4.84.6-1.rpm.tar.gz
--2014-05-04 15:20:45--  http://www.mailscanner.info/files/4/rpm/MailScanner-4.84.6-1.rpm.tar.gz
Résolution de www.mailscanner.info... 78.153.201.155
Connexion vers www.mailscanner.info|78.153.201.155|:80...connecté.
requête HTTP transmise, en attente de la réponse...200 OK
Longueur: 5893091 (5,6M) [application/x-gzip]
Sauvegarde en : «MailScanner-4.84.6-1.rpm.tar.gz»

100%[================================================================================
==================>] 5 893 091   2,83M/s   ds 2,0s

2014-05-04 15:20:47 (2,83 MB/s) - «MailScanner-4.84.6-1.rpm.tar.gz» sauvegardé [5893091/5893091]
```

et désarchivez-le :

```
[root@mail ~]# tar xvf MailScanner-4.84.6-1.rpm.tar.gz
MailScanner-4.84.6-1/
```

```
MailScanner-4.84.6-1/perl-Time-HiRes-1.9707-3.src.rpm
MailScanner-4.84.6-1/mailscanner-4.84.6-1.noarch.rpm
MailScanner-4.84.6-1/perl-Compress-Raw-Zlib-2.027-1.src.rpm
MailScanner-4.84.6-1/perl-Scalar-List-Utils-1.19-3.src.rpm
MailScanner-4.84.6-1/perl-Test-Simple-0.86-2.src.rpm
MailScanner-4.84.6-1/perl-DBI-1.607-2.src.rpm
MailScanner-4.84.6-1/tnef-1.4.5-1.i386.rpm
MailScanner-4.84.6-1/perl-Convert-BinHex-1.119-3.src.rpm
MailScanner-4.84.6-1/CheckModuleVersion
MailScanner-4.84.6-1/getPERLLIB
MailScanner-4.84.6-1/perl-MailTools-2.04-2.src.rpm
MailScanner-4.84.6-1/perl-Compress-Zlib-1.41-2.src.rpm
MailScanner-4.84.6-1/perl-Sys-SigAction-0.11-1.src.rpm
MailScanner-4.84.6-1/ExtUtils-MakeMaker-6.30.tar.gz
MailScanner-4.84.6-1/perl-Convert-TNEF-0.17-2.src.rpm
MailScanner-4.84.6-1/perl-ExtUtils-MakeMaker-6.50-2.src.rpm
MailScanner-4.84.6-1/perl-Net-IP-1.25-2.src.rpm
MailScanner-4.84.6-1/perl-File-Spec-0.82-3.src.rpm
MailScanner-4.84.6-1/perl-Getopt-Long-2.38-2.src.rpm
MailScanner-4.84.6-1/perl-DBD-SQLite-1.25-2.src.rpm
MailScanner-4.84.6-1/perl-Math-BigInt-1.89-2.src.rpm
MailScanner-4.84.6-1/perl-OLE-Storage_Lite-0.16-2.src.rpm
MailScanner-4.84.6-1/perl-IO-1.2301-5.src.rpm
MailScanner-4.84.6-1/README
MailScanner-4.84.6-1/perl-Test-Harness-2.64-3.src.rpm
MailScanner-4.84.6-1/perl-Test-Pod-1.26-2.src.rpm
MailScanner-4.84.6-1/QuickInstall.txt
MailScanner-4.84.6-1/perl-Archive-Zip-1.30-1.src.rpm
MailScanner-4.84.6-1/tnef-1.4.5-1.x86_64.rpm
MailScanner-4.84.6-1/perl-Digest-SHA1-2.11-3.src.rpm
MailScanner-4.84.6-1/perl-Digest-MD5-2.36-3.src.rpm
MailScanner-4.84.6-1/perl-Filesys-Df-0.90-3.src.rpm
MailScanner-4.84.6-1/perl-HTML-Tagset-3.03-2.src.rpm
MailScanner-4.84.6-1/install.sh
```

```
MailScanner-4.84.6-1/perl-Digest-HMAC-1.01-1.src.rpm
MailScanner-4.84.6-1/perl-IO-stringy-2.110-2.src.rpm
MailScanner-4.84.6-1/perl-Net-DNS-0.65-2.src.rpm
MailScanner-4.84.6-1/perl-Sys-Hostname-Long-1.4-2.src.rpm
MailScanner-4.84.6-1/perl-File-Temp-0.20-4.src.rpm
MailScanner-4.84.6-1/perl-MIME-Base64-3.07-3.src.rpm
MailScanner-4.84.6-1/perl-bignum-0.23-1.src.rpm
MailScanner-4.84.6-1/perl-HTML-Parser-3.64-1.src.rpm
MailScanner-4.84.6-1/perl-Storable-2.16-3.src.rpm
MailScanner-4.84.6-1/perl-Pod-Escapes-1.04-2.src.rpm
MailScanner-4.84.6-1/perl-Math-BigRat-0.22-1.src.rpm
MailScanner-4.84.6-1/perl-TimeDate-1.16-4.src.rpm
MailScanner-4.84.6-1/perl-Net-CIDR-0.13-1.src.rpm
MailScanner-4.84.6-1/perl-Sys-Syslog-0.27-1.src.rpm
MailScanner-4.84.6-1/perl-Pod-Simple-3.05-2.src.rpm
MailScanner-4.84.6-1/perl-MIME-tools-5.427-2.src.rpm
```

Placez-vous dans le répertoire **MailScanner-4.84.6-1** et exécutez le script **install.sh**. Ce script a pour but de construire les RPMs nécessaires pour l'installation puis de les installer :

```
[root@centos6 ~]# cd MailScanner-4.84.6-1
[root@centos6 MailScanner-4.84.5-2]# ./install.sh
```

A l'issu de l'installation, vous obtiendrez un résultat similaire à celui-ci :

```
...
Good, SpamAssassin site rules found in /etc/mail/spamassassin
erreur lors de la lecture d'informations sur le service sendmail : Aucun fichier ou dossier de ce type

To activate MailScanner run the following commands:

service sendmail stop
chkconfig sendmail off
chkconfig MailScanner on
```

```
service MailScanner start

For technical support, please read the MAQ at www.mailscanner.biz/maq/
and buy the book at www.mailscanner.info/store

-----------------------------------------------------------
Please buy the MailScanner book from www.mailscanner.info!
It is a very useful administration guide and introduction
to MailScanner. All the proceeds go directly to making
MailScanner a better supported package than it is today.

[root@mail MailScanner-4.84.6-1]#
```

Configuration du couple MailScanner/Postfix

Arrêtez le service postfix :

```
[root@mail MailScanner-4.84.6-1]# service postfix stop
Arrêt de postfix :                                         [  OK  ]
```

Editez ensuite **/etc/postfix/main.cf** et ajoutez la ligne suivante à la fin du fichier :

```
...
header_checks = regexp:/etc/postfix/header_checks
```

Vous obtiendrez :

/etc/postfix/main.cf

```
##############CONFIG DE BASE##############
myhostname = mail.linuxelearning.info
mydomain= linuxelearning.info
```

```
myorigin = $mydomain
mynetworks = 10.0.2.0/24, 127.0.0.0/8
mydestination = $myhostname, localhost.$mydomain, localhost, $mydomain
smtpd_banner = $myhostname ESMTP $mail_name ($mail_version)
delay_warning_time = 4h
recipient_delimiter = +
owner_request_special = no
inet_interfaces = all
unknown_local_recipient_reject_code = 450
#############  RELAY HOST  ##############
relayhost = smtp.bbox.fr
#############  USER/GROUP  ##############
mail_owner = postfix
setgid_group = postdrop
#############   ALIASES    ##############
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
############   DEBUGGING   ##############
debug_peer_level = 2
debugger_command =
         PATH=/bin:/usr/bin:/usr/local/bin:/usr/X11R6/bin
         xxgdb $daemon_directory/$process_name $process_id & sleep 5
############   COMMANDES   ##############
mailbox_command = /usr/bin/procmail -Y -a $DOMAIN
sendmail_path = /usr/sbin/sendmail.postfix
newaliases_path = /usr/bin/newaliases.postfix
mailq_path = /usr/bin/mailq.postfix
############  REPERTOIRES  ##############
mail_spool_directory = /var/spool/mail
html_directory = no
manpage_directory = /usr/share/man
sample_directory = /usr/share/doc/postfix-2.6.6/samples
readme_directory = /usr/share/doc/postfix-2.6.6/README_FILES
queue_directory = /var/spool/postfix
```

```
command_directory = /usr/sbin
daemon_directory = /usr/libexec/postfix
############      SASL     ##############
smtpd_sasl_application_name     = smtpd
smtpd_recipient_restrictions    = permit_sasl_authenticated,
                                  permit_mynetworks,
                                  reject_unauth_destination,
                                  reject_invalid_hostname,
                                  reject_non_fqdn_hostname,
                                  reject_non_fqdn_sender,
                                  reject_non_fqdn_recipient,
                                  reject_unknown_sender_domain,
                                  reject_unknown_recipient_domain,
                                  reject_unauth_pipelining,
                                  reject_rbl_client zen.spamhaus.org,
                                  reject_rbl_client bl.spamcop.net,
                                  reject_rbl_client dnsbl.njabl.org,
                                  reject_rbl_client dnsbl.sorbs.net,
                                  permit
smtpd_client_restrictions = permit_sasl_authenticated, permit_mynetworks, reject_unauth_destination
smtp_sasl_mechanism_filter = plain
smtpd_sasl_auth_enable = yes
smtpd_sasl_security_options = noanonymous
broken_sasl_auth_clients = yes
smtpd_sasl_local_domain = linuxelearning.info
smtpd_helo_required             = yes
############      TLS      ##############
smtp_tls_CAfile = /etc/postfix/cacert.pem
smtp_tls_session_cache_database = btree:/var/lib/postfix/smtp_tls_sesson_cache
smtp_tls_security_level = may
smtpd_tls_CAfile = /etc/postfix/cacert.pem
smtpd_tls_session_cache_database = btree:/var/lib/postfix/smtpd_tls_sesson_cache
smtpd_tls_cert_file = /etc/postfix/lel_cert.pem
smtpd_tls_key_file = /etc/postfix/lel_clef.pem
```

```
smtpd_tls_received_header = yes
tls_random_source = dev:/dev/urandom
smtpd_tls_security_level = may
smtpd_tls_loglevel = 2
smtpd_tls_ask_ccert = no
############ HEADER CHECKS ###############
header_checks = regexp:/etc/postfix/header_checks
```

Pour plus d'informations concernant les directives, consultez **cette page**.

Editez ensuite **/etc/postfix/header_checks** en ajoutant les lignes suivantes à la fin du fichier :

```
...
/^Received:/ HOLD
/^User-Agent:/              IGNORE
```

Le but de la première ligne est de placer tous les messages entrant dans le répertoire **/var/spool/postfix/hold** afin de les traiter par MailScanner.

Le but de la deuxième ligne est de retirer la ligne commençant par **User-Agent:** des en-têtes des messages sortants.

```
[root@mail MailScanner-4.84.6-1]# ls /var/spool/postfix
active  bounce  corrupt  defer  deferred  flush  hold  incoming  maildrop  pid  private  public  saved  trace
```

Comprendre la fonction des répertoires dans **/var/spool/postfix** nécessite une compréhension des processus principaux de postfix :

Processus	**Description**
master	Processus central de postfix. Il lance les autres processus. Il est lancé par root. Ses paramètres de configuration se trouvent dans le fichier **/etc/postfix/master.cf**
qmgr	Processus qui lit la queue **incoming** et place une partie des messages dans **active**. Ensuite il efface les messages où le traitement s'est bien passé. Dans le cas contraire, il place les messages dans **deferred**.

Processus	Description
pickup	Processus qui attend d'être informé par **postdrop** de la présence de nouveaux messages dans le répertoire **maildrop**. Il passe ensuite les messages au processus **cleanup**.
smtpd	Processus qui reçoit les messages de l'extérieur et les passe au processus **cleanup**.
cleanup	Processus qui reçoit les messages de **pickup** ou de **smtpd** et qui les complète en termes de champs manquants (p.e. From: To: etc) tout en éliminant les doublons d'adresses destinataires. Il délègue au processus **trivial-rewrite** la tâche de transformer les adresses de l'enveloppe et des en-têtes d'adresses de type nom@fqdn.extension. Il place les messages traités dans le répertoire **incoming** et informe le processus **qmgr** qu'il faut examiner ce dernier.
bounce	Processus qui délivre des messages de notification en cas d'échec définitif, de remise différée, de remise avec succès ou de vérifications d'adresses. IL maintient dans le répertoire **bounce** des informations sur les raisons des rejets des messages.
defer	Un alias du processus bounce qui maintient dans le répertoire **defer** les informations d'explications des raisons des messages différés.
trace	Un alias du processus bounce qui maintient dans le répertoire **trace** les informations de suivi de la remise des messages si ces informations ont été demandées en utilisant la commande **sendmail -bv** ou **sendmail -v**.
flush	Processus qui constitue une liste de messages, corréspondants à la directive du fichier **/etc/postfix/main.cf fast_flush_domain**, qui vont être traités plus prioritairement.
trivial-rewrite	Voir les processus **cleanup** et **qmgr**.
verify	Processus qui maintient une base d'addresses connues valides ou invalides.
scache	Processus qui maintient un cache des serveurs extérieurs où le processus smtpd a pu se connecter. Ces informations sont gardés pendant le temps spécifié par la directive **max_idle**.
anvil	Processus qui est chargé de la collecte des statistiques du nombre de connexions et de requêtes éffectuées par chaque client.
showcase	Processus qui rapporte l'état des files d'attente.

Après avoir vu les processus de postfix, nous pouvons se concentrer sur les répertoires présents dans **/var/spool/postfix** :

Répertoire	Contenu
active	Répertoire de file d'attente. Contient les messages en cours de traitement. En réalité ce répertoire est vide car les messages concernés sont tous en mémoire.
bounce	Répertoire contenant les raisons des rejets des messages.
corrupt	Répertoire contenant des messages corrompus.
defer	Répertoire de stockage temporaire. Contient les informations sur la raison des échecs des messages qui se trouvent dans le répertoire **deferred**.
deferred	Répertoire de file d'attente. Contient des sous-répertoires qui contiennent les messages qui n'ont pas pu être remis. Chaque sous-répertoire est nommé après le premier caractère de la **Queue ID** du message.

Répertoire	Contenu
flush	Répertoire utilisé par le processus **flush**.
hold	Répertoire de stockage temporaire. Voir ci-dessus.
incoming	Répertoire de file d'attente. Contient les messages placés par le processus **cleanup**.
maildrop	Répertoire de stockage temporaire. Contient des messages crées localement.
pid	Répertoire de stockage temporaire. Contient les PID des processus postfix lancés.
private	Répertoire contenant une liste de sockets disponibles pour des utilisateurs priviligiés.
public	Répertoire contenant une liste de sockets disponibles pour tout le monde.
trace	Répertoire utilisé par le processus **trace**.

Ouvrez maintenant le fichier **/etc/MailScanner/MailScanner.conf**.

Ce fichier doit être modifié pour fonctionner avec **postfix** et **clamav**. Dans un premier temps recherchez les directives suivantes et modifiez-les comme indiqué :

```
...
Run As User = postfix
...
Run As Group = postfix
...
Incoming Queue Dir = /var/spool/postfix/hold
...
Outgoing Queue Dir = /var/spool/postfix/incoming
...
MTA = postfix
...
SpamAssassin User State Dir = /var/spool/MailScanner/spamassassin
```

Le but de la cinquième ligne est d'indiquer à MailScanner qu'il doit fonctionner avec postfix. Le but de la première et la deuxième ligne est de lui donner les mêmes droits sur les mêmes fichiers que le service postfix lui-même. Le but de le la ligne 3 est d'indiquer à MailScanner où il va trouver les messages à traiter. Le but de la ligne 4 est d'indiquer où MailScanner doit mettre les messages à la fin de son traitement de ces derniers.

Ensuite, recherchez les directives suivantes et modifiez-les comme indiqué :

```
...
Virus Scanners = clamav
...
Notify Senders Of Viruses = yes
...
Spam Subject Text = [SPAM]
...
High Scoring Spam Subject Text = [SPAM]
...
Required SpamAssassin Score = 3
...
```

Ces directives indiquent respectivement que :

- Ligne 1 - MailScanner qu'il doit utiliser clamav pour examiner les messages,
- Ligne 2 - le destinataire d'un message contenant un virus doit être informé de l'adresse de l'expéditeur,
- Lignes 3, 4 et 5 - il y a compatibilité entre MailScanner et Spamassassin.

Créez le fichier **/var/spool/MailScanner/spamassassin** et donnez les droits à postfix :

```
[root@mail MailScanner-4.84.6-1]# mkdir /var/spool/MailScanner/spamassassin
[root@mail MailScanner-4.84.6-1]# chown postfix:postfix /var/spool/MailScanner/spamassassin
```

Ouvrez maintenant le fichier **/etc/MailScanner/virus.scanners.conf** :

```
[root@mail MailScanner-4.84.6-1]# cat /etc/MailScanner/virus.scanners.conf
```

/etc/MailScanner/virus.scanners.conf

```
# This is a list of the names of the virus scanning engines, along with the
# filename of the command or script to run to invoke each one.
# Three fields:
```

```
#  1.  Name of virus scanner as known by MailScanner. Do not change this.
#  2.  Location of -wrapper script. You should not need to change this.
#  3.  Installation directory of virus scanner. This does not usually include
#      any "bin" directory in the path to the scanner program itself.
# You can test a -wrapper script with a command like this:
#      /usr/lib/MailScanner/f-secure-wrapper /opt/f-secure/fsav /tmp
# That command will attempt to scan /tmp using F-Secure. If it works you
# should see some sensible output. If it fails, you will probably just see
# an error message such as "Command not found" or similar.
#
antivir     /usr/lib/MailScanner/antivir-wrapper    /usr/lib/AntiVir
avast       /usr/lib/MailScanner/avast-wrapper    /usr
avastd      /usr/lib/MailScanner/avastd-wrapper    /usr
avg     /usr/lib/MailScanner/avg-wrapper    /usr/local
bitdefender /usr/lib/MailScanner/bitdefender-wrapper /opt/bdc
clamav      /usr/lib/MailScanner/clamav-wrapper    /usr/local
clamd       /bin/false                /usr/local
clamavmodule    /bin/false                /tmp
command     /usr/lib/MailScanner/command-wrapper    /usr
css     /usr/lib/MailScanner/css-wrapper    /opt/SYMCScan
drweb       /usr/lib/MailScanner/drweb-wrapper    /opt/drweb
esets       /usr/lib/MailScanner/esets-wrapper    /usr/sbin
etrust      /usr/lib/MailScanner/etrust-wrapper    /opt/eTrustAntivirus
f-prot      /usr/lib/MailScanner/f-prot-wrapper    /usr/local/f-prot
f-prot-6    /usr/lib/MailScanner/f-prot-6-wrapper    /opt/f-prot
f-protd-6   /bin/false                /opt/f-prot
f-secure    /usr/lib/MailScanner/f-secure-wrapper    /opt/f-secure/fsav
generic     /usr/lib/MailScanner/generic-wrapper    /
inoculan    /usr/lib/MailScanner/inoculan-wrapper    /usr/local/inoculan
inoculate   /usr/lib/MailScanner/inoculate-wrapper    /usr/local/av
# Kaspersky 5.5: your kaspersky-4.5 path should be /opt/kav/5.5
# Kaspersky 4.5 and newer
kaspersky-4.5   /usr/lib/MailScanner/kaspersky-wrapper    /opt/kav
kaspersky   /usr/lib/MailScanner/kaspersky-wrapper    /opt/AVP
```

```
kavdaemonclient /usr/lib/MailScanner/kavdaemonclient-wrapper /usr/local
mcafee      /usr/lib/MailScanner/mcafee-wrapper    /usr/local/uvscan
mcafee6     /usr/lib/MailScanner/mcafee6-wrapper    /usr/local/uvscan
# Now updated to handle nod32 2.01 and upwards
#nod32-1.99 /usr/lib/MailScanner/nod32-wrapper    /usr/local/nod32
nod32-1.99  /usr/lib/MailScanner/nod32-wrapper    /usr/sbin
nod32       /usr/lib/MailScanner/nod32-wrapper    /usr/local/nod32
none        /bin/false                /tmp
norman      /usr/lib/MailScanner/norman-wrapper    /usr/bin
panda       /usr/lib/MailScanner/panda-wrapper    /usr
rav     /usr/lib/MailScanner/rav-wrapper    /usr/local/rav8
sophos      /usr/lib/MailScanner/sophos-wrapper    /opt/sophos-av
sophossavi  /bin/false                /tmp
symscanengine   /usr/lib/MailScanner/symscanengine-wrapper /opt/SYMCScan
trend       /usr/lib/MailScanner/trend-wrapper    /pack/trend
vba32       /usr/lib/MailScanner/vba32-wrapper    /opt/vba/vbacl
vexira      /usr/lib/MailScanner/vexira-wrapper    /usr/local/vexira
```

Dans la troisième colonne sont indiqués des chemins. C'est dans le chemin indiqué, ou bien dans le sous-répertoire /bin du chemin indiqué que MailScanner cherche l'exécutable de l'anti-virus concerné. Le chemin n'est pas correct pour clamav. En effet, **clamscan** se trouve dans **/usr/bin** et non pas dans /usr/local ou /usr/local/bin.

Afin de pouvoir maintenir dans l'état la configuration par défaut de ce fichier, procédez à la création de deux liens symboliques dans le répertoire **/usr/local/bin/**:

```
[root@mail MailScanner-4.84.6-1]# ln -s /usr/bin/clamscan /usr/local/bin
[root@mail MailScanner-4.84.6-1]# ln -s /usr/bin/freshclam /usr/local/bin
[root@mail MailScanner-4.84.6-1]# ls -l /usr/local/bin/*clam*
lrwxrwxrwx. 1 root root 17  4 mai   16:46 /usr/local/bin/clamscan -> /usr/bin/clamscan
```

```
lrwxrwxrwx. 1 root root 18  4 mai   16:47 /usr/local/bin/freshclam -> /usr/bin/freshclam
```

Vérifiez maintenant le **wrapper** utilisé pour appeler l'anti-virus clamav par MailScanner en testant le répertoire **/tmp** :

```
[root@mail ~]# /usr/lib/MailScanner/clamav-wrapper /usr/local/bin/clamscan /tmp
/tmp/yum_save_tx-2014-04-29-13-38UTCuDW.yumtx: OK
/tmp/yum_save_tx-2014-04-29-13-38Tk9EZy.yumtx: OK
/tmp/.X0-lock: OK
/tmp/tmp.Rj6JKxBDg8: Empty file
/tmp/tmp.Hrv4PVqLTF: Empty file
/tmp/tmp.Med33tlLWQ: Empty file
/tmp/main.cf: OK
/tmp/vboxguest-Module.symvers: OK

----------- SCAN SUMMARY -----------
Known viruses: 3347030
Engine version: 0.98.1
Scanned directories: 1
Scanned files: 5
Infected files: 0
Data scanned: 0.03 MB
Data read: 0.02 MB (ratio 2.00:1)
Time: 8.383 sec (0 m 8 s)
```

Finalement, **postfix** a besoin d'avoir accès aux répertoires suivants :

- /var/spool/MailScanner/incoming
- /var/spool/MailScanner/quarantine

Modifiez donc le propriétaire ainsi que le groupe :

```
[root@redhat MailScanner-4.81.4-1]# chown -R postfix.postfix /var/spool/MailScanner/incoming
[root@redhat MailScanner-4.81.4-1]# chown -R postfix.postfix /var/spool/MailScanner/quarantine
```

Démarrez les services postfix et MailScanner :

```
[root@mail ~]# service MailScanner start
Starting MailScanner daemons:
         incoming postfix:                                  [  OK  ]
         outgoing postfix:                                  [  OK  ]
         MailScanner:                                       [  OK  ]
```

Procédez ensuite à une envoi de test à votre serveur postfix :

```
[root@mail ~]# telnet localhost 25
Trying ::1...
telnet: connect to address ::1: Connection refused
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
220 mail.linuxelearning.info ESMTP Postfix (2.6.6)
EHLO me
250-mail.linuxelearning.info
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-STARTTLS
250-AUTH LOGIN PLAIN
250-AUTH=LOGIN PLAIN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
AUTH PLAIN dHJhaW5lZQB0cmFpbmVlAHRyYWluZWU=
235 2.7.0 Authentication successful
MAIL from: root@linuxelearning.info
250 2.1.0 Ok
RCPT to: mickey.mouse@linuxelearning.info
```

```
250 2.1.5 Ok
DATA
354 End data with <CR><LF>.<CR><LF>
Subject: MailScanner test
XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X
.
250 2.0.0 Ok: queued as EB34464A1
QUIT
221 2.0.0 Bye
Connection closed by foreign host.
```

La chaîne de caractères **XJS*C4JDBQADN1.NSBN3*2IDNEN*GTUBE-STANDARD-ANTI-UBE-TEST-EMAIL*C.34X** est une chaîne de test qui indique à MailScanner et SpamAssassin que le massage est du spam.

Consultez le fichier **/var/log/maillog** :

```
...
May  5 14:14:11 mail postfix/smtpd[17876]: connect from localhost[127.0.0.1]
May  5 14:15:13 mail postfix/smtpd[17876]: EB34464A1: client=localhost[127.0.0.1], sasl_method=PLAIN,
sasl_username=trainee@linuxelearning.info
May  5 14:15:45 mail postfix/cleanup[17884]: EB34464A1: hold: header Received: from me (localhost
[127.0.0.1])??by mail.linuxelearning.info (Postfix) with ESMTPA id EB34464A1??for
<mickey.mouse@linuxelearning.info>; Mon,  5 May 2014 14:14:55 +0200 (CEST) from localhost[127.0.0.1];
from=<root@linuxelearning.info> to=<mickey.mouse@linuxelearning.info> proto=ESMTP helo=<me>
May  5 14:15:45 mail postfix/cleanup[17884]: EB34464A1: message-
id=<20140505121513.EB34464A1@mail.linuxelearning.info>
May  5 14:15:46 mail MailScanner[17759]: New Batch: Scanning 1 messages, 1159 bytes
May  5 14:15:46 mail MailScanner[17759]: Virus and Content Scanning: Starting
May  5 14:15:47 mail postfix/scache[17870]: statistics: start interval May  5 14:12:28
May  5 14:15:47 mail postfix/scache[17870]: statistics: domain lookup hits=0 miss=1 success=0%
May  5 14:15:47 mail postfix/scache[17870]: statistics: address lookup hits=0 miss=1 success=0%
```

```
May  5 14:15:47 mail postfix/scache[17870]: statistics: max simultaneous domains=1 addresses=1 connection=1
May  5 14:15:47 mail postfix/smtpd[17876]: disconnect from localhost[127.0.0.1]
May  5 14:15:54 mail MailScanner[17759]: Spam Checks: Found 1 spam messages
```

Notez la présence de la ligne suivante : May 5 14:15:54 mail MailScanner[17759]: Spam Checks: Found 1 spam messages

Surveillance Sécuritaire

La commande last

Cette commande indique les dates et heures des dernières connexions des utilisateurs :

```
[root@centos6 ~]# last
trainee  pts/0        :0.0             Mon Oct  3 17:39   still logged in
trainee  tty1         :0               Mon Oct  3 16:16   still logged in
reboot   system boot  2.6.32-71.29.1.e Mon Oct  3 16:15 - 18:30  (02:14)
trainee  pts/0        :0.0             Mon Oct  3 16:12 - 16:13  (00:01)
trainee  pts/0        :0.0             Mon Oct  3 16:08 - 16:10  (00:02)
trainee  tty1         :0               Mon Oct  3 16:05 - down   (00:10)
reboot   system boot  2.6.32-71.29.1.e Mon Oct  3 16:04 - 16:15  (00:10)
trainee  pts/1        :0.0             Thu Sep 29 17:29 - 17:29  (00:00)
trainee  pts/0        :0.0             Thu Sep 29 11:11 - crash (4+04:53)
trainee  tty1         :0               Thu Sep 29 11:07 - crash (4+04:56)
reboot   system boot  2.6.32-71.29.1.e Thu Sep 29 11:07 - 16:15 (4+05:08)
trainee  pts/0        :0.0             Wed Sep 28 15:29 - crash  (19:37)
trainee  tty1         :0               Wed Sep 28 15:29 - crash  (19:37)
reboot   system boot  2.6.32-71.29.1.e Wed Sep 28 15:28 - 16:15 (5+00:47)
trainee  pts/0        :0.0             Wed Aug  3 14:15 - 14:29  (00:13)
trainee  tty1         :0               Wed Aug  3 14:07 - crash (56+01:20)
```

```
reboot   system boot  2.6.32-71.29.1.e Wed Aug  3 14:06 - 16:15 (61+02:09)
trainee  pts/0        :0.0             Thu Jul 28 16:23 - 16:30  (00:06)
trainee  tty1         :0               Thu Jul 28 16:21 - down   (00:08)
reboot   system boot  2.6.32-71.29.1.e Thu Jul 28 16:21 - 16:30  (00:09)
trainee  pts/2        :0.0             Thu Jul 28 16:15 - 16:15  (00:00)
trainee  pts/1        :0.0             Thu Jul 28 16:14 - down   (00:06)
trainee  pts/0        :0.0             Thu Jul 28 16:11 - down   (00:08)
trainee  pts/0        :0.0             Thu Jul 28 14:57 - 15:02  (00:05)
trainee  tty1         :0               Thu Jul 28 14:45 - down   (01:35)
reboot   system boot  2.6.32-71.el6.i6 Thu Jul 28 14:43 - 16:20  (01:37)
```

La commande lastlog

Cette commande indique aussi les dates et heures des dernières connexions des utilisateurs :

```
[root@centos6 ~]# lastlog
Utilisateur      Port     Venant de        Dernière
root                                       **Jamais connecté**
bin                                        **Jamais connecté**
daemon                                     **Jamais connecté**
adm                                        **Jamais connecté**
lp                                         **Jamais connecté**
sync                                       **Jamais connecté**
shutdown                                   **Jamais connecté**
halt                                       **Jamais connecté**
mail                                       **Jamais connecté**
uucp                                       **Jamais connecté**
operator                                   **Jamais connecté**
games                                      **Jamais connecté**
gopher                                     **Jamais connecté**
ftp                                        **Jamais connecté**
nobody                                     **Jamais connecté**
dbus                                       **Jamais connecté**
```

```
usbmuxd                                          **Jamais connecté**
avahi-autoipd                                    **Jamais connecté**
vcsa                                             **Jamais connecté**
rpc                                              **Jamais connecté**
rtkit                                            **Jamais connecté**
abrt                                             **Jamais connecté**
nscd                                             **Jamais connecté**
tcpdump                                          **Jamais connecté**
haldaemon                                        **Jamais connecté**
apache                                           **Jamais connecté**
nslcd                                            **Jamais connecté**
saslauth                                         **Jamais connecté**
postfix                                          **Jamais connecté**
avahi                                            **Jamais connecté**
ntp                                              **Jamais connecté**
rpcuser                                          **Jamais connecté**
nfsnobody                                        **Jamais connecté**
sshd                                             **Jamais connecté**
pulse                                            **Jamais connecté**
gdm                                              **Jamais connecté**
trainee                                          **Jamais connecté**
vboxadd                                          **Jamais connecté**
prison                                           **Jamais connecté**
```

La Commande faillog

La commande **faillog** sous RHEL/CentOS 6 affiche le contenu du journal des échecs de connexion (/var/log/faillog), et maintient le décompte et les limitations de ces échecs. Exécuter faillog sans argument n’affiche que la liste des échecs des utilisateurs qui ont déjà eu un échec de connexion.

/var/log/secure

Sous RHEL/CentOS 6 ce fichier contient la journalisation des opérations de gestion des authentifications :

```
[root@centos6 ~]# tail -n 15 /var/log/secure
Oct  3 18:19:26 centos su: pam_unix(su-l:session): session closed for user prison
Oct  3 18:20:33 centos su: pam_unix(su-l:session): session opened for user prison by trainee(uid=0)
Oct  3 18:21:26 centos su: pam_unix(su-l:session): session closed for user prison
Oct  3 18:23:07 centos su: pam_unix(su-l:session): session opened for user prison by trainee(uid=0)
Oct  3 18:23:17 centos su: pam_unix(su-l:session): session closed for user prison
Oct  3 18:23:19 centos su: pam_unix(su-l:session): session opened for user prison by trainee(uid=0)
Oct  3 18:23:39 centos su: pam_unix(su-l:session): session closed for user prison
Oct  3 18:25:50 centos su: pam_unix(su-l:session): session closed for user root
Oct  3 18:26:28 centos sudo:  trainee : user NOT in sudoers ; TTY=pts/0 ; PWD=/home/trainee ; USER=root ;
COMMAND=/bin/cat /etc/sudoers
Oct  3 18:26:53 centos su: pam_unix(su-l:session): session opened for user root by trainee(uid=500)
Oct  3 18:26:55 centos usermod[3061]: add 'trainee' to group 'wheel'
Oct  3 18:26:55 centos usermod[3061]: add 'trainee' to shadow group 'wheel'
Oct  3 18:27:22 centos su: pam_unix(su-l:session): session closed for user root
Oct  3 18:27:29 centos sudo:  trainee : TTY=pts/0 ; PWD=/home/trainee ; USER=root ; COMMAND=/bin/cat /etc/sudoers
Oct  3 18:29:53 centos su: pam_unix(su-l:session): session opened for user root by trainee(uid=500)
```

<html>

</html>
