Version : **2024.01**

Dernière mise-à-jour : 2024/04/26 09:28

LRF408 - Sécurité Applicative

Contenu du Module

- Préparation
- Gestion de serveurs virtuels
    - Hôte virtuel par nom
    - Hôte virtuel par adresse IP
- mod_auth_basic
    - Configuration de la sécurité avec .htaccess
    - Mise en place d'un fichier de mots de passe
- mod_auth_mysql
    - Installation
    - Configuration de MariaDB
    - Configuration d'Apache
- mod_authnz_ldap
- mod_ssl
    - Présentation de SSL
    - Fonctionnement de SSL
    - Installation de ssl
    - Configuration de SSL
    - Mise en place des paramètres de sécurité SSL
    - Tester Votre Configuration

Le Problématique

La plupart des failles de sécurité ne sont pas du fait du système d'exploitation mais des applications installées.

Préparation

Les Outils

LAB #1 - Netwox

Le programme **netwox** est un utilitaire puissant de vérification de la sécurité.

Installation

Commencez par télécharger le paquet **netwox-5.35.0-1.el6.rf.x86_64.rpm** :

```
[root@centos7 ~]# wget
https://www.dropbox.com/scl/fi/e55p8pmn5sbo4uflddpue/netwox-5.35.0-1.el5.rf.i386.rpm?rlkey=1l475ob83ktbja21s18fht
brb&st=7umpk4yj
```

Netwox s'installe en utilisant yum :

```
[root@centos7 ~]# yum localinstall netwox-5.35.0-1.el6.rf.x86_64.rpm --nogpgcheck
```

Utilisation

```
[root@centos7 ~]# 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
Select a node (key in 0123456abcd):
```

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.

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"
```

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 #2 - OpenVAS

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.

Préparation

Mettez SELinux en mode permissive et désactivez-le dans le fichier **/etc/selinux/config** :

```
[root@centos7 ~]# setenforce permissive
[root@centos7 ~]# sed -i 's/=enforcing/=disabled/' /etc/selinux/config
```

Insérez une règle dans le pare-feu pour permettre la consultation de l'interface HTML du client OpenVAS :

```
[root@centos7 ~]# firewall-cmd --zone=public --add-port=9443/tcp --permanent
success
[root@centos7 ~]# firewall-cmd --reload
success
```

Installation

OpenVAS se trouve dans les dépôts d'EPEL. Installez donc ce dépôt :

```
[root@centos7 ~]# yum install https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
```

Installez ensuite **openvas-scanner**, **openvas-manager**, **openvas-gsa** et **openvas-cli** en utilisant yum :

```
[root@centos6 ~]# yum install openvas-scanner openvas-manager openvas-gsa openvas-cli coreutils openssl
```

Configuration

Les commandes d'OpenVAS sont les suivantes :

```
[root@centos7 ~]# ls -l /usr/sbin/openvas*
-rwxr-xr-x. 1 root root   18066 Sep  6  2016 /usr/sbin/openvas-certdata-sync
-rwxr-xr-x. 1 root root 2182496 Sep  6  2016 /usr/sbin/openvasmd
-rwxr-xr-x. 1 root root   37993 Sep  6  2016 /usr/sbin/openvas-migrate-to-postgres
-rwxr-xr-x. 1 root root   11998 Sep  6  2016 /usr/sbin/openvas-mkcert
-rwxr-xr-x. 1 root root   10976 Sep  6  2016 /usr/sbin/openvas-nvt-sync
-rwxr-xr-x. 1 root root     766 Sep  6  2016 /usr/sbin/openvas-nvt-sync-cron
-rwxr-xr-x. 1 root root    2555 Sep  6  2016 /usr/sbin/openvas-portnames-update
-rwxr-xr-x. 1 root root   38378 Sep  6  2016 /usr/sbin/openvas-scapdata-sync
-rwxr-xr-x. 1 root root   86640 Sep  6  2016 /usr/sbin/openvassd
```

- **/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/openvasd**,
  - Cette commande lance le serveur OpenVAS.

Exécutez maintenant la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
openvas-check-setup 2.3.3
```

```
  Test completeness and readiness of OpenVAS-8
  (add '--v6' or '--v7' or '--v9'
   if you want to check for another OpenVAS version)

  Please report us any non-detected problems and
  help us to improve this check routine:
  http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss

  Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the problem.

  Use the parameter --server to skip checks for client tools
  like GSD and OpenVAS-CLI.

Step 1: Checking OpenVAS Scanner ...
        OK: OpenVAS Scanner is present in version 5.0.6.
        ERROR: No CA certificate file of OpenVAS Scanner found.
        FIX: Run 'openvas-mkcert'.

 ERROR: Your OpenVAS-8 installation is not yet complete!

Please follow the instructions marked with FIX above and run this
script again.

If you think this result is wrong, please report your observation
and help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
Please attach the log-file (/tmp/openvas-check-setup.log) to help us analyze the problem.
```

Important - Notez l'erreur **ERROR: No CA certificate file of OpenVAS Scanner found.**

Créez donc un certificat SSL :

```
[root@centos7 ~]# openvas-mkcert

-------------------------------------------------------------------------------
            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]: 3650
Server certificate life time in days [365]: 3650
Your country (two letter code) [DE]: UK
Your state or province name [none]: SURREY
Your location (e.g. town) [Berlin]: ADDLESTONE
Your organization [OpenVAS Users United]: I2TCH LIMITED

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

Congratulations. Your server certificate was properly created.

The following files were created:

. Certification authority:
   Certificate = /etc/pki/openvas/CA/cacert.pem
   Private key = /etc/pki/openvas/private/CA/cakey.pem

. OpenVAS Server :
    Certificate = /etc/pki/openvas/CA/servercert.pem
```

```
    Private key = /etc/pki/openvas/private/CA/serverkey.pem

Press [ENTER] to exit

[Entrée]
[root@centos7 ~]#
```

Exécutez de nouveau la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
openvas-check-setup 2.3.3
  Test completeness and readiness of OpenVAS-8
  (add '--v6' or '--v7' or '--v9'
   if you want to check for another OpenVAS version)

  Please report us any non-detected problems and
  help us to improve this check routine:
  http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss

  Send us the log-file (/tmp/openvas-check-setup.log) to help analyze the problem.

  Use the parameter --server to skip checks for client tools
  like GSD and OpenVAS-CLI.

Step 1: Checking OpenVAS Scanner ...
        OK: OpenVAS Scanner is present in version 5.0.6.
        OK: OpenVAS Scanner CA Certificate is present as /etc/pki/openvas/CA/cacert.pem.
/bin/openvas-check-setup: line 219: redis-server: command not found
        ERROR: No redis-server installation found.
        FIX: You should install redis-server for improved scalability and ability to trace/debug the KB

 ERROR: Your OpenVAS-8 installation is not yet complete!

Please follow the instructions marked with FIX above and run this
```

```
script again.

If you think this result is wrong, please report your observation
and help us to improve this check routine:
http://lists.wald.intevation.org/mailman/listinfo/openvas-discuss
Please attach the log-file (/tmp/openvas-check-setup.log) to help us analyze the problem.
```

Important - Notez l'erreur **ERROR: No redis-server installation found.**

Installez donc **redis** :

```
[root@centos7 ~]# yum install redis
```

Activez les deux lignes suivantes dans le fichier **/etc/redis.conf** :

```
...
# unixsocket /tmp/redis.sock
# unixsocketperm 700...
```

```
[root@centos7 ~]# sed -i '/^#.*unixsocket/s/^# //' /etc/redis.conf
```

Ajoutez la ligne **kb_location = /tmp/redis.sock** dans le fichier **/etc/openvas/openvassd.conf** :

```
...
# KB test replay :
kb_dont_replay_scanners = no
kb_dont_replay_info_gathering = no
kb_dont_replay_attacks = no
kb_dont_replay_denials = no
kb_max_age = 864000
kb_location = /tmp/redis.sock
```

```
#--- end of the KB section
...
```

Activez et démarrez le service **redis** :

```
[root@centos7 ~]# systemctl enable redis
Created symlink from /etc/systemd/system/multi-user.target.wants/redis.service to
/usr/lib/systemd/system/redis.service.
[root@centos7 ~]# systemctl start redis
[root@centos7 ~]# systemctl status redis
● redis.service - Redis persistent key-value database
   Loaded: loaded (/usr/lib/systemd/system/redis.service; enabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/redis.service.d
           └─limit.conf
   Active: active (running) since Wed 2018-06-20 02:58:35 CEST; 7s ago
 Main PID: 18881 (redis-server)
   CGroup: /system.slice/redis.service
           └─18881 /usr/bin/redis-server 127.0.0.1:6379

Jun 20 02:58:35 centos7.fenestros.loc systemd[1]: Started Redis persistent key-value database.
Jun 20 02:58:35 centos7.fenestros.loc systemd[1]: Starting Redis persistent key-value database...
```

Exécutez encore une fois la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
...
Step 1: Checking OpenVAS Scanner ...
        OK: OpenVAS Scanner is present in version 5.0.6.
        OK: OpenVAS Scanner CA Certificate is present as /etc/pki/openvas/CA/cacert.pem.
        OK: redis-server is present in version v=3.2.10.
        OK: scanner (kb_location setting) is configured properly using the redis-server socket: /tmp/redis.sock
        OK: redis-server is running and listening on socket: /tmp/redis.sock.
        OK: redis-server configuration is OK and redis-server is running.
        ERROR: The NVT collection is very small.
```

```
        FIX: Run a synchronization script like openvas-nvt-sync or greenbone-nvt-sync.
...
```

Important - Notez l'erreur **ERROR: The NVT collection is very small.**

Téléchargez le script **greenbone-nvt-sync** :

```
[root@centos7 ~]# wget
https://www.dropbox.com/scl/fi/10hf8fpdq2yhd821qb5pk/greenbone-nvt-sync?rlkey=7f4taliexlpg54pa1c1yz8czx&st=tkvnjg
55

[root@centos7 ~]# mv greenbone-nvt-sync?rlkey=7f4taliexlpg54pa1c1yz8czx greenbone-nvt-sync
```

Si vous ne pouvez pas téléchargez le script **greenbone-nvt-sync**, copiez son contenu ci-dessous et créez-le :

```
[root@centos7 ~]# vi greenbone-nvt-sync
[root@centos7 ~]# cat greenbone-nvt-sync
#!/bin/sh
# Copyright (C) 2009-2021 Greenbone Networks GmbH
#
# SPDX-License-Identifier: GPL-2.0-or-later
#
# This program is free software; you can redistribute it and/or
# modify it under the terms of the GNU General Public License
# as published by the Free Software Foundation; either version 2
# of the License, or (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU General Public License for more details.
```

```
#
# You should have received a copy of the GNU General Public License
# along with this program; if not, write to the Free Software
# Foundation, Inc., 51 Franklin St, Fifth Floor, Boston, MA 02110-1301 USA.

# This script updates the local Network Vulnerability Tests (NVTs) from the
# Greenbone Security Feed (GSF) or the Greenbone Community Feed (GCF).

VERSION=@OPENVAS_VERSION@

# SETTINGS
# ========

# PRIVATE_SUBDIR defines a subdirectory of the NVT directory that is excluded
# from the feed sync. This is where to place your own NVTs.
if [ -z "$PRIVATE_SUBDIR" ]
then
  PRIVATE_SUBDIR="private"
fi

# RSYNC_DELETE controls whether files which are not part of the repository will
# be removed from the local directory after synchronization. The default value
# for this setting is
# "--delete --exclude \"$PRIVATE_SUBDIR/\"",
# which means that files which are not part of the feed or private directory
# will be deleted.
RSYNC_DELETE="--delete --exclude $PRIVATE_SUBDIR/"

# RSYNC_SSH_OPTS contains options which should be passed to ssh for the rsync
# connection to the repository.
RSYNC_SSH_OPTS="-o \"UserKnownHostsFile=/dev/null\" -o \"StrictHostKeyChecking=no\""

# RSYNC_COMPRESS specifies the compression level to use for the rsync connection.
RSYNC_COMPRESS="--compress-level=9"
```

```
# RSYNC_CHMOD specifies the permissions to chmod the files to.
RSYNC_CHMOD="--perms --chmod=Fugo+r,Fug+w,Dugo-s,Dugo+rx,Dug+w"

# Verbosity flag for rsync. "-q" means a quiet rsync, "-v" a verbose rsync.
RSYNC_VERBOSE="-q"

# RSYNC_OPTIONS controls the general parameters for the rsync connection.
RSYNC_OPTIONS="--links --times --omit-dir-times $RSYNC_VERBOSE --recursive --partial --progress"

# Script and feed information which will be made available to user through
# command line options and automated tools.
# Script name which will be used for logging
SCRIPT_NAME="greenbone-nvt-sync"

# Result of selftest () is stored here. If it is not 0, the selftest has failed
# and the sync script is unlikely to work.
SELFTEST_FAIL=0

# Port to use for synchronization. Default value is 24.
PORT=24

# Directory where the OpenVAS configuration is located
OPENVAS_SYSCONF_DIR="@OPENVAS_SYSCONF_DIR@"

# Directory where the feed update lock file will be placed.
OPENVAS_FEED_LOCK_PATH="@OPENVAS_FEED_LOCK_PATH@"

# Location of the GSF Access Key
ACCESS_KEY="@GVM_ACCESS_KEY_DIR@/gsf-access-key"

# If ENABLED is set to 0, the sync script will not perform a synchronization.
ENABLED=1

# LOG_CMD defines the command to use for logging. To have logger log to stderr
```

```
# as well as syslog, add "-s" here. The logging facility is checked. In case of error
# all will be logged in the standard error and the socket error check will be
# disabled.
LOG_CMD="logger -t $SCRIPT_NAME"

check_logger () {
  logger -p daemon.info -t $SCRIPT_NAME "Checking logger" --no-act 1>/dev/null 2>&1
  if [ $? -gt 0 ]
  then
    LOG_CMD="logger -s -t $SCRIPT_NAME"
    $LOG_CMD -p daemon.warning "The log facility is not working as expected. All messages will be written to the
standard error stream."
  fi
}
check_logger


# Source configuration file if it is readable
[ -r $OPENVAS_SYSCONF_DIR/greenbone-nvt-sync.conf ] && . $OPENVAS_SYSCONF_DIR/greenbone-nvt-sync.conf

# NVT_DIR is the place where the NVTs are located.
if [ -z "$NVT_DIR" ]
then
  NVT_DIR="@OPENVAS_NVT_DIR@"
fi

log_write () {
  $LOG_CMD -p daemon.notice $1
}

log_debug () {
  $LOG_CMD -p daemon.debug "$1"
}
```

```
log_info () {
  $LOG_CMD -p daemon.info "$1"
}

log_notice () {
  $LOG_CMD -p daemon.notice "$1"
}

log_warning () {
  $LOG_CMD -p daemon.warning "$1"
}

log_err () {
  $LOG_CMD -p daemon.err "$1"
}

stderr_write ()
{
  echo "$1" > /dev/stderr
}

# Read the general information about the feed origin from
# the file "plugin_feed_info.inc" inside the feed directory.
get_feed_info ()
{
  INFOFILE="$NVT_DIR/plugin_feed_info.inc"
  if [ -r $INFOFILE ] ; then
    FEED_VERSION=`grep PLUGIN_SET $INFOFILE | sed -e 's/[^0-9]//g'`
    FEED_NAME=`awk -F\" '/PLUGIN_FEED/ { print $2 }' $INFOFILE`
    FEED_VENDOR=`awk -F\" '/FEED_VENDOR/ { print $2 }' $INFOFILE`
    FEED_HOME=`awk -F\" '/FEED_HOME/ { print $2 }' $INFOFILE`
    FEED_PRESENT=1
  else
    FEED_PRESENT=0
```

```
  fi

  if [ -z "$FEED_NAME" ] ; then
    FEED_NAME="Unidentified Feed"
  fi

  if [ -z "$FEED_VENDOR" ] ; then
    FEED_VENDOR="Unidentified Vendor"
  fi

  if [ -z "$FEED_HOME" ] ; then
    FEED_HOME="Unidentified Feed Homepage"
  fi
}

# Prevent that root executes this script
if [ "`id -u`" -eq "0" ]
then
  stderr_write "$0 must not be executed as privileged user root"
  stderr_write
  stderr_write "Unlike the actual scanner the sync routine does not need privileges."
  stderr_write "Accidental execution as root would prevent later overwriting of"
  stderr_write "files with a non-privileged user."

  log_err "Denied to run as root"
  exit 1
fi

# Always try to get the information when started.
# This also ensures variables like FEED_PRESENT are set.
get_feed_info

# Determine whether a GSF access key is present. If yes,
# then use the Greenbone Security Feed. Else use the
```

```
# Greenbone Community Feed.
if [ -e $ACCESS_KEY ]
then
  RESTRICTED=1
else
  RESTRICTED=0

  if [ -z "$COMMUNITY_NVT_RSYNC_FEED" ]; then
    COMMUNITY_NVT_RSYNC_FEED=rsync://feed.community.greenbone.net:/nvt-feed
    # An alternative syntax which might work if the above doesn't:
    # COMMUNITY_NVT_RSYNC_FEED=rsync@feed.community.greenbone.net::/nvt-feed
  fi
fi

RSYNC=`command -v rsync`

if [ -z "$TMPDIR" ]; then
  SYNC_TMP_DIR=/tmp
  # If we have mktemp, create a temporary dir (safer)
  if [ -n "`which mktemp`" ]; then
    SYNC_TMP_DIR=`mktemp -t -d greenbone-nvt-sync.XXXXXXXXXX` || { echo "ERROR: Cannot create temporary directory
for file download" >&2; exit 1 ; }
    trap "rm -rf $SYNC_TMP_DIR" EXIT HUP INT TRAP TERM
  fi
else
  SYNC_TMP_DIR="$TMPDIR"
fi

# Initialize this indicator variable with default assuming the
# feed is not up-to-date.
FEED_CURRENT=0

# This function uses gos-state-manager to get information about the settings.
# If gos-state-manager is not installed the values of the settings can not be
```

```
# retrieved.
#
# Input: option
# Output: value as string or empty String if gos-state-manager is not installed
#         or option not set
get_value ()
{
  value=""
  key=$1
  if which gos-state-manager 1>/dev/null 2>&1
  then
    if gos-state-manager get "$key.value" 1>/dev/null 2>&1
    then
      value="$(gos-state-manager get "$key.value")"
    fi
  fi
  echo "$value"
}

# Creates a restricted access copy of the access key if necessary.
setup_temp_access_key () {
  if [ -e "$ACCESS_KEY" ]
  then
    FILE_ACCESS=`stat -c%a "$ACCESS_KEY" | cut -c2-`
  fi
  if [ -n "$FILE_ACCESS" ] && [ "00" != "$FILE_ACCESS" ]
  then
    TEMP_ACCESS_KEY_DIR=`mktemp -d`
    TEMP_ACCESS_KEY="$TEMP_ACCESS_KEY_DIR/gsf-access-key"
    cp "$ACCESS_KEY" "$TEMP_ACCESS_KEY"
    chmod 400 "$TEMP_ACCESS_KEY"
  else
    TEMP_ACCESS_KEY_DIR=""
    TEMP_ACCESS_KEY="$ACCESS_KEY"
```

```
  fi
}

# Deletes the read-only copy of the access key.
cleanup_temp_access_key () {
  if [ -n "$TEMP_ACCESS_KEY_DIR" ]
  then
    rm -rf "$TEMP_ACCESS_KEY_DIR"
  fi
  TEMP_ACCESS_KEY_DIR=""
  TEMP_ACCESS_KEY=""
}

is_feed_current () {
  if [ -z "$FEED_VERSION" ]
  then
    log_write "Could not determine feed version."
    FEED_CURRENT=0
    return $FEED_CURRENT
  fi

  if [ -z "$RSYNC" ]
  then
    log_notice "rsync not available, skipping feed version test"
    FEED_CURRENT=0
    rm -rf $FEED_INFO_TEMP_DIR
    cleanup_temp_access_key
    return 0
  fi

  FEED_INFO_TEMP_DIR=`mktemp -d`

  if [ -e $ACCESS_KEY ]
  then
```

```
    gsmproxy=$(get_value proxy_feed | sed -r -e 's/^.*\/\///' -e 's/:([0-9]+)$/ \1/')
    syncport=$(get_value syncport)
    if [ "$syncport" ]
    then
      PORT="$syncport"
    fi

    read feeduser < $ACCESS_KEY
    custid=`awk -F@ 'NR > 1 { exit }; { print $1 }' $ACCESS_KEY`
    if [ -z "$feeduser" ] || [ -z "$custid" ]
    then
      log_err "Could not determine credentials, aborting synchronization."
      exit 1
    fi

    setup_temp_access_key

    if [ "$gsmproxy" = "proxy_feed" ] || [ -z "$gsmproxy" ]
    then
      RSYNC_SSH_PROXY_CMD=""
    else
      if [ -e $OPENVAS_SYSCONF_DIR/proxyauth ] && [ -r $OPENVAS_SYSCONF_DIR/proxyauth ]
      then
        RSYNC_SSH_PROXY_CMD="-o \"ProxyCommand corkscrew $gsmproxy %h %p $OPENVAS_SYSCONF_DIR/proxyauth\""
      else
        RSYNC_SSH_PROXY_CMD="-o \"ProxyCommand corkscrew $gsmproxy %h %p\""
      fi
    fi

    rsync -e "ssh $RSYNC_SSH_OPTS $RSYNC_SSH_PROXY_CMD -p $PORT -i $TEMP_ACCESS_KEY" $RSYNC_OPTIONS $RSYNC_DELETE
$RSYNC_COMPRESS $RSYNC_CHMOD "$feeduser"plugin_feed_info.inc $FEED_INFO_TEMP_DIR

    if [ $? -ne 0 ]
    then
```

```
    log_err "Error: rsync failed."
    rm -rf "$FEED_INFO_TEMP_DIR"
    exit 1
  fi
else
  # Sleep for five seconds (a previous feed might have been synced a few seconds before) to prevent
  # IP blocking due to network equipment in between keeping the previous connection too long open.
  sleep 5
  log_notice "No Greenbone Security Feed access key found, falling back to Greenbone Community Feed"
  eval "$RSYNC -ltvrP \"$COMMUNITY_NVT_RSYNC_FEED/plugin_feed_info.inc\" \"$FEED_INFO_TEMP_DIR\""
  if [ $? -ne 0 ]
  then
    log_err "rsync failed, aborting synchronization."
    rm -rf "$FEED_INFO_TEMP_DIR"
    exit 1
  fi
fi

FEED_VERSION_SERVER=`grep PLUGIN_SET $FEED_INFO_TEMP_DIR/plugin_feed_info.inc | sed -e 's/[^0-9]//g'`

if [ -z "$FEED_VERSION_SERVER" ]
then
  log_err "Could not determine server feed version."
  rm -rf $FEED_INFO_TEMP_DIR
  cleanup_temp_access_key
  exit 1
fi
# Check against FEED_VERSION
if [ $FEED_VERSION -lt $FEED_VERSION_SERVER ] ; then
  FEED_CURRENT=0
else
  FEED_CURRENT=1
fi
# Cleanup
```

```
  rm -rf "$FEED_INFO_TEMP_DIR"
  cleanup_temp_access_key

  return $FEED_CURRENT
}

do_rsync_community_feed () {
  # Sleep for five seconds (a previous feed might have been synced a few seconds before) to prevent
  # IP blocking due to network equipment in between keeping the previous connection too long open.
  sleep 5
  log_notice "Configured NVT rsync feed: $COMMUNITY_NVT_RSYNC_FEED"
  mkdir -p "$NVT_DIR"
  eval "$RSYNC -ltvrP $RSYNC_DELETE \"$COMMUNITY_NVT_RSYNC_FEED\" \"$NVT_DIR\" --exclude=plugin_feed_info.inc"
  if [ $? -ne 0 ] ; then
    log_err "rsync failed."
    exit 1
  fi
  # Sleep for five seconds (after the above rsync call) to prevent IP blocking due
  # to network equipment in between keeping the previous connection too long open.
  sleep 5
  eval "$RSYNC -ltvrP $RSYNC_DELETE \"$COMMUNITY_NVT_RSYNC_FEED/plugin_feed_info.inc\" \"$NVT_DIR\""
  if [ $? -ne 0 ] ; then
    log_err "rsync failed."
    exit 1
  fi
}

sync_nvts(){
  if [ $ENABLED -ne 1 ]
  then
    log_write "NVT synchronization is disabled, exiting."
    exit 0
  fi
```

```
if [ -e $ACCESS_KEY ]
then
  log_write "Synchronizing NVTs from the Greenbone Security Feed into $NVT_DIR..."
  if [ $FEED_PRESENT -eq 1 ] ; then
    FEEDCOUNT=`grep -E "nasl$|inc$" $NVT_DIR/md5sums | wc -l`
    log_write "Current status: Using $FEED_NAME at version $FEED_VERSION ($FEEDCOUNT NVTs)"
  else
    log_write "Current status: No feed installed."
  fi
  notsynced=1
  retried=0

  mkdir -p "$NVT_DIR"
  read feeduser < $ACCESS_KEY
  custid=`awk -F@ 'NR > 1 { exit }; { print $1 }' $ACCESS_KEY`
  if [ -z "$feeduser" ] || [ -z "$custid" ]
  then
    log_err "Could not determine credentials, aborting synchronization."
    exit 1
  fi

  setup_temp_access_key

  while [ $notsynced -eq 1 ]
  do

    gsmproxy=$(get_value proxy_feed | sed -r -e 's/^.*\/\///' -e 's/:([0-9]+)$/ \1/')
    syncport=$(get_value syncport)
    if [ "$syncport" ]
    then
      PORT="$syncport"
    fi

    if [ "$gsmproxy" = "proxy_feed" ] || [ -z "$gsmproxy" ]
```

```
      then
        RSYNC_SSH_PROXY_CMD=""
      else
        if [ -e $OPENVAS_SYSCONF_DIR/proxyauth ] && [ -r $OPENVAS_SYSCONF_DIR/proxyauth ]; then
          RSYNC_SSH_PROXY_CMD="-o \"ProxyCommand corkscrew $gsmproxy %h %p $OPENVAS_SYSCONF_DIR/proxyauth\""
        else
          RSYNC_SSH_PROXY_CMD="-o \"ProxyCommand corkscrew $gsmproxy %h %p\""
        fi
      fi
      rsync -e "ssh $RSYNC_SSH_OPTS $RSYNC_SSH_PROXY_CMD -p $PORT -i $TEMP_ACCESS_KEY" --
exclude=plugin_feed_info.inc $RSYNC_OPTIONS $RSYNC_DELETE $RSYNC_COMPRESS $RSYNC_CHMOD $feeduser $NVT_DIR
      if [ $? -ne 0 ]  ; then
        log_err "rsync failed, aborting synchronization."
        exit 1
      fi
      rsync -e "ssh $RSYNC_SSH_OPTS $RSYNC_SSH_PROXY_CMD -p $PORT -i $TEMP_ACCESS_KEY" $RSYNC_OPTIONS
$RSYNC_DELETE $RSYNC_COMPRESS $RSYNC_CHMOD "$feeduser"plugin_feed_info.inc $NVT_DIR
      if [ $? -ne 0 ]  ; then
        log_err "rsync failed, aborting synchronization."
        exit 1
      fi
      eval "cd \"$NVT_DIR\" ; md5sum -c --status \"$NVT_DIR/md5sums\""
      if [ $? -ne 0 ]  ; then
        if [ -n "$retried" ]
        then
          log_err "Feed integrity check failed twice, aborting synchronization."
          cleanup_temp_access_key
          exit 1
        else
          log_write "The feed integrity check failed. This may be due to a concurrent feed update or other
temporary issues."
          log_write "Sleeping 15 seconds before retrying ..."
          sleep 15
          retried=1
```

```
        fi
      else
        notsynced=0
      fi
    done
    cleanup_temp_access_key
    log_write "Synchronization with the Greenbone Security Feed successful."
    get_feed_info
    if [ $FEED_PRESENT -eq 1 ] ; then
      FEEDCOUNT=`grep -E "nasl$|inc$" $NVT_DIR/md5sums | wc -l`
      log_write "Current status: Using $FEED_NAME at version $FEED_VERSION ($FEEDCOUNT NVTs)"
    else
      log_write "Current status: No feed installed."
    fi
  else
    log_notice "No Greenbone Security Feed access key found, falling back to Greenbone Community Feed"
    do_rsync_community_feed
  fi
}

do_self_test ()
{
  MD5SUM_AVAIL=`command -v md5sum`
  if [ $? -ne 0 ] ; then
    SELFTEST_FAIL=1
    stderr_write "The md5sum binary could not be found."
  fi

  RSYNC_AVAIL=`command -v rsync`
  if [ $? -ne 0 ] ; then
    SELFTEST_FAIL=1
    stderr_write "The rsync binary could not be found."
  fi
}
```

```
do_describe ()
{
  echo "This script synchronizes an NVT collection with the '$FEED_NAME'."
  echo "The '$FEED_NAME' is provided by '$FEED_VENDOR'."
  echo "Online information about this feed: '$FEED_HOME'."
}

do_feedversion () {
  if [ $FEED_PRESENT -eq 1 ] ; then
    echo $FEED_VERSION
  else
    stderr_write "The file containing the feed version could not be found."
    exit 1
  fi
}

do_sync ()
{
  do_self_test
  if [ $SELFTEST_FAIL -ne 0 ] ; then
    exit $SELFTEST_FAIL
  fi

  if [ $FEED_CURRENT -eq 1 ]
  then
    log_write "Feed is already current, skipping synchronization."
  else
    (
      chmod +660 $OPENVAS_FEED_LOCK_PATH
      flock -n 9
      if [ $? -eq 1 ] ; then
          log_warning "Another process related to the feed update is already running"
          exit 1
      fi
```

```
      date > $OPENVAS_FEED_LOCK_PATH
      sync_nvts
      echo -n $OPENVAS_FEED_LOCK_PATH
    )9>>$OPENVAS_FEED_LOCK_PATH
  fi
}

do_help () {
  echo "$0: Sync NVT data"
  echo " --describe     display current feed info"
  echo " --feedcurrent  just check if feed is up-to-date"
  echo " --feedversion  display version of this feed"
  echo " --help         display this help"
  echo " --identify     display information"
  echo " --nvtdir dir   set dir as NVT directory"
  echo " --selftest     perform self-test and set exit code"
  echo " --verbose      makes the sync process print details"
  echo " --version      display version"
  echo ""
  echo ""
  echo "Environment variables:"
  echo "NVT_DIR         where to extract plugins (absolute path)"
  echo "PRIVATE_SUBDIR  subdirectory of \$NVT_DIR to exclude from synchronization"
  echo "TMPDIR          temporary directory used to download the files"
  echo "Note that you can use standard ones as well (e.g. RSYNC_PROXY) for rsync"
  echo ""
  exit 0
}

while test $# -gt 0; do
  case "$1" in
    --version)
      echo $VERSION
      exit 0
```

```
    ;;
  --identify)
    echo "NVTSYNC|$SCRIPT_NAME|$VERSION|$FEED_NAME|$RESTRICTED|NVTSYNC"
    exit 0
    ;;
  --selftest)
    do_self_test
    exit $SELFTEST_FAIL
    ;;
  --describe)
    do_describe
    exit 0
    ;;
  --feedversion)
    do_feedversion
    exit 0
    ;;
  --help)
    do_help
    exit 0
    ;;
  --nvt-dir)
    NVT_DIR="$2"
    shift
    ;;
  --feedcurrent)
    is_feed_current
    exit $?
    ;;
  --verbose)
    RSYNC_VERBOSE="-v"
    ;;
esac
shift
```

```
done

do_sync

exit 0
```

Rendez le script exécutable :

```
[root@centos7 ~]# chmod +x greenbone-nvt-sync
```

Déplacez le script vers **/usr/sbin/** :

```
[root@centos7 ~]# mv greenbone-nvt-sync /usr/sbin
mv: overwrite ‘/usr/sbin/greenbone-nvt-sync’? y
```

Devenez l'utilisateur trainee et mettez à jour les modules d'extensions de OpenVAS :

```
[root@centos7 ~]# su - trainee
Last login: Thu Mar  4 10:28:01 UTC 2021 from ns3072874.ip-79-137-68.eu on pts/0
[trainee@centos7 ~]$ greenbone-nvt-sync
...
[trainee@centos7 ~]$ exit
[root@centos7 ~]#
```

Déplacez les plugins vers le répertoire **/var/lib/openvas/plugins** :

```
[root@centos7 ~]# mv /home/trainee/@OPENVAS_NVT_DIR@/* /var/lib/openvas/plugins
```

Vérifiez ensuite la réussite de la commande précédente :

```
[root@centos7 ~]# ls -l /var/lib/openvas/plugins/ | more
total 36288
drwxr-xr-x   2 trainee trainee   32768 Mar  3 11:33 2008
```

```
drwxr-xr-x   2 trainee trainee   77824 Mar  3 11:33 2009
drwxr-xr-x   2 trainee trainee   77824 Mar  4 10:59 2010
drwxr-xr-x   2 trainee trainee  253952 Mar  3 11:33 2011
drwxr-xr-x   2 trainee trainee  307200 Mar  3 11:33 2012
drwxr-xr-x   3 trainee trainee  266240 Mar  3 11:33 2013
drwxr-xr-x   3 trainee trainee  249856 Mar  3 11:33 2014
drwxr-xr-x   3 trainee trainee  401408 Mar  3 11:33 2015
drwxr-xr-x   3 trainee trainee  389120 Mar  4 10:59 2016
drwxr-xr-x  64 trainee trainee  282624 Mar  3 11:33 2017
drwxr-xr-x 289 trainee trainee   12288 Feb 16 12:02 2018
drwxr-xr-x 214 trainee trainee   12288 Nov 25 11:24 2019
drwxr-xr-x 180 trainee trainee    4096 Jan 25 11:10 2020
drwxr-xr-x  72 trainee trainee    4096 Mar  4 10:59 2021
-rw-r--r--   1 trainee trainee    3470 Jul 20  2020 404.inc
-rw-r--r--   1 trainee trainee    3012 Dec  9 10:01 aas_detect.nasl
-rw-r--r--   1 trainee trainee    3166 Aug 27  2020 adaptbb_detect.nasl
-rw-r--r--   1 trainee trainee    4016 Aug 27  2020 AfterLogic_WebMail_Pro_detect.nasl
-rw-r--r--   1 trainee trainee    3176 Nov 12 11:33 amanda_detect.nasl
-rw-r--r--   1 trainee trainee    3173 Nov 12 11:33 amanda_version.nasl
-rw-r--r--   1 trainee trainee    3549 Mar  1 11:32 apache_server_info.nasl
-rw-r--r--   1 trainee trainee    7491 Mar  4 10:59 apache_SSL_complain.nasl
-rw-r--r--   1 trainee trainee    4679 Nov 12 11:33 apcnisd_detect.nasl
-rw-r--r--   1 trainee trainee    3303 Aug 27  2020 AproxEngine_detect.nasl
-rw-r--r--   1 trainee trainee    2706 Feb 14  2020 arcserve_backup_detect.nasl
-rw-r--r--   1 trainee trainee    2700 Mar  3 11:33 arkoon.nasl
-rw-r--r--   1 trainee trainee    7477 Nov 12 11:33 asip-status.nasl
-rw-r--r--   1 trainee trainee    4522 Aug 27  2020 atmail_detect.nasl
drwxr-xr-x   4 trainee trainee   20480 Mar  2 12:14 attic
-rw-r--r--   1 trainee trainee    2703 Nov 12 11:33 auth_enabled.nasl
-rw-r--r--   1 trainee trainee    2573 May  7  2020 aventail_asap.nasl
-rw-r--r--   1 trainee trainee    4620 Dec 21 15:00 awstats_detect.nasl
-rw-r--r--   1 trainee trainee    3711 Aug 27  2020 axigen_web_detect.nasl
-rw-r--r--   1 trainee trainee 1639798 Feb 14  2020 bad_dsa_ssh_host_keys.txt
--More--
```

Exécutez de nouveau la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
...
Step 2: Checking OpenVAS Manager ...
        OK: OpenVAS Manager is present in version 6.0.9.
        ERROR: No client certificate file of OpenVAS Manager found.
        FIX: Run 'openvas-mkcert-client -n -i'

 ERROR: Your OpenVAS-8 installation is not yet complete!
...
```

Important - Notez l'erreur **ERROR: No client certificate file of OpenVAS Manager found.**

Consultez la signification des options suggérées pour la commande **openvas-mkcert-client** :

```
[root@centos7 ~]# openvas-mkcert-client --help
/bin/openvas-mkcert-client: illegal option -- -
Usage:
  openvas-mkcert-client [OPTION...] - Create SSL client certificates for OpenVAS.

Options:
  -h           Display help
  -n           Run non-interactively, create certificates
               and register with the OpenVAS scanner
  -i           Install client certificates for use with OpenVAS manager
```

Exécutez donc la commande **openvas-mkcert-client -i** :

```
[root@centos7 ~]# openvas-mkcert-client -i
```

```
This script will now ask you the relevant information to create the SSL client certificates for OpenVAS.

Client certificates life time in days [365]: 3650
Your country (two letter code) [DE]: UK
Your state or province name [none]: SURREY
Your location (e.g. town) [Berlin]: ADDLESTONE
Your organization [none]: I2TCH LIMITED
Your organizational unit [none]: TRAINING
**********
We are going to ask you some question for each client certificate.

If some question has a default answer, you can force an empty answer by entering a single dot '.'

*********
Client certificates life time in days [3650]:
Country (two letter code) [UK]:
State or province name [SURREY]:
Location (e.g. town) [ADDLESTONE]:
Organization [I2TCH LIMITED]:
Organization unit [TRAINING]:
e-Mail []: infos@i2tch.eu
Generating RSA private key, 4096 bit long modulus
....++
.......++
e is 65537 (0x10001)
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) [DE]:State or Province Name (full name) [Some-State]:Locality Name (eg, city)
[]:Organization Name (eg, company) [Internet Widgits Pty Ltd]:Organizational Unit Name (eg, section) []:Common
```

```
Name (eg, your name or your server's hostname) []:Email Address []:Using configuration from /tmp/openvas-mkcert-client.13962/stdC.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'UK'
stateOrProvinceName   :ASN.1 12:'SURREY'
localityName          :ASN.1 12:'ADDLESTONE'
organizationName      :ASN.1 12:'I2TCH LIMITED'
organizationalUnitName:ASN.1 12:'TRAINING'
commonName            :ASN.1 12:'om'
emailAddress          :IA5STRING:'infos@i2tch.eu'
Certificate is to be certified until Jun 17 02:03:34 2028 GMT (3650 days)

Write out database with 1 new entries
Data Base Updated
/bin/openvas-mkcert-client: line 370: [: argument expected
```

Exécutez encore une fois la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
...
Step 2: Checking OpenVAS Manager ...
        OK: OpenVAS Manager is present in version 6.0.9.
        OK: OpenVAS Manager client certificate is present as /etc/pki/openvas/CA/clientcert.pem.
        ERROR: No OpenVAS Manager database found. (Tried: /var/lib/openvas/mgr/tasks.db)
        FIX: Run 'openvasmd --rebuild' while OpenVAS Scanner is running.
        WARNING: OpenVAS Scanner is NOT running!
        SUGGEST: Start OpenVAS Scanner (openvassd).

 ERROR: Your OpenVAS-8 installation is not yet complete!
...
```

Important - Notez l'erreur **ERROR: No OpenVAS Manager database found. (Tried: /var/lib/openvas/mgr/tasks.db).**

Afin de générer la base de données, OpenVAS Scanner doit être en cours d'exécution. Activez et démarrez donc le service :

```
[root@centos7 ~]# systemctl enable openvas-scanner
Created symlink from /etc/systemd/system/multi-user.target.wants/openvas-scanner.service to
/usr/lib/systemd/system/openvas-scanner.service.
[root@centos7 ~]# systemctl start openvas-scanner
[root@centos7 ~]# systemctl status openvas-scanner
● openvas-scanner.service - OpenVAS Scanner
   Loaded: loaded (/usr/lib/systemd/system/openvas-scanner.service; enabled; vendor preset: disabled)
   Active: active (running) since Wed 2018-06-20 04:08:49 CEST; 11s ago
  Process: 16956 ExecStart=/usr/sbin/openvassd $SCANNER_PORT $SCANNER_LISTEN $SCANNER_SRCIP (code=exited,
status=0/SUCCESS)
 Main PID: 16957 (openvassd)
   CGroup: /system.slice/openvas-scanner.service
           ├─16957 openvassd: Reloaded 200 of 45658 NVTs (0% / ETA: 26:31)
           └─16958 openvassd (Loading Handler)

Jun 20 04:08:49 centos7.fenestros.loc systemd[1]: Starting OpenVAS Scanner...
Jun 20 04:08:49 centos7.fenestros.loc systemd[1]: Started OpenVAS Scanner.
```

Construisez maintenant la base de données :

```
[root@centos7 ~]# openvasmd --rebuild --progress
Rebuilding NVT cache... -
```

Exécutez de nouveau la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
```

```
...
Step 2: Checking OpenVAS Manager ...
        OK: OpenVAS Manager is present in version 6.0.9.
        OK: OpenVAS Manager client certificate is present as /etc/pki/openvas/CA/clientcert.pem.
        OK: OpenVAS Manager database found in /var/lib/openvas/mgr/tasks.db.
        OK: Access rights for the OpenVAS Manager database are correct.
        OK: sqlite3 found, extended checks of the OpenVAS Manager installation enabled.
        OK: OpenVAS Manager database is at revision 146.
        OK: OpenVAS Manager expects database at revision 146.
        OK: Database schema is up to date.
        OK: OpenVAS Manager database contains information about 45654 NVTs.
        ERROR: No users found. You need to create at least one user to log in.
        It is recommended to have at least one user with role Admin.
        FIX: create a user by running 'openvasmd --create-user=<name> --role=Admin && openvasmd --user=<name> --
new-password=<password>'
...
```

Important - Notez l'erreur **ERROR: No users found. You need to create at least one user to log in.**

Créez donc un utilisateur :

```
[root@centos7 ~]# openvasmd --create-user=fenestros --role=Admin
User created with password 'e366e2ec-8d8f-442d-9d19-5a158ccc50ae'.
[root@centos7 ~]# openvasmd --user=fenestros --new-password=fenestros
```

Exécutez encore une fois la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
...
Step 2: Checking OpenVAS Manager ...
```

```
        OK: OpenVAS Manager is present in version 6.0.9.
        OK: OpenVAS Manager client certificate is present as /etc/pki/openvas/CA/clientcert.pem.
        OK: OpenVAS Manager database found in /var/lib/openvas/mgr/tasks.db.
        OK: Access rights for the OpenVAS Manager database are correct.
        OK: sqlite3 found, extended checks of the OpenVAS Manager installation enabled.
        OK: OpenVAS Manager database is at revision 146.
        OK: OpenVAS Manager expects database at revision 146.
        OK: Database schema is up to date.
        OK: OpenVAS Manager database contains information about 45654 NVTs.
        OK: At least one user exists.
        ERROR: No OpenVAS SCAP database found. (Tried: /var/lib/openvas/scap-data/scap.db)
        FIX: Run a SCAP synchronization script like openvas-scapdata-sync or greenbone-scapdata-sync.

 ERROR: Your OpenVAS-8 installation is not yet complete!
...
```

Important - Notez l'erreur **ERROR: No OpenVAS SCAP database found. (Tried: /var/lib/openvas/scap-data/scap.db).**

La prochaine étape donc consiste à récupérer la base SCAP (Security Content Automation Protocol).

Téléchargez le script **greenbone-feed-sync** :

```
[root@centos7 ~]# wget
https://www.dropbox.com/scl/fi/10hf8fpdq2yhd821qb5pk/greenbone-nvt-sync?rlkey=7f4taliexlpg54pa1c1yz8czx&st=tkvnjg
55

[root@centos7 ~]# mv greenbone-nvt-sync?rlkey=7f4taliexlpg54pa1c1yz8czx greenbone-nvt-sync
```

Si vous ne pouvez pas téléchargez le script **greenbone-feed-sync**, copiez son contenu ci-dessous et créez-le :

```
[root@centos7 ~]# vi greenbone-feed-sync
[root@centos7 ~]# cat greenbone-feed-sync
#!/bin/sh
# Copyright (C) 2011-2020 Greenbone Networks GmbH
#
# SPDX-License-Identifier: AGPL-3.0-or-later
#
# This program is free software: you can redistribute it and/or modify
# it under the terms of the GNU Affero General Public License as
# published by the Free Software Foundation, either version 3 of the
# License, or (at your option) any later version.
#
# This program is distributed in the hope that it will be useful,
# but WITHOUT ANY WARRANTY; without even the implied warranty of
# MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the
# GNU Affero General Public License for more details.
#
# You should have received a copy of the GNU Affero General Public License
# along with this program.  If not, see <http://www.gnu.org/licenses/>.

# This script synchronizes a GVM installation with the
# feed data from either the Greenbone Security Feed (in
# case a GSF access key is present) or else from the Greenbone
# Community Feed.

log_notice () {
  $LOG_CMD -p daemon.notice "$1"
}



########## SETTINGS
########## ========

# PRIVATE_SUBDIR defines a subdirectory of the feed data directory
```

```
# where files not part of the feed or database will not be deleted by rsync.
if [ -z "$PRIVATE_SUBDIR" ]
then
  PRIVATE_SUBDIR="private"
fi

# RSYNC_DELETE controls whether files which are not part of the repository will
# be removed from the local directory after synchronization. The default value
# for this setting is
# "--delete --exclude feed.xml --exclude $PRIVATE_SUBDIR/",
# which means that files which are not part of the feed, feed info or private
# directory will be deleted.
RSYNC_DELETE="--delete --exclude feed.xml --exclude \"$PRIVATE_SUBDIR/\""

# RSYNC_SSH_OPTS contains options which should be passed to ssh for the rsync
# connection to the repository.
RSYNC_SSH_OPTS="-o \"UserKnownHostsFile=/dev/null\" -o \"StrictHostKeyChecking=no\""

# RSYNC_COMPRESS specifies the compression level to use for the rsync connection.
RSYNC_COMPRESS="--compress-level=9"

# PORT controls the outgoing TCP port for updates. If PAT/Port-Translation is
# not used, this should be "24". For some application layer firewalls or gates
# the value 22 (Standard SSH) is useful. Only change if you know what you are
# doing.
PORT=24

# SCRIPT_NAME is the name the scripts will use to identify itself and to mark
# log messages.
SCRIPT_NAME="greenbone-feed-sync"

# LOG_CMD defines the command to use for logging. To have logger log to stderr
# as well as syslog, add "-s" here.
LOG_CMD="logger -t $SCRIPT_NAME"
```

```
# LOCK_FILE is the name of the file used to lock the feed during sync or update.
if [ -z "$LOCK_FILE" ]
then
  LOCK_FILE="@GVM_FEED_LOCK_PATH@"
fi



########## GLOBAL VARIABLES
########## ================

VERSION=@GVMD_VERSION@

[ -r "@GVM_SYSCONF_DIR@/greenbone-feed-sync.conf" ] && . "@GVM_SYSCONF_DIR@/greenbone-feed-sync.conf"

if [ -z "$DROP_USER" ]; then
  DROP_USER="@GVM_DEFAULT_DROP_USER@"
fi

ACCESSKEY="@GVM_ACCESS_KEY_DIR@/gsf-access-key"

# Note when running as root or restart as $DROP_USER if defined
if [ $(id -u) -eq 0 ]
then
  if [ -z "$DROP_USER" ]
  then
    log_notice "Running as root"
  else
    log_notice "Started as root, restarting as $DROP_USER"
    su --shell /bin/sh --command "$0 $*" "$DROP_USER"
    exit $?
  fi
fi

# Determine whether a GSF access key is present. If yes,
```

```
# then use the Greenbone Security Feed. Else use the
# Greenbone Community Feed.
if [ -e $ACCESSKEY ]
then
  RESTRICTED=1

  if [ -z "$FEED_VENDOR" ]; then
    FEED_VENDOR="Greenbone Networks GmbH"
  fi

  if [ -z "$FEED_HOME" ]; then
    FEED_HOME="https://www.greenbone.net/en/security-feed/"
  fi

else
  RESTRICTED=0

  if [ -z "$FEED_VENDOR" ]; then
    FEED_VENDOR="Greenbone Networks GmbH"
  fi

  if [ -z "$FEED_HOME" ]; then
    FEED_HOME="https://community.greenbone.net/t/about-greenbone-community-feed-gcf/1224"
  fi

fi

RSYNC=`command -v rsync`

# Current supported feed types (for --type parameter)
FEED_TYPES_SUPPORTED="CERT, SCAP or GVMD_DATA"

########## FUNCTIONS
########## =========
```

```
log_debug () {
  $LOG_CMD -p daemon.debug "$1"
}

log_info () {
  $LOG_CMD -p daemon.info "$1"
}

log_warning () {
  $LOG_CMD -p daemon.warning "$1"
}

log_err () {
  $LOG_CMD -p daemon.err "$1"
}

init_feed_type () {
  if [ -z "$FEED_TYPE" ]
  then
    echo "No feed type given to --type parameter"
    log_err "No feed type given to --type parameter"
    exit 1
  elif [ "CERT" = "$FEED_TYPE" ]
  then
    [ -r "@GVM_SYSCONF_DIR@/greenbone-certdata-sync.conf" ] && . "@GVM_SYSCONF_DIR@/greenbone-certdata-sync.conf"

    FEED_TYPE_LONG="CERT data"
    FEED_DIR="@GVM_CERT_DATA_DIR@"
    TIMESTAMP="$FEED_DIR/timestamp"
    SCRIPT_ID="CERTSYNC"

    if [ -z "$COMMUNITY_CERT_RSYNC_FEED" ]; then
      COMMUNITY_RSYNC_FEED="rsync://feed.community.greenbone.net:/cert-data"
      # An alternative syntax which might work if the above doesn't:
```

```
    # COMMUNITY_RSYNC_FEED="rsync@feed.community.greenbone.net::cert-data"
  else
    COMMUNITY_RSYNC_FEED="$COMMUNITY_CERT_RSYNC_FEED"
  fi

  GSF_RSYNC_PATH="/cert-data"

  if [ -e $ACCESSKEY ]; then
    if [ -z "$FEED_NAME" ]; then
      FEED_NAME="Greenbone CERT Feed"
    fi
  else
    if [ -z "$FEED_NAME" ]; then
      FEED_NAME="Greenbone Community CERT Feed"
    fi
  fi
elif [ "SCAP" = "$FEED_TYPE" ]
then
  [ -r "@GVM_SYSCONF_DIR@/greenbone-scapdata-sync.conf" ] && . "@GVM_SYSCONF_DIR@/greenbone-scapdata-sync.conf"

  FEED_TYPE_LONG="SCAP data"
  FEED_DIR="@GVM_SCAP_DATA_DIR@"
  TIMESTAMP="$FEED_DIR/timestamp"
  SCRIPT_ID="SCAPSYNC"

  if [ -z "$COMMUNITY_SCAP_RSYNC_FEED" ]; then
    COMMUNITY_RSYNC_FEED="rsync://feed.community.greenbone.net:/scap-data"
    # An alternative syntax which might work if the above doesn't:
    # COMMUNITY_RSYNC_FEED="rsync@feed.community.greenbone.net::scap-data"
  else
    COMMUNITY_RSYNC_FEED="$COMMUNITY_SCAP_RSYNC_FEED"
  fi

  GSF_RSYNC_PATH="/scap-data"
```

```
    if [ -e $ACCESSKEY ]; then
      if [ -z "$FEED_NAME" ]; then
        FEED_NAME="Greenbone SCAP Feed"
      fi
    else
      if [ -z "$FEED_NAME" ]; then
        FEED_NAME="Greenbone Community SCAP Feed"
      fi
    fi
  elif [ "GVMD_DATA" = "$FEED_TYPE" ]
  then
    [ -r "@GVM_SYSCONF_DIR@/greenbone-data-objects-sync.conf" ] && . "@GVM_SYSCONF_DIR@/greenbone-data-objects-
sync.conf"

    FEED_TYPE_LONG="gvmd Data"
    FEED_DIR="@GVMD_FEED_DIR@"
    TIMESTAMP="$FEED_DIR/timestamp"
    SCRIPT_ID="GVMD_DATA_SYNC"

    if [ -z "$COMMUNITY_GVMD_DATA_RSYNC_FEED" ]; then
      COMMUNITY_RSYNC_FEED="rsync://feed.community.greenbone.net:/data-objects/gvmd/"
      # An alternative syntax which might work if the above doesn't:
      # COMMUNITY_RSYNC_FEED="rsync@feed.community.greenbone.net::data-objects/gvmd/"
    else
      COMMUNITY_RSYNC_FEED="$COMMUNITY_GVMD_DATA_RSYNC_FEED"
    fi

    GSF_RSYNC_PATH="/data-objects/gvmd/"

    if [ -e $ACCESSKEY ]; then
      if [ -z "$FEED_NAME" ]; then
        FEED_NAME="Greenbone gvmd Data Feed"
      fi
    else
```

```
      if [ -z "$FEED_NAME" ]; then
        FEED_NAME="Greenbone Community gvmd Data Feed"
      fi
    fi
  else
    echo "Invalid feed type $FEED_TYPE given to --type parameter. Currently supported: $FEED_TYPES_SUPPORTED"
    log_err "Invalid feed type $FEED_TYPE given to --type parameter. Currently supported: $FEED_TYPES_SUPPORTED"
    exit 1
  fi
}

write_feed_xml () {
  if [ -r $TIMESTAMP ]
  then
    FEED_VERSION=`cat $TIMESTAMP`
  else
    FEED_VERSION=0
  fi

  mkdir -p $FEED_DIR
  echo '<feed id="6315d194-4b6a-11e7-a570-28d24461215b">' > $FEED_DIR/feed.xml
  echo "<type>$FEED_TYPE</type>" >> $FEED_DIR/feed.xml
  echo "<name>$FEED_NAME</name>" >> $FEED_DIR/feed.xml
  echo "<version>$FEED_VERSION</version>" >> $FEED_DIR/feed.xml
  echo "<vendor>$FEED_VENDOR</vendor>" >> $FEED_DIR/feed.xml
  echo "<home>$FEED_HOME</home>" >> $FEED_DIR/feed.xml
  echo "<description>" >> $FEED_DIR/feed.xml
  echo "This script synchronizes a $FEED_TYPE collection with the '$FEED_NAME'." >> $FEED_DIR/feed.xml
  echo "The '$FEED_NAME' is provided by '$FEED_VENDOR'." >> $FEED_DIR/feed.xml
  echo "Online information about this feed: '$FEED_HOME'." >> $FEED_DIR/feed.xml
  echo "</description>" >> $FEED_DIR/feed.xml
  echo "</feed>" >> $FEED_DIR/feed.xml
}
```

```
create_tmp_key () {
  KEYTEMPDIR=`mktemp -d`
  cp "$ACCESSKEY" "$KEYTEMPDIR"
  TMPACCESSKEY="$KEYTEMPDIR/gsf-access-key"
  chmod 400 "$TMPACCESSKEY"
}

remove_tmp_key () {
  rm -rf "$KEYTEMPDIR"
}

set_interrupt_trap () {
  trap "handle_interrupt $1" 2
}

handle_interrupt () {
  echo "$1:X" >&3
}

do_describe () {
  echo "This script synchronizes a $FEED_TYPE collection with the '$FEED_NAME'."
  echo "The '$FEED_NAME' is provided by '$FEED_VENDOR'."
  echo "Online information about this feed: '$FEED_HOME'."
}

do_feedversion () {
  if [ -r $TIMESTAMP ]; then
      cat $TIMESTAMP
  fi
}

# This function uses gos-state-manager to get information about the settings.
# gos-state-manager is only available on a Greenbone OS.
# If gos-state-manager is missing the settings values can not be retrieved.
```

```
#
# Input: option
# Output: value as string or empty String if gos-state-manager is not installed
#         or option not set
get_value ()
{
  value=""
  key=$1
  if which gos-state-manager 1>/dev/null 2>&1
  then
    if gos-state-manager get "$key.value" 1>/dev/null 2>&1
    then
      value="$(gos-state-manager get "$key.value")"
    fi
  fi
  echo "$value"
}

is_feed_current () {
  if [ -r $TIMESTAMP ]
  then
    FEED_VERSION=`cat $TIMESTAMP`
  fi

  if [ -z "$FEED_VERSION" ]
  then
    log_warning "Could not determine feed version."
    FEED_CURRENT=0
    return $FEED_CURRENT
  fi

  FEED_INFO_TEMP_DIR=`mktemp -d`

  if [ -e $ACCESSKEY ]
```

```
  then
    read feeduser < $ACCESSKEY
    custid_at_host=`head -1 $ACCESSKEY | cut -d : -f 1`

    if [ -z "$feeduser" ] || [ -z "$custid_at_host" ]
    then
      log_err "Could not determine credentials, aborting synchronization."
      rm -rf "$FEED_INFO_TEMP_DIR"
      exit 1
    fi

    gsmproxy=$(get_value proxy_feed | sed -r -e 's/^.*\/\///' -e 's/:([0-9]+)$/ \1/')
    syncport=$(get_value syncport)
    if [ "$syncport" ]
    then
      PORT="$syncport"
    fi

    if [ -z "$gsmproxy" ] || [ "$gsmproxy" = "proxy_feed" ]
    then
      RSYNC_SSH_PROXY_CMD=""
    else
      if [ -e $GVM_SYSCONF_DIR/proxyauth ] && [ -r $GVM_SYSCONF_DIR/proxyauth ]; then
        RSYNC_SSH_PROXY_CMD="-o \"ProxyCommand corkscrew $gsmproxy %h %p $GVM_SYSCONF_DIR/proxyauth\""
      else
        RSYNC_SSH_PROXY_CMD="-o \"ProxyCommand corkscrew $gsmproxy %h %p\""
      fi
    fi
    create_tmp_key
    rsync -e "ssh $RSYNC_SSH_OPTS $RSYNC_SSH_PROXY_CMD -p $PORT -i $TMPACCESSKEY" -ltvrP --chmod=D+x
$RSYNC_DELETE $RSYNC_COMPRESS $custid_at_host:$GSF_RSYNC_PATH/timestamp "$FEED_INFO_TEMP_DIR"
    if [ $? -ne 0 ]
    then
      log_err "rsync failed, aborting synchronization."
```

```
    rm -rf "$FEED_INFO_TEMP_DIR"
    remove_tmp_key
    exit 1
  fi
  remove_tmp_key
else
  # Sleep for five seconds (a previous feed might have been synced a few seconds before) to prevent
  # IP blocking due to network equipment in between keeping the previous connection too long open.
  sleep 5
  log_notice "No Greenbone Security Feed access key found, falling back to Greenbone Community Feed"
  eval "$RSYNC -ltvrP \"$COMMUNITY_RSYNC_FEED/timestamp\" \"$FEED_INFO_TEMP_DIR\""
  if [ $? -ne 0 ]
  then
    log_err "rsync failed, aborting synchronization."
    rm -rf "$FEED_INFO_TEMP_DIR"
    exit 1
  fi
fi

FEED_VERSION_SERVER=`cat "$FEED_INFO_TEMP_DIR/timestamp"`

if [ -z "$FEED_VERSION_SERVER" ]
then
  log_err "Could not determine server feed version."
  rm -rf "$FEED_INFO_TEMP_DIR"
  exit 1
fi

# Check against FEED_VERSION
if [ $FEED_VERSION -lt $FEED_VERSION_SERVER ]; then
  FEED_CURRENT=0
else
  FEED_CURRENT=1
fi
```

```
  # Cleanup
  rm -rf "$FEED_INFO_TEMP_DIR"

  return $FEED_CURRENT
}

do_help () {
  echo "$0: Sync feed data"

  if [ -e $ACCESSKEY ]
  then
    echo "GSF access key found: Using Greenbone Security Feed"
  else
    echo "No GSF access key found: Using Community Feed"
  fi

  echo " --describe      display current feed info"
  echo " --feedversion   display version of this feed"
  echo " --help          display this help"
  echo " --identify      display information"
  echo " --selftest      perform self-test"
  echo " --type <TYPE>   choose type of data to sync ($FEED_TYPES_SUPPORTED)"
  echo " --version       display version"
  echo ""
  exit 0
}

do_rsync_community_feed () {
  if [ -z "$RSYNC" ]; then
    log_err "rsync not found!"
  else
    # Sleep for five seconds (after is_feed_current) to prevent IP blocking due to
    # network equipment in between keeping the previous connection too long open.
    sleep 5
```

```
    log_notice "Using rsync: $RSYNC"
    log_notice "Configured $FEED_TYPE_LONG rsync feed: $COMMUNITY_RSYNC_FEED"
    mkdir -p "$FEED_DIR"
    eval "$RSYNC -ltvrP $RSYNC_DELETE \"$COMMUNITY_RSYNC_FEED\" \"$FEED_DIR\""
    if [ $? -ne 0 ]; then
      log_err "rsync failed. Your $FEED_TYPE_LONG might be broken now."
      exit 1
    fi
  fi
}

do_sync_community_feed () {
  if [ -z "$RSYNC" ]; then
    log_err "rsync not found!"
    log_err "No utility available in PATH environment variable to download Feed data"
    exit 1
  else
    log_notice "Will use rsync"
    do_rsync_community_feed
  fi
}

sync_feed_data(){
  if [ -e $ACCESSKEY ]
  then
    log_notice "Found Greenbone Security Feed subscription file, trying to synchronize with Greenbone
$FEED_TYPE_LONG Repository ..."
    notsynced=1

    mkdir -p "$FEED_DIR"
    read feeduser < $ACCESSKEY
    custid_at_host=`head -1 $ACCESSKEY | cut -d : -f 1`

    if [ -z "$feeduser" ] || [ -z "$custid_at_host" ]
```

```
    then
      log_err "Could not determine credentials, aborting synchronization."
      exit 1
    fi

    while [ 0 -ne "$notsynced" ]
    do

      gsmproxy=$(get_value proxy_feed | sed -r -e 's/^.*\/\///' -e 's/:([0-9]+)$/ \1/')
      syncport=$(get_value syncport)
      if [ "$syncport" ]
      then
        PORT="$syncport"
      fi

      if [ -z "$gsmproxy" ] || [ "$gsmproxy" = "proxy_feed" ]
      then
        RSYNC_SSH_PROXY_CMD=""
      else
        if [ -e $GVM_SYSCONF_DIR/proxyauth ] && [ -r $GVM_SYSCONF_DIR/proxyauth ]; then
          RSYNC_SSH_PROXY_CMD="-o \"ProxyCommand corkscrew $gsmproxy %h %p $GVM_SYSCONF_DIR/proxyauth\""
        else
          RSYNC_SSH_PROXY_CMD="-o \"ProxyCommand corkscrew $gsmproxy %h %p\""
        fi
      fi
      create_tmp_key
      rsync -e "ssh $RSYNC_SSH_OPTS $RSYNC_SSH_PROXY_CMD -p $PORT -i $ACCESSKEY" -ltvrP --chmod=D+x $RSYNC_DELETE
$RSYNC_COMPRESS $custid_at_host:$GSF_RSYNC_PATH/ $FEED_DIR
      if [ 0 -ne "$?" ]; then
        log_err "rsync failed, aborting synchronization."
        remove_tmp_key
        exit 1
      fi
      remove_tmp_key
```

```
      notsynced=0
    done
    log_notice "Synchronization with the Greenbone $FEED_TYPE_LONG Repository successful."
  else
    log_notice "No Greenbone Security Feed access key found, falling back to Greenbone Community Feed"
    do_sync_community_feed
  fi

  write_feed_xml
}

do_self_test () {
  if [ -z "$SELFTEST_STDERR" ]
  then
    SELFTEST_STDERR=0
  fi

  if [ -z "$RSYNC" ]
  then
    if [ 0 -ne $SELFTEST_STDERR ]
    then
      echo "rsync not found (required)." 1>&2
    fi
    log_err "rsync not found (required)."
    SELFTEST_FAIL=1
  fi
}


########## START
########## =====

while test $# -gt 0; do
  case "$1" in
```

```
    "--version"|"--identify"|"--describe"|"--feedversion"|"--selftest"|"--feedcurrent")
      if [ -z "$ACTION" ]; then
        ACTION="$1"
      fi
      ;;
    "--help")
      do_help
      exit 0
      ;;
    "--type")
      FEED_TYPE=$(echo "$2" | tr '[:lower:]-' '[:upper:]_')
      shift
      ;;
  esac
  shift
done

init_feed_type

write_feed_xml

case "$ACTION" in
  --version)
    echo $VERSION
    exit 0
    ;;
  --identify)
    echo "$SCRIPT_ID|$SCRIPT_NAME|$VERSION|$FEED_NAME|$RESTRICTED|$SCRIPT_ID"
    exit 0
    ;;
  --describe)
    do_describe
    exit 0
    ;;
```

```
  --feedversion)
    do_feedversion
    exit 0
    ;;
  --selftest)
    SELFTEST_FAIL=0
    SELFTEST_STDERR=1
    do_self_test
    exit $SELFTEST_FAIL
    ;;
  --feedcurrent)
    is_feed_current
    exit $?
    ;;
esac

SELFTEST_FAIL=0
do_self_test
if [ $SELFTEST_FAIL -ne 0 ]
then
  exit 1
fi

is_feed_current
if [ $FEED_CURRENT -eq 1 ]
then
  log_notice "Feed is already current, skipping synchronization."
  exit 0
fi
(
  chmod +660 $LOCK_FILE
  flock -n 9
  if [ $? -eq 1 ]; then
    log_notice "Sync in progress, exiting."
```

```
    exit 1
  fi
  date > $LOCK_FILE
  sync_feed_data
  echo -n > $LOCK_FILE
) 9>>$LOCK_FILE

exit 0
```

Rendez le script exécutable :

```
[root@centos7 ~]# chmod +x greenbone-feed-sync
```

Déplacez le script vers **/usr/sbin/** :

```
[root@centos7 ~]# mv greenbone-feed-sync /usr/sbin/
```

Devenez l'utilisateur trainee et mettez à jour les modules d'extensions de OpenVAS :

```
[root@centos7 ~]# su - trainee
Last login: Fri Mar  5 07:35:08 UTC 2021 on pts/0
[trainee@centos7 ~]$ greenbone-feed-sync --type SCAP
...
[root@centos7 ~]# exit
```

Exécutez de nouveau la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
...
Step 2: Checking OpenVAS Manager ...
        OK: OpenVAS Manager is present in version 6.0.9.
        OK: OpenVAS Manager client certificate is present as /etc/pki/openvas/CA/clientcert.pem.
        OK: OpenVAS Manager database found in /var/lib/openvas/mgr/tasks.db.
        OK: Access rights for the OpenVAS Manager database are correct.
```

```
        OK: sqlite3 found, extended checks of the OpenVAS Manager installation enabled.
        OK: OpenVAS Manager database is at revision 146.
        OK: OpenVAS Manager expects database at revision 146.
        OK: Database schema is up to date.
        OK: OpenVAS Manager database contains information about 45654 NVTs.
        OK: At least one user exists.
        OK: OpenVAS SCAP database found in /var/lib/openvas/scap-data/scap.db.
        ERROR: No OpenVAS CERT database found. (Tried: /var/lib/openvas/cert-data/cert.db)
        FIX: Run a CERT synchronization script like openvas-certdata-sync or greenbone-certdata-sync.

 ERROR: Your OpenVAS-8 installation is not yet complete!
...
```

Important - Notez l'erreur **ERROR: No OpenVAS CERT database found. (Tried: /var/lib/openvas/cert-data/cert.db).**

Récupérer donc la base CERT :

```
[root@centos7 ~]# openvas-certdata-sync
```

Exécutez encore une fois la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
...
Step 7: Checking if OpenVAS services are up and running ...
        OK: netstat found, extended checks of the OpenVAS services enabled.
        OK: OpenVAS Scanner is running and listening on all interfaces.
        OK: OpenVAS Scanner is listening on port 9391, which is the default port.
        ERROR: OpenVAS Manager is NOT running!
        FIX: Start OpenVAS Manager (openvasmd).
        ERROR: Greenbone Security Assistant is NOT running!
```

```
        FIX: Start Greenbone Security Assistant (gsad).

 ERROR: Your OpenVAS-8 installation is not yet complete!
...
```

Important - Notez l'erreur **ERROR: Greenbone Security Assistant is NOT running!.**

Activer et démarrer OpenVAS Manager :

```
[root@centos7 ~]# systemctl enable openvas-manager
Created symlink from /etc/systemd/system/multi-user.target.wants/openvas-manager.service to
/usr/lib/systemd/system/openvas-manager.service.
[root@centos7 ~]# systemctl start openvas-manager
[root@centos7 ~]# systemctl status openvas-manager
● openvas-manager.service - OpenVAS Manager
   Loaded: loaded (/usr/lib/systemd/system/openvas-manager.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2018-06-21 11:49:32 CEST; 6s ago
  Process: 24857 ExecStart=/usr/sbin/openvasmd $MANAGER_LISTEN $MANAGER_PORT $SCANNER_LISTEN $SCANNER_PORT
$MANAGER_OTP (code=exited, status=0/SUCCESS)
 Main PID: 24862 (openvasmd)
   CGroup: /system.slice/openvas-manager.service
           └─24862 openvasmd

Jun 21 11:49:31 centos7.fenestros.loc systemd[1]: Starting OpenVAS Manager...
Jun 21 11:49:32 centos7.fenestros.loc systemd[1]: Started OpenVAS Manager.
```

Activer et démarrer le Greenbone Security Assistant :

```
[root@centos7 ~]# systemctl enable openvas-gsa
Created symlink from /etc/systemd/system/multi-user.target.wants/openvas-gsa.service to
```

```
/usr/lib/systemd/system/openvas-gsa.service.
[root@centos7 ~]# systemctl start openvas-gsa
[root@centos7 ~]# systemctl status openvas-gsa
● openvas-gsa.service - OpenVAS Greenbone Security Assistant
   Loaded: loaded (/usr/lib/systemd/system/openvas-gsa.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2018-06-21 11:50:52 CEST; 8s ago
  Process: 25464 ExecStart=/usr/sbin/gsad $GSA_LISTEN $GSA_PORT $MANAGER_LISTEN $MANAGER_PORT $GNUTLSSTRING
(code=exited, status=0/SUCCESS)
 Main PID: 25465 (gsad)
   CGroup: /system.slice/openvas-gsa.service
           ├─25465 /usr/sbin/gsad --port=9443 --mlisten=127.0.0.1 --mport=939...
           └─25466 /usr/sbin/gsad --port=9443 --mlisten=127.0.0.1 --mport=939...

Jun 21 11:50:51 centos7.fenestros.loc systemd[1]: Starting OpenVAS Greenbone ...
Jun 21 11:50:52 centos7.fenestros.loc systemd[1]: Started OpenVAS Greenbone S...
Hint: Some lines were ellipsized, use -l to show in full.
```

Exécutez encore une fois la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
...
Step 7: Checking if OpenVAS services are up and running ...
        OK: netstat found, extended checks of the OpenVAS services enabled.
        OK: OpenVAS Scanner is running and listening on all interfaces.
        OK: OpenVAS Scanner is listening on port 9391, which is the default port.
        OK: OpenVAS Manager is running and listening on all interfaces.
        OK: OpenVAS Manager is listening on port 9390, which is the default port.
        WARNING: Greenbone Security Assistant is listening on port 9443, which is NOT the default port!
        SUGGEST: Ensure Greenbone Security Assistant is listening on one of the following ports: 80, 443, 9392.
Step 8: Checking nmap installation ...
        WARNING: Your version of nmap is not fully supported: 6.40
        SUGGEST: You should install nmap 5.51 if you plan to use the nmap NSE NVTs.
Step 10: Checking presence of optional tools ...
        WARNING: Could not find pdflatex binary, the PDF report format will not work.
```

```
        SUGGEST: Install pdflatex.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
        OK: rpm found, LSC credential package generation for RPM based targets is likely to work.
        WARNING: Could not find alien binary, LSC credential package generation for DEB based targets will not
work.
        SUGGEST: Install alien.
        WARNING: Could not find makensis binary, LSC credential package generation for Microsoft Windows targets
will not work.
        SUGGEST: Install nsis.
        OK: SELinux is disabled.

It seems like your OpenVAS-8 installation is OK.
...
```

Important - Notez les WARNINGS.

Installez les paquets suggérés :

```
[root@centos7 ~]# yum install texlive-latex-bin-bin alien mingw32-nsis
```

Exécutez de nouveau la commande **openvas-check-setup** :

```
[root@centos7 ~]# openvas-check-setup
...
Step 10: Checking presence of optional tools ...
        OK: pdflatex found.
        WARNING: PDF generation failed, most likely due to missing LaTeX packages. The PDF report format will not
work.
        SUGGEST: Install required LaTeX packages.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
        OK: rpm found, LSC credential package generation for RPM based targets is likely to work.
```

```
        OK: alien found, LSC credential package generation for DEB based targets is likely to work.
        OK: nsis found, LSC credential package generation for Microsoft Windows targets is likely to work.
        OK: SELinux is disabled.

It seems like your OpenVAS-8 installation is OK.
...
```

> **Important** - Notez la ligne **WARNING: PDF generation failed, most likely due to missing LaTeX packages. The PDF report format will not work.**

Pour pouvoir utiliser les rapports au format PDF, installez les paquets suivants :

```
[root@centos7 ~]# yum -y install texlive-collection-fontsrecommended texlive-collection-latexrecommended texlive-changepage texlive-titlesec
```

Téléchargez ensuite le fichier **comment.sty** vers le répertoire **/usr/share/texlive/texmf-local/tex/latex/comment** :

```
[root@centos7 ~]# mkdir -p /usr/share/texlive/texmf-local/tex/latex/comment
[root@centos7 ~]# cd /usr/share/texlive/texmf-local/tex/latex/comment
[root@centos7 comment]# wget http://mirrors.ctan.org/macros/latex/contrib/comment/comment.sty
--2018-06-21 12:49:45--  http://mirrors.ctan.org/macros/latex/contrib/comment/comment.sty
Resolving mirrors.ctan.org (mirrors.ctan.org)... 176.28.54.184, 2a01:488:67:1000:b01c:36b8:0:1
Connecting to mirrors.ctan.org (mirrors.ctan.org)|176.28.54.184|:80... connected.
HTTP request sent, awaiting response... 302 Moved Temporarily
Location: http://mirrors.standaloneinstaller.com/ctan/macros/latex/contrib/comment/comment.sty [following]
--2018-06-21 12:49:45--  http://mirrors.standaloneinstaller.com/ctan/macros/latex/contrib/comment/comment.sty
Resolving mirrors.standaloneinstaller.com (mirrors.standaloneinstaller.com)... 37.59.26.59
Connecting to mirrors.standaloneinstaller.com (mirrors.standaloneinstaller.com)|37.59.26.59|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10197 (10.0K) [text/plain]
```

```
Saving to: ‘comment.sty’

100%[======================================>] 10,197      --.-K/s   in 0.02s

2018-06-21 12:49:46 (592 KB/s) - ‘comment.sty’ saved [10197/10197]

[root@centos7 comment]# chmod 644 comment.sty
[root@centos7 comment]# texhash
texhash: Updating /usr/share/texlive/texmf/ls-R...
texhash: Updating /usr/share/texlive/texmf-config/ls-R...
texhash: Updating /usr/share/texlive/texmf-dist/ls-R...
texhash: Updating /usr/share/texlive/texmf-local///ls-R...
texhash: Updating /usr/share/texlive/texmf-var/ls-R...
texhash: Done.
```

Exécutez une dernière fois la commande **openvas-check-setup** :

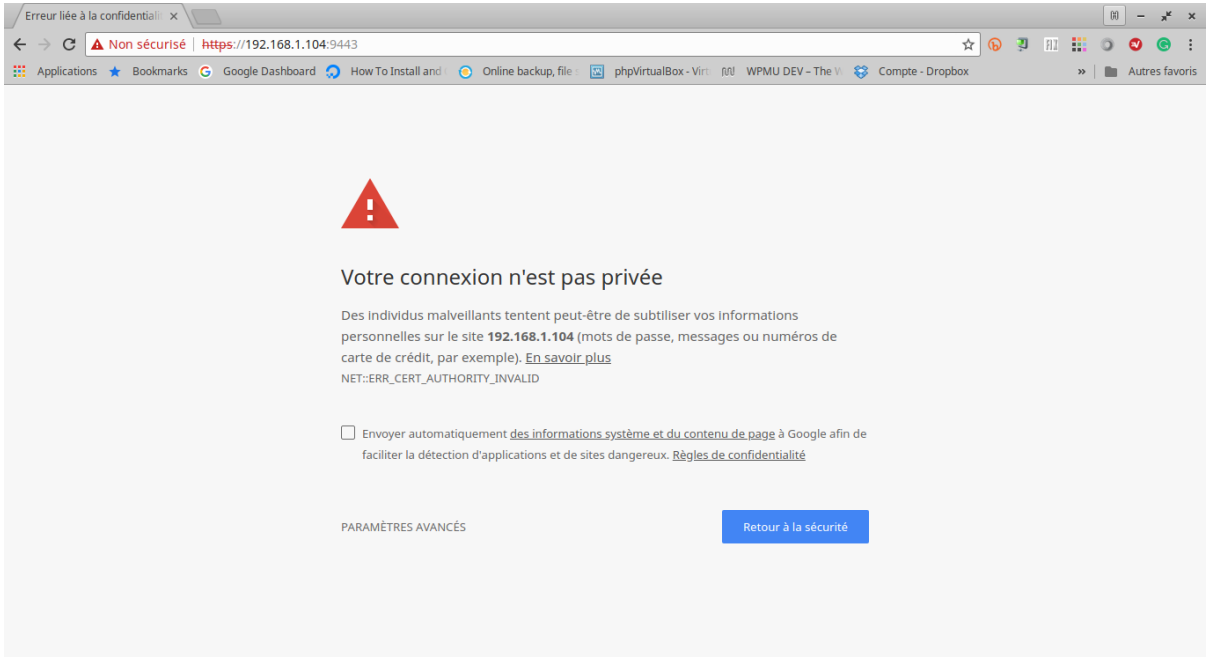
```
[root@centos7 ~]# openvas-check-setup
...
Step 10: Checking presence of optional tools ...
        OK: pdflatex found.
        OK: PDF generation successful. The PDF report format is likely to work.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
        OK: rpm found, LSC credential package generation for RPM based targets is likely to work.
        OK: alien found, LSC credential package generation for DEB based targets is likely to work.
        OK: nsis found, LSC credential package generation for Microsoft Windows targets is likely to work.
        OK: SELinux is disabled.

It seems like your OpenVAS-8 installation is OK.
...
```

Utilisation

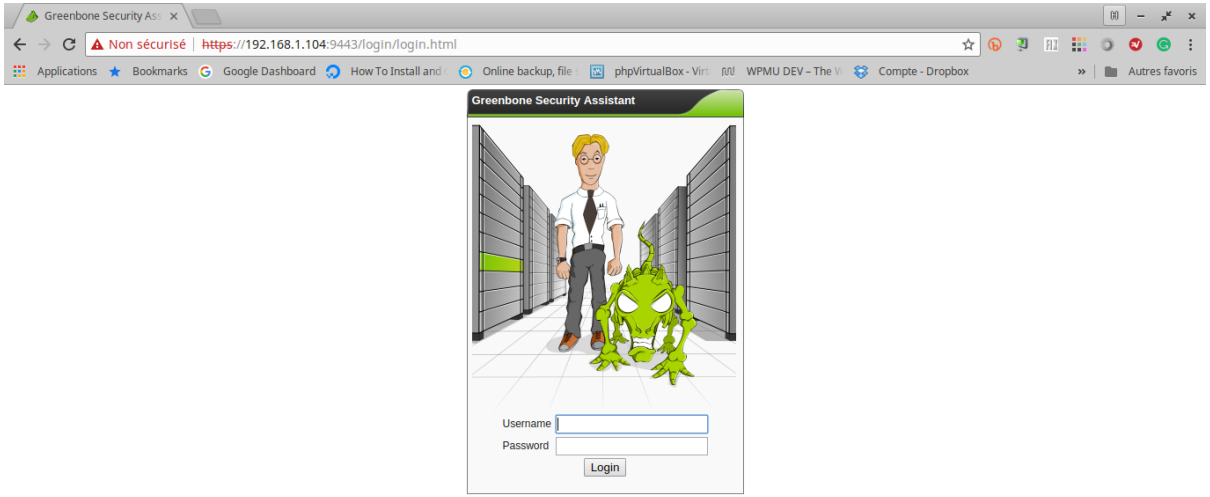
Passez votre VM en mode graphique :

```
[root@centos7 bin]# ls -l /etc/systemd/system/default.target
lrwxrwxrwx. 1 root root 37 Apr 30  2016 /etc/systemd/system/default.target -> /lib/systemd/system/multi-
user.target
[root@centos7 bin]# rm -rf /etc/systemd/system/default.target
[root@centos7 bin]# ln -s /lib/systemd/system/graphical.target /etc/systemd/system/default.target
[root@centos7 bin]# ls -l /etc/systemd/system/default.target
lrwxrwxrwx 1 root root 36 Apr 27 16:42 /etc/systemd/system/default.target -> /lib/systemd/system/graphical.target
[root@centos7 bin]# shutdown -r now
```

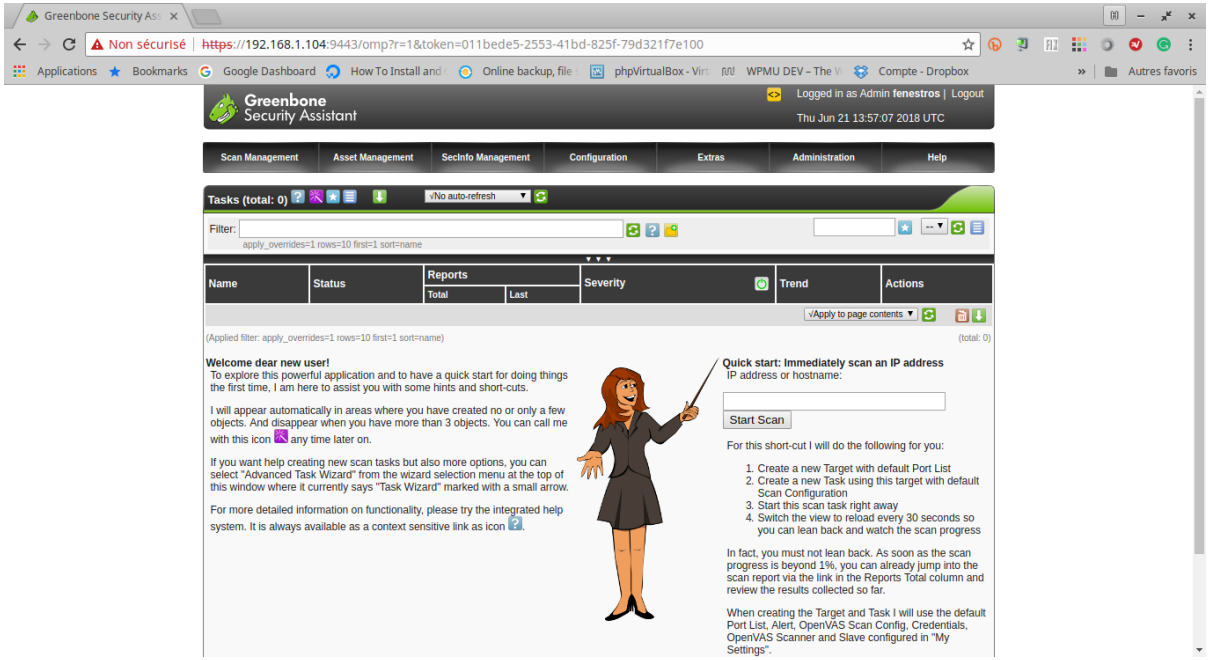
Ouvrez un navigateur web dans votre VM et saisissez l'adresse https:>//localhost:9443. Vous obtiendrez une fenêtre similaire à celle-ci :



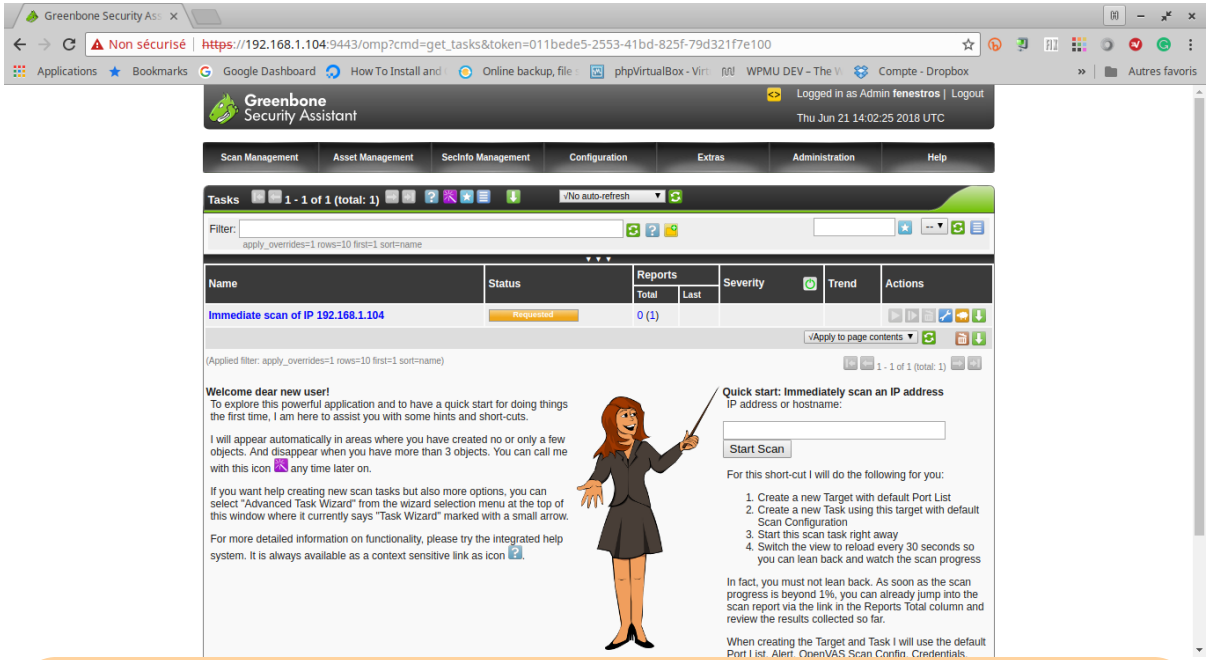
Créez une exception pour le Self Signed Certificate. Vous obtiendrez une fenêtre similaire à celle-ci:



Entrez le nom de votre utilisateur ainsi que son mot de passe et cliquez sur le bouton **Login**. Vous obtiendrez une fenêtre similaire à celle-ci :



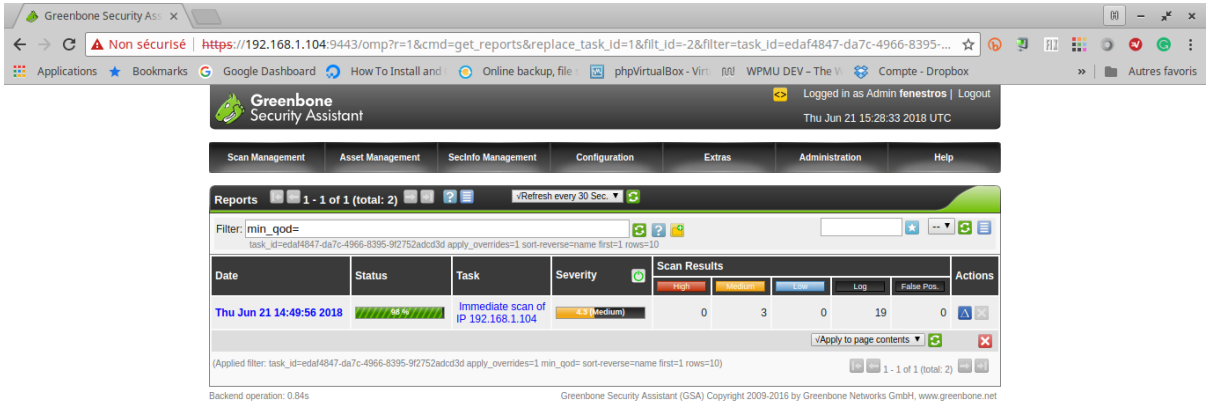
Dans la boîte **Quick start**, entrez l'adresse IP de votre VM et cliquez sur le bouton **Start Scan**. Vous obtiendrez une fenêtre similaire à celle-ci :



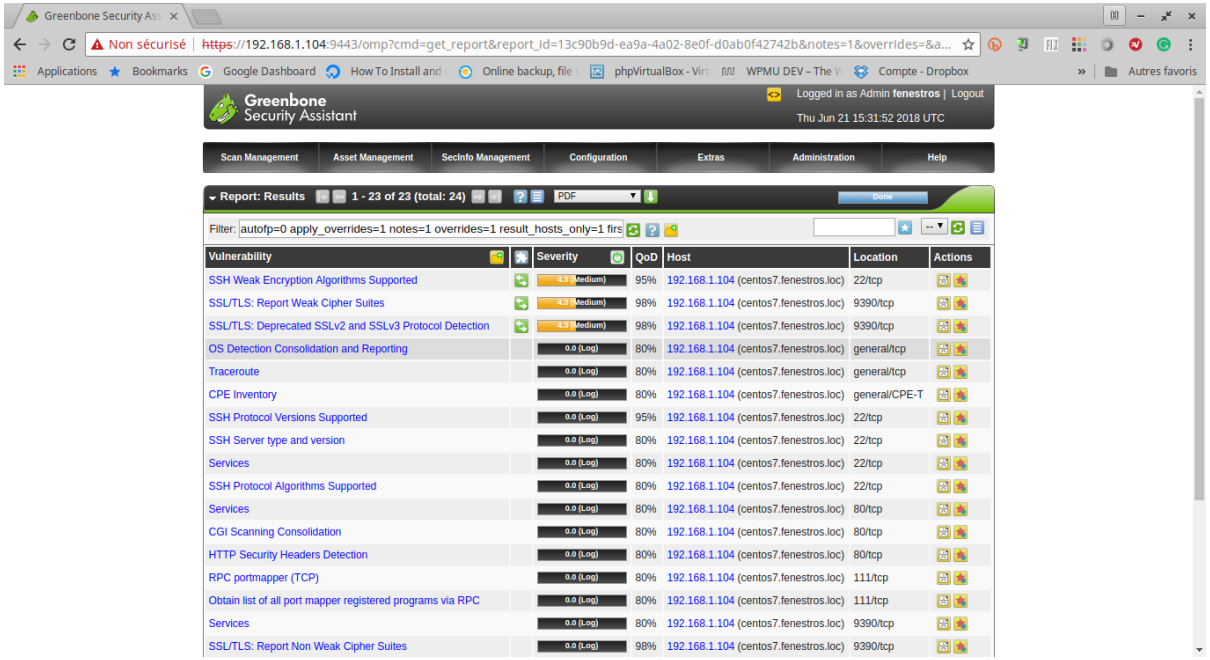
Important - Vous pouvez indiquer un réseau entier de la forme 10.0.2.0/24

Analyse des Résultats

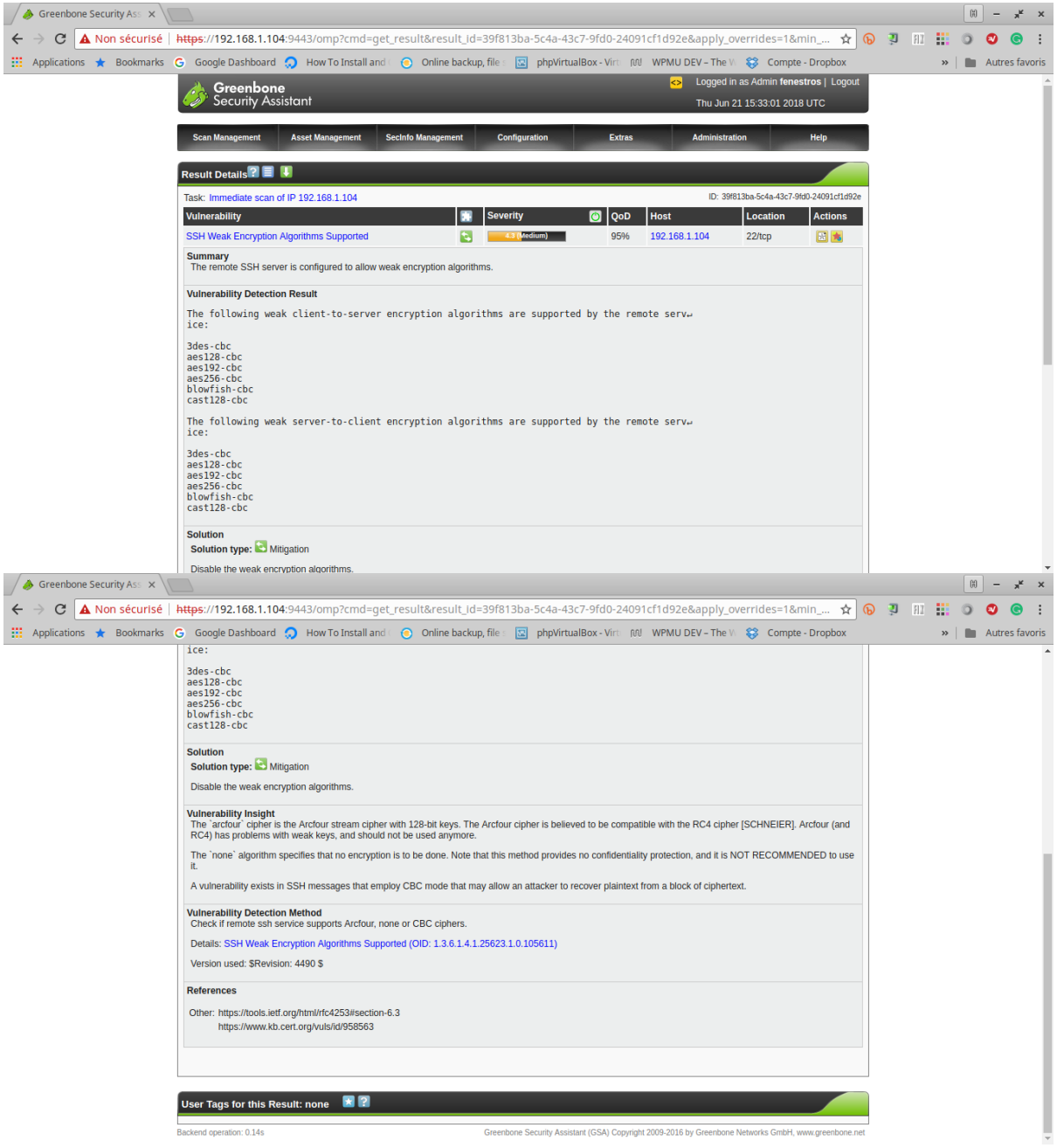
A l'issu de l'analyse, il est possible de consulter les résultats :



ainsi que les détails de celui-ci :



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


Greenbone Security Assistant
Logged in as Admin fenestros | Logout
Thu Jun 21 15:33:01 2018 UTC
Scan Management
Asset Management
SecInfo Management
Configuration
Extras
Administration
Help
Result Details
Task: Immediate scan of IP 192.168.1.104
ID: 39f813ba-5c4a-43c7-9fd0-24091cf1d92e
Vulnerability
Severity
QoD
Host
Location
Actions
SSH Weak Encryption Algorithms Supported
95%
192.168.1.104
22/tcp
Summary
The remote SSH server is configured to allow weak encryption algorithms.
Vulnerability Detection Result
The following weak client-to-server encryption algorithms are supported by the remote server:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
The following weak server-to-client encryption algorithms are supported by the remote server:
3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
Solution
Solution type: Mitigation
Disable the weak encryption algorithms.
Vulnerability Insight
The `arcfour` cipher is the Arcfour stream cipher with 128-bit keys. The Arcfour cipher is believed to be compatible with the RC4 cipher [SCHNEIER]. Arcfour (and RC4) has problems with weak keys, and should not be used anymore.
The `none` algorithm specifies that no encryption is to be done. Note that this method provides no confidentiality protection, and it is NOT RECOMMENDED to use it.
A vulnerability exists in SSH messages that employ CBC mode that may allow an attacker to recover plaintext from a block of ciphertext.
Vulnerability Detection Method
Check if remote ssh service supports Arcfour, none or CBC ciphers.
Details: SSH Weak Encryption Algorithms Supported (OID: 1.3.6.1.4.1.25623.1.0.105611)
Version used: $Revision: 4490 $
References
Other: https://tools.ietf.org/html/rfc4253#section-6.3
https://www.kb.cert.org/vuls/id/958563
User Tags for this Result: none
Backend operation: 0.14s
Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

Les Contres-Mesures

Les contre-mesures consistent en la mise en place de chroot pour certains serveurs ainsi que le durcissement de la configuration de serveurs d'application.

LAB #3 - La commande chroot

Le chrootage permet de séparer un utilisateur ou un utilisateur système (et donc un serveur) du système.

Sous RHEL/CentOS 7 le binaire chroot est installé par défaut :

```
[root@centos7 ~]# whereis chroot
chroot: /usr/sbin/chroot /usr/share/man/man1/chroot.1.gz /usr/share/man/man2/chroot.2.gz
```

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

```
[root@centos7 ~]# mkdir /home/prison
```

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

```
[root@centos7 ~]# ls -l /usr/sbin/chroot
-rwxr-xr-x. 1 root root 33240 Nov  5  2016 /usr/sbin/chroot
[root@centos7 ~]# chmod +s /usr/sbin/chroot
[root@centos7 ~]# ls -l /usr/sbin/chroot
-rwsr-sr-x. 1 root root 33240 Nov  5  2016 /usr/sbin/chroot
```

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

```
[root@centos7 ~]# vi /bin/chroot
[root@centos7 ~]# cat /bin/chroot
#!/bin/bash
```

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

Rendez ce script exécutable :

```
[root@centos7 ~]# 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@centos7 ~]# mkdir /home/prison/bin
[root@centos7 ~]# cp /bin/bash /home/prison/bin/
[root@centos7 ~]# ldd /bin/bash
    linux-vdso.so.1 =>  (0x00007fffe4199000)
    libtinfo.so.5 => /lib64/libtinfo.so.5 (0x00007f0e3804c000)
    libdl.so.2 => /lib64/libdl.so.2 (0x00007f0e37e48000)
    libc.so.6 => /lib64/linux-vdso.so.1(0x00007f0e37a84000)
    /lib64/ld-linux-x86-64.so.2 (0x0000559894c7a000)
[root@centos7 ~]# mkdir /home/prison/lib64
[root@centos7 ~]# cp /lib64/libtinfo.so.5 /home/prison/lib64
[root@centos7 ~]# cp /lib64/libdl.so.2 /home/prison/lib64
[root@centos7 ~]# cp /lib64/libc.so.6 /home/prison/lib64
[root@centos7 ~]# cp /lib64/ld-linux-x86-64.so.2 /home/prison/lib64
[root@centos7 ~]# cp /bin/ls /home/prison/bin/
[root@centos7 ~]# ldd /bin/ls
    linux-vdso.so.1 =>  (0x00007ffc7a1b1000)
    libselinux.so.1 => /lib64/libselinux.so.1 (0x00007fc4fc9e7000)
    libcap.so.2 => /lib64/libcap.so.2 (0x00007fc4fc7e2000)
    libacl.so.1 => /lib64/libacl.so.1 (0x00007fc4fc5d8000)
    libc.so.6 => /lib64/libc.so.6 (0x00007fc4fc215000)
    libpcre.so.1 => /lib64/libpcre.so.1 (0x00007fc4fbfb3000)
    libdl.so.2 => /lib64/libdl.so.2 (0x00007fc4fbdae000)
    /lib64/ld-linux-x86-64.so.2 (0x000055f5b5006000)
    libattr.so.1 => /lib64/libattr.so.1 (0x00007fc4fbba9000)
    libpthread.so.0 => /lib64/libpthread.so.0 (0x00007fc4fb98d000)
```

```
[root@centos7 ~]# cp /lib64/libselinux.so.1 /home/prison/lib64
[root@centos7 ~]# cp /lib64/libcap.so.2 /home/prison/lib64
[root@centos7 ~]# cp /lib64/libacl.so.1 /home/prison/lib64
[root@centos7 ~]# cp /lib64/libpcre.so.1 /home/prison/lib64
[root@centos7 ~]# cp /lib64/libattr.so.1 /home/prison/lib64
[root@centos7 ~]# cp /lib64/libpthread.so.0 /home/prison/lib64
```

Créez maintenant le groupe chroot :

```
[root@centos7 ~]# groupadd chroot
[root@centos7 ~]# cat /etc/group | grep chroot
chroot:x:1002:
```

Créez maintenant l'utilisateur **prison** :

```
[root@centos7 ~]# useradd prison -c chroot_user -d /home/prison -g chroot -s /bin/chroot
useradd: warning: the home directory already exists.
Not copying any file from skel directory into it.

[root@centos7 ~]# cp /etc/skel/.* /home/prison
cp: omitting directory ‘/etc/skel/.’
cp: omitting directory ‘/etc/skel/..’
cp: omitting directory ‘/etc/skel/.mozilla’

[root@centos7 ~]# cp -pfR /etc/skel/.m* /home/prison

[root@centos7 ~]# passwd prison
Changing password for user prison.
New password: prison
BAD PASSWORD: The password is shorter than 8 characters
Retype new password: prison
passwd: all authentication tokens updated successfully.
```

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

```
[root@centos7 ~]# chown -R prison:chroot /home/prison
```

Essayez maintenant de vous connecter en tant que prison :

```
[root@centos7 ~]# su - prison
Last login: Wed Jun 20 00:01:21 CEST 2018 on pts/2
bash-4.2$ pwd
/
bash-4.2$ /bin/ls
bin  lib64
bash-4.2$ /bin/ls -la
total 28
drwxr-xr-x. 5 1002 1002 4096 Jun 19 21:52 .
drwxr-xr-x. 5 1002 1002 4096 Jun 19 21:52 ..
-rw-------. 1 1002 1002   47 Jun 19 22:01 .bash_history
-rw-r--r--. 1 1002 1002   18 Jun 19 19:01 .bash_logout
-rw-r--r--. 1 1002 1002  193 Jun 19 19:01 .bash_profile
-rw-r--r--. 1 1002 1002  231 Jun 19 19:01 .bashrc
drwxr-xr-x. 4 1002 1002   37 Dec 10  2015 .mozilla
drwxr-xr-x. 2 1002 1002   26 Jun 19 17:46 bin
drwxr-xr-x. 2 1002 1002 4096 Jun 19 18:05 lib64
bash-4.2$ exit
exit
[root@centos7 ~]#
```

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

LAB #4 - Sécuriser Apache

Installation

Sous **RHEL / CentOS 7**, Apache n'est pas installé par défaut. Utilisez donc yum pour l'installer :

```
[root@centos7 ~]# rpm -qa | grep httpd
[root@centos7 ~]#
[root@centos7 ~]# yum install httpd
```

La version d'Apache est la **2.4.6** :

```
[root@centos7 ~]# rpm -qa | grep httpd
httpd-2.4.6-45.el7.centos.4.x86_64
httpd-tools-2.4.6-45.el7.centos.4.x86_64
```

Configurez le service pour démarrer automatiquement :

```
[root@centos7 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:httpd(8)
           man:apachectl(8)
[root@centos7 ~]# systemctl enable httpd
Created symlink from /etc/systemd/system/multi-user.target.wants/httpd.service to
/usr/lib/systemd/system/httpd.service.
```

Lancez votre service apache :

```
[root@centos7 ~]# systemctl start httpd
[root@centos7 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2017-08-22 11:19:18 CEST; 3s ago
     Docs: man:httpd(8)
           man:apachectl(8)
 Main PID: 1293 (httpd)
   Status: "Processing requests..."
```

```
   CGroup: /system.slice/httpd.service
           ├─1293 /usr/sbin/httpd -DFOREGROUND
           ├─1296 /usr/sbin/httpd -DFOREGROUND
           ├─1297 /usr/sbin/httpd -DFOREGROUND
           ├─1298 /usr/sbin/httpd -DFOREGROUND
           ├─1299 /usr/sbin/httpd -DFOREGROUND
           └─1300 /usr/sbin/httpd -DFOREGROUND

Aug 22 11:19:18 centos7.fenestros.loc systemd[1]: Starting The Apache HTTP Server...
Aug 22 11:19:18 centos7.fenestros.loc systemd[1]: Started The Apache HTTP Server.
```

Testez le serveur apache

Avec un navigateur

Lancez maintenant le navigateur et saisissez l'adresse http://localhost dans la barre d'adresses. Vous devez obtenir une page web servie par votre apache.

Avec Telnet

Premièrement, ouvrez un console et en tant que root et installez telnet :

```
[root@centos7 ~]# yum install telnet
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: mirrors.atosworldline.com
 * extras: mirrors.atosworldline.com
 * updates: ftp.ciril.fr
Resolving Dependencies
--> Running transaction check
---> Package telnet.x86_64 1:0.17-60.el7 will be installed
```

```
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
=====================================
 Package                            Arch                              Version
Repository                        Size
================================================================================================================
=====================================
Installing:
 telnet                             x86_64                            1:0.17-60.el7
base                              63 k

Transaction Summary
================================================================================================================
=====================================
Install  1 Package

Total download size: 63 k
Installed size: 113 k
Is this ok [y/d/N]: y
```

Utilisez ensuite telnet pour vérifier le bon fonctionnement d'Apache :

```
[root@centos7 ~]# telnet localhost 80
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.
GET /
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.1//EN" "http://www.w3.org/TR/xhtml11/DTD/xhtml11.dtd"><html><head>
<meta http-equiv="content-type" content="text/html; charset=UTF-8">
        <title>Apache HTTP Server Test Page powered by CentOS</title>
        <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
```

```
    <!-- Bootstrap -->
    <link href="/noindex/css/bootstrap.min.css" rel="stylesheet">
    <link rel="stylesheet" href="noindex/css/open-sans.css" type="text/css" />

<style type="text/css"><!--

body {
  font-family: "Open Sans", Helvetica, sans-serif;
  font-weight: 100;
  color: #ccc;
  background: rgba(10, 24, 55, 1);
  font-size: 16px;
}

h2, h3, h4 {
  font-weight: 200;
}

h2 {
  font-size: 28px;
}

.jumbotron {
  margin-bottom: 0;
  color: #333;
  background: rgb(212,212,221); /* Old browsers */
  background: radial-gradient(ellipse at center top, rgba(255,255,255,1) 0%,rgba(174,174,183,1) 100%); /* W3C */
}

.jumbotron h1 {
  font-size: 128px;
  font-weight: 700;
  color: white;
  text-shadow: 0px 2px 0px #abc,
```

```
               0px 4px 10px rgba(0,0,0,0.15),
               0px 5px 2px rgba(0,0,0,0.1),
               0px 6px 30px rgba(0,0,0,0.1);
}

.jumbotron p {
  font-size: 28px;
  font-weight: 100;
}

.main {
   background: white;
   color: #234;
   border-top: 1px solid rgba(0,0,0,0.12);
   padding-top: 30px;
   padding-bottom: 40px;
}

.footer {
   border-top: 1px solid rgba(255,255,255,0.2);
   padding-top: 30px;
}

    --></style>
</head>
<body>
  <div class="jumbotron text-center">
    <div class="container">
      <h1>Testing 123..</h1>
        <p class="lead">This page is used to test the proper operation of the <a href="http://apache.org">Apache
HTTP server</a> after it has been installed. If you can read this page it means that this site is working
properly. This server is powered by <a href="http://centos.org">CentOS</a>.</p>
        </div>
  </div>
```

```
  <div class="main">
    <div class="container">
       <div class="row">
            <div class="col-sm-6">
                <h2>Just visiting?</h2>
                      <p class="lead">The website you just visited is either experiencing problems or is
undergoing routine maintenance.</p>
                    <p>If you would like to let the administrators of this website know that you've seen this
page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster"
and directed to the website's domain should reach the appropriate person.</p>
                    <p>For example, if you experienced problems while visiting www.example.com, you should send
e-mail to "webmaster@example.com".</p>
                  </div>
                <div class="col-sm-6">
                      <h2>Are you the Administrator?</h2>
                      <p>You should add your website content to the directory <tt>/var/www/html/</tt>.</p>
                      <p>To prevent this page from ever being used, follow the instructions in the file
<tt>/etc/httpd/conf.d/welcome.conf</tt>.</p>

                      <h2>Promoting Apache and CentOS</h2>
                      <p>You are free to use the images below on Apache and CentOS Linux powered HTTP servers.
Thanks for using Apache and CentOS!</p>
                      <p><a href="http://httpd.apache.org/"><img src="images/apache_pb.gif" alt="[ Powered by
Apache ]"></a> <a href="http://www.centos.org/"><img src="images/poweredby.png" alt="[ Powered by CentOS Linux ]"
height="31" width="88"></a></p>
                </div>
              </div>
        </div>
        </div>
    </div>
      <div class="footer">
      <div class="container">
        <div class="row">
          <div class="col-sm-6">
```

```
            <h2>Important note:</h2>
            <p class="lead">The CentOS Project has nothing to do with this website or its content,
            it just provides the software that makes the website run.</p>
            <p>If you have issues with the content of this site, contact the owner of the domain, not the CentOS
project.
            Unless you intended to visit CentOS.org, the CentOS Project does not have anything to do with this
website,
            the content or the lack of it.</p>
            <p>For example, if this website is www.example.com, you would find the owner of the example.com
domain at the following WHOIS server:</p>
            <p><a href="http://www.internic.net/whois.html">http://www.internic.net/whois.html</a></p>
          </div>
          <div class="col-sm-6">
            <h2>The CentOS Project</h2>
            <p>The CentOS Linux distribution is a stable, predictable, manageable and reproduceable platform
derived from
               the sources of Red Hat Enterprise Linux (RHEL).<p>
            <p>Additionally to being a popular choice for web hosting, CentOS also provides a rich platform for
open source communities to build upon. For more information
               please visit the <a href="http://www.centos.org/">CentOS website</a>.</p>
          </div>
        </div>
          </div>
    </div>
  </div>
</body></html>
Connection closed by foreign host.
```

Préparation

Afin d'éviter les problèmes liés au pare-feu arrêtez le service firewalld :

```
[root@centos7 ~]# systemctl stop firewalld
```

```
[root@centos7 ~]# systemctl disable firewalld
[root@centos7 ~]# systemctl status firewalld
● firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; disabled; vendor preset: enabled)
   Active: inactive (dead)
     Docs: man:firewalld(1)

Aug 21 16:23:02 centos7.fenestros.loc systemd[1]: Starting firewalld - dynamic firewall daemon...
Aug 21 16:23:07 centos7.fenestros.loc systemd[1]: Started firewalld - dynamic firewall daemon.
Aug 21 16:29:49 centos7.fenestros.loc systemd[1]: Stopping firewalld - dynamic firewall daemon...
Aug 21 16:29:49 centos7.fenestros.loc systemd[1]: Stopped firewalld - dynamic firewall daemon.
```

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

```
10.0.2.15       www.homeland.net
```

Re-démarrez le serveur httpd :

```
[root@centos7 ~]# systemctl restart httpd
[root@centos7 ~]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2017-08-24 10:19:38 CEST; 9s ago
     Docs: man:httpd(8)
           man:apachectl(8)
  Process: 17996 ExecStop=/bin/kill -WINCH ${MAINPID} (code=exited, status=0/SUCCESS)
  Process: 21235 ExecReload=/usr/sbin/httpd $OPTIONS -k graceful (code=exited, status=0/SUCCESS)
 Main PID: 18013 (httpd)
   Status: "Total requests: 0; Current requests/sec: 0; Current traffic:   0 B/sec"
   CGroup: /system.slice/httpd.service
           ├─18013 /usr/sbin/httpd -DFOREGROUND
           ├─18014 /usr/sbin/httpd -DFOREGROUND
           ├─18015 /usr/sbin/httpd -DFOREGROUND
           ├─18016 /usr/sbin/httpd -DFOREGROUND
```

```
           ├─18017 /usr/sbin/httpd -DFOREGROUND
           ├─18018 /usr/sbin/httpd -DFOREGROUND
           ├─18019 /usr/sbin/httpd -DFOREGROUND
           ├─18020 /usr/sbin/httpd -DFOREGROUND
           └─18021 /usr/sbin/httpd -DFOREGROUND

Aug 24 10:19:38 centos7.fenestros.loc systemd[1]: Starting The Apache HTTP Server...
Aug 24 10:19:38 centos7.fenestros.loc systemd[1]: Started The Apache HTTP Server.
```

Gestion de serveurs virtuels

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@centos7 ~]# mkdir /etc/httpd/conf/vhosts.d/
```

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

```
[root@centos7 ~]# 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**:

```
...
# Supplemental configuration
#
# Load config files in the "/etc/httpd/conf.d" directory, if any.
IncludeOptional conf.d/*.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@centos7 ~]# mkdir -p /www/site1
```

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

```
[root@centos7 ~]# 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>
Require all granted
</Directory>
</VirtualHost>
```

Important : 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@centos7 ~]# systemctl restart httpd
```

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

```
[root@centos7 ~]# yum install lynx
Loaded plugins: fastestmirror, langpacks
adobe-linux-x86_64
| 2.9 kB  00:00:00
base
| 3.6 kB  00:00:00
extras
| 3.4 kB  00:00:00
updates
| 3.4 kB  00:00:00
Loading mirror speeds from cached hostfile
 * base: centos.mirrors.ovh.net
 * extras: ftp.rezopole.net
 * updates: centos.mirrors.ovh.net
Resolving Dependencies
--> Running transaction check
---> Package lynx.x86_64 0:2.8.8-0.3.dev15.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
=====================================
 Package                         Arch                              Version
Repository                       Size
================================================================================================================
=====================================
Installing:
 lynx                            x86_64                            2.8.8-0.3.dev15.el7
base                            1.4 M

Transaction Summary
```

```
================================================================================================================
=====================================
Install  1 Package

Total download size: 1.4 M
Installed size: 5.4 M
Is this ok [y/d/N]: y
```

Testez votre configuration avec **lynx** :

```
[root@centos7 ~]# lynx --dump http://www.vhostnom.com
                              Accueil du site 1


[root@centos7 ~]#
```

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>
Require all granted
</Directory>
</VirtualHost>
```

Créez ensuite le répertoire /www/logs/site1 :

```
[root@centos7 ~]# mkdir -p /www/logs/site1
```

Redémarrez le serveur Apache :

```
[root@centos7 ~]# systemctl restart httpd
```

Testez votre configuration avec **lynx** :

```
[root@centos7 ~]# lynx --dump http://www.vhostnom.com
                            Accueil du site 1


[root@centos7 ~]#
```

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

```
[root@centos7 ~]# ls -l /www/logs/site1/
total 4
-rw-r--r--. 1 root root   0 Aug 24 11:06 error.log
```

```
-rw-r--r--. 1 root root 138 Aug 24 11:06 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@centos7 ~]# cat /www/logs/site1/vhostnom.log
10.0.2.15 - - [24/Aug/2017:11:06:47 +0200] "GET / HTTP/1.0" 200 100 "-" "Lynx/2.8.8dev.15 libwww-FM/2.14 SSL-
MM/1.4.1 OpenSSL/1.0.1e-fips"
```

Hôte virtuel par adresse IP

Commencez par créer une adresse IP fixe :

```
[root@centos7 ~]# nmcli connection add con-name ip_fixe ifname enp0s3 type ethernet ip4 10.0.2.16/24 gw4 10.0.2.2
[root@centos7 ~]# nmcli connection up ip_fixe
[root@centos7 ~]# nmcli connection mod ip_fixe ipv4.dns 8.8.8.8
[root@centos7 ~]# systemctl restart NetworkManager
[root@centos7 ~]# nslookup www.free.fr
Server:     8.8.8.8
Address:    8.8.8.8#53

Non-authoritative answer:
Name:   www.free.fr
Address: 212.27.48.10
```

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 enp0s3. Saisissez donc la commande suivante dans une fenêtre de console en tant que root :

```
[root@centos7 ~]# ip a | grep 'inet '
```

```
    inet 127.0.0.1/8 scope host lo
    inet 10.0.2.16/24 brd 10.0.2.255 scope global enp0s3
[root@centos7 ~]# ip a add 192.168.1.99/24 dev enp0s3
[root@centos7 ~]# ip a | grep 'inet '
    inet 127.0.0.1/8 scope host lo
    inet 10.0.2.16/24 brd 10.0.2.255 scope global enp0s3
    inet 192.168.1.99/24 scope global enp0s3
```

Créez maintenant le répertoire pour notre site2 :

```
[root@centos7 ~]# mkdir /www/site2
```

Créez la page d'accueil :

```
[root@centos7 ~]# vi /www/site2/index.html
```

Editez la page d'accueil :

index.html

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

Créez ensuite le répertoire /www/logs/site2 :

```
[root@centos7 ~]# 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>
Require all granted
</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>
Require all granted
</Directory>
</VirtualHost>
```

Éditez ensuite le fichier **/etc/hosts** :

```
[root@centos7 ~]# vi /etc/hosts
[root@centos7 ~]# cat /etc/hosts
127.0.0.1       localhost.localdomain localhost
::1     localhost6.localdomain6 localhost6
10.0.2.16   centos7.fenestros.loc
10.0.2.16   www.homeland.net
10.0.2.16       www.vhostnom.com
192.168.1.99    www.vhostip.com
```

Redémarrez votre serveur Apache :

```
[root@centos7 ~]# systemctl restart httpd
```

Testez votre configuration avec **lynx** :

```
[root@centos7 ~]# lynx --dump http://www.vhostip.com
                            Accueil du site 2



[root@centos7 ~]#
```

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

```
[root@centos7 ~]# ls -l /www/logs/site2/
total 4
-rw-r--r--. 1 root root   0 Aug 24 14:28 error.log
-rw-r--r--. 1 root root 141 Aug 24 14:29 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 2.4, 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@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep auth_basic
LoadModule auth_basic_module modules/mod_auth_basic.so
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep authn_file
LoadModule authn_file_module modules/mod_authn_file.so
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.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@centos7 ~]# mkdir /www/site1/secret/
```

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

```
[root@centos6 ~]# 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@centos7 ~]# mkdir -p /www/passwords/site1
```

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

```
[root@centos7 ~]# 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@centos7 ~]# cat /www/passwords/site1/.htpasswd
webmaster:$apr1$jnlskgOH$a/SaUQCeDHobz.PM2pDun.
```

Créez maintenant une page html dans le répertoire secret :

```
[root@centos7 ~]# 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>
Require all granted
</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>
Require all granted
</Directory>
<Directory /www/site1/secret>
AllowOverride AuthConfig
</Directory>
</VirtualHost>
```

Sauvegardez votre fichier et puis redémarrez votre serveur Apache :

```
[root@centos7 ~]# systemctl restart httpd
```

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 serveur MariaDB ainsi que **apr-util-mysql** :

```
[root@centos7 ~]# yum install mariadb mariadb-server apr-util-mysql
```

Vérifiez que le module **mod_authn_dbd** est activé :

```
[root@centos7 ~]# cat /etc/httpd/conf.modules.d/00-base.conf | grep authn_dbd
LoadModule authn_dbd_module modules/mod_authn_dbd.so
```

Copiez le module **/usr/lib64/apr-util-1/apr_dbd_mysql.so** dans le répertoire **/usr/lib64/httpd/modules/** :

```
[root@centos7 ~]# updatedb
[root@centos7 ~]# locate apr_dbd_mysql.so
/usr/lib64/apr-util-1/apr_dbd_mysql.so
[root@centos7 ~]# cp /usr/lib64/apr-util-1/apr_dbd_mysql.so /usr/lib64/httpd/modules/
```

Configuration de MariaDB

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

```
[root@centos7 ~]# systemctl enable mariadb
[root@centos7 ~]# systemctl start mariadb
[root@centos7 ~]# systemctl status mariadb
● mariadb.service - MariaDB database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2017-11-05 08:04:45 CET; 1h 41min ago
 Main PID: 1293 (mysqld_safe)
   CGroup: /system.slice/mariadb.service
           ├─1293 /bin/sh /usr/bin/mysqld_safe --basedir=/usr
           └─1964 /usr/libexec/mysqld --basedir=/usr --datadir=/var/lib/mysql --plugin-
dir=/usr/lib64/mysql/plugin --log-error=/var...

Nov 05 08:04:24 centos7.fenestros.loc systemd[1]: Starting MariaDB database server...
```

```
Nov 05 08:04:31 centos7.fenestros.loc mariadb-prepare-db-dir[687]: Database MariaDB is probably initialized in
/var/lib/mysql a...one.
Nov 05 08:04:36 centos7.fenestros.loc mysqld_safe[1293]: 171105 08:04:36 mysqld_safe Logging to
'/var/log/mariadb/mariadb.log'.
Nov 05 08:04:37 centos7.fenestros.loc mysqld_safe[1293]: 171105 08:04:37 mysqld_safe Starting mysqld daemon with
databases fro...mysql
Nov 05 08:04:45 centos7.fenestros.loc systemd[1]: Started MariaDB database server.
Hint: Some lines were ellipsized, use -l to show in full.
```

Définissez le mot de passe fenestros pour root avec la commande suivante :

```
[root@centos7 ~]# mysqladmin -u root password fenestros
```

Connectez-vous à MariaDB :

```
[root@centos7 ~]# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 4
Server version: 5.5.56-MariaDB MariaDB Server

Copyright (c) 2000, 2017, Oracle, MariaDB Corporation Ab and others.

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

MariaDB [(none)]>
```

Puis saisissez les requêtes et commandes suivantes :

```
CREATE DATABASE auth;
```

```
USE auth;
```

```
CREATE TABLE users (
    user_name VARCHAR(50) NOT NULL,
    user_passwd VARCHAR(50) NOT NULL,
    PRIMARY KEY (user_name)
    );
```

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

Vous obtiendrez :

```
MariaDB [(none)]> CREATE DATABASE auth;
Query OK, 1 row affected (0.00 sec)

MariaDB [(none)]> USE auth;
Database changed
MariaDB [auth]> CREATE TABLE users (
    -> user_name VARCHAR(50) NOT NULL,
    -> user_passwd VARCHAR(50) NOT NULL,
    -> PRIMARY KEY (user_name)
    -> );
Query OK, 0 rows affected (0.42 sec)

MariaDB [auth]> GRANT SELECT
    -> ON auth.users
    -> TO apache@localhost
    -> IDENTIFIED BY 'PaSsW0Rd';
Query OK, 0 rows affected (0.32 sec)

MariaDB [auth]> exit
Bye
[root@centos7 ~]# mysql -u root -p -e "INSERT INTO users (user_name, user_passwd) VALUES (\"apache\",\"$(htpasswd
```

```
-nb apache password |cut -d ':' -f 2)\")" auth
Enter password:
[root@centos7 ~]# mysql -u root -p -e "SELECT * FROM auth.users;"
Enter password:
+-----------+-------------------------------------+
| user_name | user_passwd                         |
+-----------+-------------------------------------+
| apache    | $apr1$isUDg5bK$8oh0oMFUDfL41h84M9vYu1 |
+-----------+-------------------------------------+
[root@centos7 ~]#
```

Configuration d'Apache

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

```
[root@centos7 ~]# mkdir /www/site1/secret2
```

Créez maintenant une page **index.html** dans le répertoire **secret2** :

```
[root@centos7 ~]# vi /www/site1/secret2/index.html
[root@centos7 ~]# cat /www/site1/secret2/index.html
<html>
<body>
<center>Si vous voyez ce message, vous connaissez mon secret MariaDB !</center>
</body>
</html>
```

Ouvrez ensuite le fichier de configuration **/etc/httpd/conf/vhosts.d/Vhosts.conf** et modifiez-le ainsi :

```
[root@centos7 vhosts.d]# vi /etc/httpd/conf/vhosts.d/Vhosts.conf
[root@centos7 vhosts.d]# cat /etc/httpd/conf/vhosts.d/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>
Require all granted
</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
DBDriver mysql
DBDParams "dbname=auth user=apache pass=PaSsW0Rd"
DBDMin  4
DBDKeep 8
DBDMax  20
DBDExptime 300
<Directory /www/site1>
Require all granted
</Directory>
<Directory /www/site1/secret>
```

```
AllowOverride AuthConfig
</Directory>
<Directory /www/site1/secret2>
 AuthType Basic
 AuthName "MariaDB Secret"
 AuthBasicProvider dbd
 Require valid-user
 AuthDBDUserPWQuery "SELECT user_passwd FROM users WHERE user_name = %s"
</Directory>
</VirtualHost>
```

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

```
[root@centos7 ~]# systemctl restart httpd
```

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

Vous devrez découvert le secret MySQL !

mod_authnz_ldap

Vous devez maintenant utiliser **mod_authnz_ldap** pour protéger l'accès à votre site principal. Pour activer l'authentification en utilisant OpenLDAP sous apache 2.4, le module **mod_ldap** doit être installée :

```
[root@centos7 ~]# yum install mod_ldap
```

Pour installer le serveur OpenLDAP sous GNU/Linux ou Unix vous pouvez soit utiliser la version binaire fournie par les dépôts de paquets de votre distribution GNU/Linux ou Unix soit télécharger la dernière version à compiler du site d'OpenLDAP.

Dans notre cas, nous allons installer OpenLDAP à partir des dépôts. Commencez par installer OpenLDAP :

```
[root@centos7 ~]# yum install openldap-servers openldap-clients openldap
```

```
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.ate.info
 * extras: distrib-coffee.ipsl.jussieu.fr
 * updates: mirror.guru
Resolving Dependencies
--> Running transaction check
---> Package openldap.x86_64 0:2.4.40-13.el7 will be updated
---> Package openldap.x86_64 0:2.4.44-5.el7 will be an update
---> Package openldap-clients.x86_64 0:2.4.44-5.el7 will be installed
---> Package openldap-servers.x86_64 0:2.4.44-5.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================================================
=====================
 Package                                Arch                           Version                                Repository
Size
================================================================================================================
=====================
Installing:
 openldap-clients                       x86_64                         2.4.44-5.el7                           base
188 k
 openldap-servers                       x86_64                         2.4.44-5.el7                           base
2.2 M
Updating:
 openldap                               x86_64                         2.4.44-5.el7                           base
354 k

Transaction Summary
================================================================================================================
=====================
Install  2 Packages
```

```
Upgrade  1 Package

Total download size: 2.7 M
Is this ok [y/d/N]:  y
```

Sous CentOS le service OpenLDAP s'appelle **slapd** :

```
[root@centos7 ~]# systemctl status slapd.service
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
[root@centos7 ~]# systemctl enable slapd.service
Created symlink from /etc/systemd/system/multi-user.target.wants/slapd.service to
/usr/lib/systemd/system/slapd.service.
[root@centos7 ~]# systemctl start slapd.service
[root@centos7 ~]# systemctl status slapd.service
● slapd.service - OpenLDAP Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/slapd.service; enabled; vendor preset: disabled)
   Active: active (running) since Sun 2017-11-05 12:39:40 CET; 6s ago
     Docs: man:slapd
           man:slapd-config
           man:slapd-hdb
           man:slapd-mdb
           file:///usr/share/doc/openldap-servers/guide.html
  Process: 28650 ExecStart=/usr/sbin/slapd -u ldap -h ${SLAPD_URLS} $SLAPD_OPTIONS (code=exited,
status=0/SUCCESS)
  Process: 28632 ExecStartPre=/usr/libexec/openldap/check-config.sh (code=exited, status=0/SUCCESS)
 Main PID: 28653 (slapd)
   CGroup: /system.slice/slapd.service
```

```
           └─28653 /usr/sbin/slapd -u ldap -h ldapi:/// ldap:///

Nov 05 12:39:39 centos7.fenestros.loc systemd[1]: Starting OpenLDAP Server Daemon...
Nov 05 12:39:39 centos7.fenestros.loc runuser[28637]: pam_unix(runuser:session): session opened for user ldap by
(uid=0)
Nov 05 12:39:39 centos7.fenestros.loc slapcat[28643]: DIGEST-MD5 common mech free
Nov 05 12:39:40 centos7.fenestros.loc slapd[28650]: @(#) $OpenLDAP: slapd 2.4.44 (Aug  4 2017 14:23:27) $
mockbuild@c1bm.rdu2.centos.org:/builddir/build/BUILD/openldap-2.4.../slapd
Nov 05 12:39:40 centos7.fenestros.loc slapd[28653]: hdb_db_open: warning - no DB_CONFIG file found in directory
/var/lib/ldap: (2).
                                                    Expect poor performance for suffix "dc=my-domain,dc=com".
Nov 05 12:39:40 centos7.fenestros.loc slapd[28653]: slapd starting
Nov 05 12:39:40 centos7.fenestros.loc systemd[1]: Started OpenLDAP Server Daemon.
Hint: Some lines were ellipsized, use -l to show in full.
```

Créez le répertoire **/var/lib/ldap/ittraining** pour contenir un nouveau base de données :

```
[root@centos7 ~]# mkdir /var/lib/ldap/ittraining
```

Nettoyez les anciens fichiers de configuration et fichiers de données :

```
[root@centos7 ~]# rm -Rf /etc/openldap/slapd.d/*
[root@centos7 ~]# rm -f /var/lib/ldap/alock
[root@centos7 ~]# rm -f /var/lib/ldap/__db.00?
```

Créez le fichier **/etc/openldap/slapd.conf** :

```
[root@centos7 ~]# vi /etc/openldap/slapd.conf
[root@centos7 ~]# cat /etc/openldap/slapd.conf
include     /etc/openldap/schema/corba.schema
include     /etc/openldap/schema/core.schema
include     /etc/openldap/schema/cosine.schema
include     /etc/openldap/schema/duaconf.schema
include     /etc/openldap/schema/dyngroup.schema
```

```
include     /etc/openldap/schema/inetorgperson.schema
include     /etc/openldap/schema/java.schema
include     /etc/openldap/schema/misc.schema
include     /etc/openldap/schema/nis.schema
include     /etc/openldap/schema/openldap.schema
include     /etc/openldap/schema/ppolicy.schema
include     /etc/openldap/schema/collective.schema

allow bind_v2

pidfile     /var/run/openldap/slapd.pid
argsfile    /var/run/openldap/slapd.args

TLSCACertificatePath /etc/openldap/certs
TLSCertificateFile "\"OpenLDAP Server\""
TLSCertificateKeyFile /etc/openldap/certs/password

database config
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" manage
    by * none

database monitor
access to *
    by dn.exact="gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth" read
        by dn.exact="cn=Admin,o=fenestros" read
        by * none

#######################################################

database    bdb
suffix      "o=ittraining"
checkpoint      1024 15
rootdn      "cn=Admin,o=ittraining"
```

```
rootpw
directory   /var/lib/ldap/ittraining
lastmod         on
index           cn,sn,st        eq,pres,sub
```

Créez un mot de passe crypté pour l'admistrateur LDAP :

```
[root@centos7 ~]# slappasswd -s fenestros
{SSHA}B4p7daRzJZPbf7AjuuYzohaW9nS7hGXi
```

Editez ensuite la section **database** du fichier **/etc/openldap/slapd.conf** :

```
...
database        bdb
suffix          "o=ittraining"
checkpoint      1024 15
rootdn          "cn=Admin,o=ittraining"
rootpw          {SSHA}B4p7daRzJZPbf7AjuuYzohaW9nS7hGXi
directory       /var/lib/ldap/ittraining
lastmod         on
index           cn,sn,st                eq,pres,sub
```

Copiez le fichier /usr/share/openldap-servers/DB_CONFIG.example vers **/var/lib/ldap/ittraining/DB_CONFIG** :

```
[root@centos6 ~]# cp /usr/share/openldap-servers/DB_CONFIG.example /var/lib/ldap/ittraining/DB_CONFIG
```

Initialisez la première base de données :

```
[root@centos7 ~]# echo “” | slapadd -f /etc/openldap/slapd.conf
59ff01da The first database does not allow slapadd; using the first available one (2)
59ff01da str2entry: entry -1 has no dn
slapadd: could not parse entry (line=1)
```

Initialisez ensuite l'arborescence dans **/etc/openldap/slapd.d** :

```
[root@centos7 ~]# slaptest -f /etc/openldap/slapd.conf -F /etc/openldap/slapd.d
config file testing succeeded
```

Vérifiez que l'arborescence initiale soit créée :

```
[root@centos7 ~]# ls -l /etc/openldap/slapd.d
total 8
drwxr-x--- 3 root root 4096 Nov  5 13:20 cn=config
-rw------- 1 root root 1258 Nov  5 13:20 cn=config.ldif
```

Modifiez le propriétaire, le groupe ainsi que le droits du répertoire **/etc/openldap/slapd.d** :

```
[root@centos7 ~]# chown -R ldap:ldap /etc/openldap/slapd.d
[root@centos7 ~]# chmod -R u+rwX /etc/openldap/slapd.d
```

Modifiez le propriétaire et le groupe répertoire **/var/lib/ldap/ittraining** ainsi que le fichier **/etc/openldap/slapd.conf** :

```
[root@centos7 ~]# chown -R ldap:ldap /var/lib/ldap/ittraining /etc/openldap/slapd.conf
```

Démarrez ensuite le service slapd :

```
[root@centos7 ~]# systemctl restart slapd
```

Créez le fichier **ittraining.ldif** :

```
[root@centos7 ~]# vi ittraining.ldif
[root@centos7 ~]# cat ittraining.ldif
dn: o=ittraining
objectClass: top
objectClass: organization
o: ittraining
```

```
description: LDAP Authentification

dn: cn=Admin,o=ittraining
objectClass: organizationalRole
cn: Admin
description: Administrateur LDAP

dn: ou=GroupA,o=ittraining
ou: GroupA
objectClass: top
objectClass: organizationalUnit
description: Membres de GroupA

dn: ou=GroupB,o=ittraining
ou: GroupB
objectClass: top
objectClass: organizationalUnit
description: Membres de GroupB

dn: ou=group,o=ittraining
ou: group
objectclass: organizationalUnit
objectclass: domainRelatedObject
associatedDomain: ittraining

dn: cn=users,ou=group,o=ittraining
cn: users
objectClass: top
objectClass: posixGroup
gidNumber: 100
memberUid: jean
memberUid: jacques

dn: cn=Jean Legrand,ou=GroupA,o=ittraining
```

```
ou: GroupA
o: ittraining
cn: Jean Legrand
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
mail: jean.legrand@ittraining.loc
givenname: Jean
sn: Legrand
uid: jean
uidNumber: 1001
gidNumber: 100
gecos: Jean Legrand
loginShell: /bin/bash
homeDirectory: /home/jean
shadowLastChange: 14368
shadowMin: 0
shadowMax: 999999
shadowWarning: 7
userPassword: secret1
homePostalAddress: 99 avenue de Linux, 75000 Paris
postalAddress: 99 avenue de Linux.
l: Paris
st: 75
postalcode: 75000
telephoneNumber: 01.10.20.30.40
homePhone: 01.50.60.70.80
facsimileTelephoneNumber: 01.99.99.99.99
title: Ingénieur

dn: cn=Jacques Lebeau,ou=GroupA,o=ittraining
```

```
ou: GroupA
o: ittraining
cn: Jacques Lebeau
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
objectClass: posixAccount
objectClass: shadowAccount
objectClass: top
mail: jacques.lebeau@ittraining.loc
givenname: Jacques
sn: Lebeau
uid: jacques
uidNumber: 1002
gidNumber: 100
gecos: Jacques Lebeau
loginShell: /bin/bash
homeDirectory: /home/jacques
shadowLastChange: 14365
shadowMin: 0
shadowMax: 999999
shadowWarning: 7
userPassword: secret2
initials: JL
homePostalAddress: 99 route d'Unix, 75000 Paris
postalAddress: 99 route d'Unix.
l: Paris
st: 75
postalcode: 75000
pager: 01.04.04.04.04
homePhone: 01.05.05.05.05
telephoneNumber: 01.06.06.06.06
mobile: 06.01.02.03.04
title: Technicienne
```

```
facsimileTelephoneNumber: 01.04.09.09.09
manager: cn=Jean Legrand,ou=GroupA,o=ittraining
```

Injectez le fichier ittraining.ldif dans OpenLDAP :

```
[root@centos7 ~]# ldapadd -f ittraining.ldif -xv -D "cn=Admin,o=ittraining" -h 127.0.0.1 -w fenestros
ldap_initialize( ldap://127.0.0.1 )
add objectClass:
    top
    organization
add o:
    ittraining
add description:
    LDAP Authentification
adding new entry "o=ittraining"
modify complete

add objectClass:
    organizationalRole
add cn:
    Admin
add description:
    Administrateur LDAP
adding new entry "cn=Admin,o=ittraining"
modify complete

add ou:
    GroupA
add objectClass:
    top
    organizationalUnit
add description:
    Membres de GroupA
adding new entry "ou=GroupA,o=ittraining"
```

```
modify complete

add ou:
    GroupB
add objectClass:
    top
    organizationalUnit
add description:
    Membres de GroupB
adding new entry "ou=GroupB,o=ittraining"
modify complete

add ou:
    group
add objectclass:
    organizationalUnit
    domainRelatedObject
add associatedDomain:
    ittraining
adding new entry "ou=group,o=ittraining"
modify complete

add cn:
    users
add objectClass:
    top
    posixGroup
add gidNumber:
    100
add memberUid:
    jean
    jacques
adding new entry "cn=users,ou=group,o=ittraining"
modify complete
```

```
add ou:
    GroupA
add o:
    ittraining
add cn:
    Jean Legrand
add objectClass:
    person
    organizationalPerson
    inetOrgPerson
    posixAccount
    shadowAccount
    top
add mail:
    jean.legrand@ittraining.loc
add givenname:
    Jean
add sn:
    Legrand
add uid:
    jean
add uidNumber:
    1001
add gidNumber:
    100
add gecos:
    Jean Legrand
add loginShell:
    /bin/bash
add homeDirectory:
    /home/jean
add shadowLastChange:
    14368
add shadowMin:
```

```
    0
add shadowMax:
    999999
add shadowWarning:
    7
add userPassword:
    secret1
add homePostalAddress:
    99 avenue de Linux, 75000 Paris
add postalAddress:
    99 avenue de Linux.
add l:
    Paris
add st:
    75
add postalcode:
    75000
add telephoneNumber:
    01.10.20.30.40
add homePhone:
    01.50.60.70.80
add facsimileTelephoneNumber:
    01.99.99.99.99
add title:
    NOT ASCII (10 bytes)
adding new entry "cn=Jean Legrand,ou=GroupA,o=ittraining"
modify complete

add ou:
    GroupA
add o:
    ittraining
add cn:
    Jacques Lebeau
```

```
add objectClass:
    person
    organizationalPerson
    inetOrgPerson
    posixAccount
    shadowAccount
    top
add mail:
    jacques.lebeau@ittraining.loc
add givenname:
    Jacques
add sn:
    Lebeau
add uid:
    jacques
add uidNumber:
    1002
add gidNumber:
    100
add gecos:
    Jacques Lebeau
add loginShell:
    /bin/bash
add homeDirectory:
    /home/jacques
add shadowLastChange:
    14365
add shadowMin:
    0
add shadowMax:
    999999
add shadowWarning:
    7
add userPassword:
```

```
    secret2
add initials:
    JL
add homePostalAddress:
    99 route d'Unix, 75000 Paris
add postalAddress:
    99 route d'Unix.
add l:
    Paris
add st:
    75
add postalcode:
    75000
add pager:
    01.04.04.04.04
add homePhone:
    01.05.05.05.05
add telephoneNumber:
    01.06.06.06.06
add mobile:
    06.01.02.03.04
add title:
    Technicienne
add facsimileTelephoneNumber:
    01.04.09.09.09
add manager:
    cn=Jean Legrand,ou=GroupA,o=ittraining
adding new entry "cn=Jacques Lebeau,ou=GroupA,o=ittraining"
modify complete
```

Arrêtez le serveur Apache :

```
[root@centos7 ~]# systemctl stop httpd
```

Remplacez la section **<Directory “/var/www/html”>** du fichier **/etc/httpd/conf/httpd.conf** avec les lignes suivantes :

```
...
# <Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    # Options Indexes FollowSymLinks
    #
    # AllowOverride controls what directives may be placed in .htaccess files.
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    # AllowOverride None
    #
    # Controls who can get stuff from this server.
    #
    # Require all granted
# </Directory>

<Directory "/var/www/html">
   AuthType Basic
   AuthName "LDAP Authentifaction"
   AuthBasicProvider ldap
   AuthLDAPURL ldap://localhost:389/o=ittraining?uid?sub
```

```
   AuthLDAPBindDN "cn=Admin,o=ittraining"
   AuthLDAPBindPassword fenestros
   require ldap-user jean jacques
   AllowOverride None
   Options Indexes FollowSymLinks
</Directory>
...
```

AuthzLDAPAuthoritative

Re-démarrez le serveur apache :

```
[root@centos7 ~]# systemctl restart httpd
```

Connectez-vous à http://localhost en utilisant le compte de jean et le mot de passe secret1.

Editez de nouveau le fichier **/etc/httpd/conf/httpd.conf** en supprimant la section <Directory> de la configuration LDAP :

```
<Directory "/var/www/html">
    #
    # Possible values for the Options directive are "None", "All",
    # or any combination of:
    #   Indexes Includes FollowSymLinks SymLinksifOwnerMatch ExecCGI MultiViews
    #
    # Note that "MultiViews" must be named *explicitly* --- "Options All"
    # doesn't give it to you.
    #
    # The Options directive is both complicated and important.  Please see
    # http://httpd.apache.org/docs/2.4/mod/core.html#options
    # for more information.
    #
    Options Indexes FollowSymLinks
    #
    # AllowOverride controls what directives may be placed in .htaccess files.
```

```
    # It can be "All", "None", or any combination of the keywords:
    #   Options FileInfo AuthConfig Limit
    #
    AllowOverride None
    #
    # Controls who can get stuff from this server.
    #
    Require all granted
</Directory>

#
# DirectoryIndex: sets the file that Apache will serve if a directory
# is requested.
#
...
```

Re-démarrez le serveur apache :

```
[root@centos7 ~]# systemctl restart httpd
```

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**.

Installation de ssl

Afin de pouvoir configurer le serveur apache en mode ssl, il est necessaire d'installer les paquets **mod_ssl** et **openssl**. Le paquet **openssl** étant déjà installé, installez donc **mod_ssl** :

```
[root@centos7 ~]# yum install mod_ssl
Loaded plugins: fastestmirror, langpacks
adobe-linux-x86_64                                                                          |
2.9 kB  00:00:00
```

```
base                                                                                                                        |
3.6 kB  00:00:00
extras                                                                                                                      |
3.4 kB  00:00:00
updates                                                                                                                     |
3.4 kB  00:00:00
Loading mirror speeds from cached hostfile
 * base: centos.mirrors.ovh.net
 * extras: distrib-coffee.ipsl.jussieu.fr
 * updates: mirror.guru
Resolving Dependencies
--> Running transaction check
---> Package mod_ssl.x86_64 1:2.4.6-67.el7.centos.6 will be installed
--> Processing Dependency: libcrypto.so.10(OPENSSL_1.0.2)(64bit) for package:
1:mod_ssl-2.4.6-67.el7.centos.6.x86_64
--> Running transaction check
---> Package openssl-libs.x86_64 1:1.0.1e-60.el7_3.1 will be updated
--> Processing Dependency: openssl-libs(x86-64) = 1:1.0.1e-60.el7_3.1 for package:
1:openssl-1.0.1e-60.el7_3.1.x86_64
---> Package openssl-libs.x86_64 1:1.0.2k-8.el7 will be an update
--> Running transaction check
---> Package openssl.x86_64 1:1.0.1e-60.el7_3.1 will be updated
---> Package openssl.x86_64 1:1.0.2k-8.el7 will be an update
--> Finished Dependency Resolution

Dependencies Resolved

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

```
 mod_ssl                        x86_64                  1:2.4.6-67.el7.centos.6                  updates
109 k
Updating for dependencies:
 openssl                        x86_64                  1:1.0.2k-8.el7                           base
492 k
 openssl-libs                   x86_64                  1:1.0.2k-8.el7                           base
1.2 M

Transaction Summary
================================================================================================================
====================
Install  1 Package
Upgrade             ( 2 Dependent packages)

Total download size: 1.8 M
Is this ok [y/d/N]: y
```

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@centos7 ~]# 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@centos7 ~]# 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]:GB
State or Province Name (full name) []:SURREY
Locality Name (eg, city) [Default City]:ADDLESTONE
Organization Name (eg, company) [Default Company Ltd]:I2TCH LIMITED
Organizational Unit Name (eg, section) []:TRAINING
Common Name (eg, your name or your server's hostname) []:centos7.fenestros.loc
Email Address []:infos@i2tch.co.uk

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@centos7 ~]# openssl x509 -req -days 365 -in www.homeland.net.csr -signkey www.homeland.net.key -out
www.homeland.net.crt
Signature ok
subject=/C=GB/ST=SURREY/L=ADDLESTONE/O=I2TCH
LIMITED/OU=TRAINING/CN=centos7.fenestros.loc/emailAddress=infos@i2tch.co.uk
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@centos7 ~]# cp /root/www.homeland.net.key /etc/pki/tls/private/
[root@centos7 ~]# 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 :

```
[root@centos7 ~]# mkdir /www/ssl
```

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

```
[root@centos7 ~]# vi /www/ssl/index.html
[root@centos7 ~]# cat /www/ssl/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** :

```
[root@centos7 ~]# ls /etc/httpd/conf.d
autoindex.conf  README  ssl.conf  userdir.conf  welcome.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">
Require all granted
</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@centos7 ~]# systemctl restart httpd
```

A Faire - 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@centos7 ~]# openssl s_client -connect www.homeland.net:443
CONNECTED(00000003)
depth=0 C = GB, ST = SURREY, L = ADDLESTONE, O = I2TCH LIMITED, OU = TRAINING, CN = centos7.fenestros.loc,
emailAddress = infos@i2tch.co.uk
verify error:num=18:self signed certificate
verify return:1
depth=0 C = GB, ST = SURREY, L = ADDLESTONE, O = I2TCH LIMITED, OU = TRAINING, CN = centos7.fenestros.loc,
emailAddress = infos@i2tch.co.uk
verify return:1
---
Certificate chain
 0 s:/C=GB/ST=SURREY/L=ADDLESTONE/O=I2TCH
LIMITED/OU=TRAINING/CN=centos7.fenestros.loc/emailAddress=infos@i2tch.co.uk
   i:/C=GB/ST=SURREY/L=ADDLESTONE/O=I2TCH
LIMITED/OU=TRAINING/CN=centos7.fenestros.loc/emailAddress=infos@i2tch.co.uk
---
Server certificate
-----BEGIN CERTIFICATE-----
MIICuTCCAiICCQDauUN3s4rA2zANBgkqhkiG9w0BAQsFADCBoDELMAkGA1UEBhMC
R0IxDzANBgNVBAgMBlNVUlJFWTETMBEGA1UEBwwKQURETEVTVE9ORTEWMBQGA1UE
```

```
CgwNSTJUQ0ggTElNSVRFRDERMA8GA1UECwwIVFJBSU5JTkcxHjAcBgNVBAMMFWNl
bnRvczcuZmVuZXN0cm9zLmxvYzEgMB4GCSqGSIb3DQEJARYRaW5mb3NAaTJ0Y2gu
Y28udWswHhcNMTcxMTA1MTI1NDM4WhcNMTgxMTA1MTI1NDM4WjCBoDELMAkGA1UE
BhMCR0IxDzANBgNVBAgMBlNVUlJFWTETMBEGA1UEBwwKQURETEVTVE9ORTEWMBQG
A1UECgwNSTJUQ0ggTElNSVRFRDERMA8GA1UECwwIVFJBSU5JTkcxHjAcBgNVBAMM
FWNlbnRvczcuZmVuZXN0cm9zLmxvYzEgMB4GCSqGSIb3DQEJARYRaW5mb3NAaTJ0
Y2guY28udWswgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJAoGBALTR07YEuayyb23D
2TXd6Zh4ZZg1cHLKURQN1sjxkJTKwmscKFHExqtQKEmQV+CKAAMj51DL5M1j55dp
G9/72AEAniMVlXT6mOCihRcpEoiiESRz9i71EJtLAIT7c7/ptaxLdTMScDIAUqZN
PcX6yTdDDyb4MqBjaHfaHTxS/JgzAgMBAAEwDQYJKoZIhvcNAQELBQADgYEAaNKp
eBmvUNVmsYzK6N5WgVtdVgKARVlPRwrWAPp2KDTRBNNz7lkgyYt9zmjHFBYifcQW
iLFSb+cl6EtDrty+zWBztKA3CRVdNejI3Q9YQ56ztOAYrGlrRMtUINNxnZcHBe05
bTSecVYeyRu6aChGIyISwL5LjNyMKpXiSjSi5u0=
-----END CERTIFICATE-----
subject=/C=GB/ST=SURREY/L=ADDLESTONE/O=I2TCH
LIMITED/OU=TRAINING/CN=centos7.fenestros.loc/emailAddress=infos@i2tch.co.uk
issuer=/C=GB/ST=SURREY/L=ADDLESTONE/O=I2TCH
LIMITED/OU=TRAINING/CN=centos7.fenestros.loc/emailAddress=infos@i2tch.co.uk
---
No client certificate CA names sent
Peer signing digest: SHA512
Server Temp Key: ECDH, P-256, 256 bits
---
SSL handshake has read 1264 bytes and written 415 bytes
---
New, TLSv1/SSLv3, Cipher is ECDHE-RSA-AES256-GCM-SHA384
Server public key is 1024 bit
Secure Renegotiation IS supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
SSL-Session:
    Protocol  : TLSv1.2
    Cipher    : ECDHE-RSA-AES256-GCM-SHA384
```

```
    Session-ID: AF724406B1B2C2F3E8B33EEC51E51364F8E2B62374CCC16054217FBE866C4D09
    Session-ID-ctx:
    Master-Key: A6BF30C3757101E375F74A3075E1F68FCEF2C6450D18DD3AF12F42F65162B53FBCC4B27C80BE5C3F27A104BFC40CEF15
    Key-Arg   : None
    Krb5 Principal: None
    PSK identity: None
    PSK identity hint: None
    TLS session ticket lifetime hint: 300 (seconds)
    TLS session ticket:
    0000 - a8 28 11 9b 9f 2b 09 f9-ac 4c 20 5f 0c b7 ae 87   .(...+...L _....
    0010 - 7d 3b 12 4b b2 d1 f5 6f-ce 2e a8 74 9f 2d 59 a9   };.K...o...t.-Y.
    0020 - 6a d6 53 c9 54 f9 3e cc-0b c3 e6 92 58 8d 45 9c   j.S.T.>.....X.E.
    0030 - 41 ab a7 a4 b5 24 7c 2a-f2 4f 67 48 d5 35 68 29   A....$|*.OgH.5h)
    0040 - 3b 24 b6 2b 16 99 2d 6e-aa ea 4c c8 7e df 59 08   ;$.+..-n..L.~.Y.
    0050 - 42 06 1b 88 fa 5b c1 0b-4b 7c 01 d3 1a 28 6b 61   B....[..K|...(ka
    0060 - 70 c9 7b d0 74 93 f7 1e-c1 a6 58 54 b7 e6 4c 83   p.{.t.....XT..L.
    0070 - 5a d4 53 ff 61 71 46 f1-14 55 26 8f 83 29 11 69   Z.S.aqF..U&..).i
    0080 - e2 ee 08 dc 4e 7e 95 23-f7 54 c6 79 2e 88 7f 1d   ....N~.#.T.y....
    0090 - 5a a7 72 be 80 84 e3 4f-77 aa 63 28 06 a5 58 d1   Z.r....Ow.c(..X.
    00a0 - fa a8 28 9c 0d 22 ba 62-51 dc 33 d6 0c 56 57 c1   ..(.."bQ.3..VW.
    00b0 - b7 8c e3 eb da 54 82 d0-df e1 63 66 2b 10 85 cd   .....T....cf+...

    Start Time: 1509887084
    Timeout   : 300 (sec)
    Verify return code: 18 (self signed certificate)
---
^C
```

Procédez maintenant au test en utilisant le navigateur web de votre VM en saisissant l'adresse **https://www.homeland.net**.

> **Important** - Il est normal que la vérification échoue car dans ce cas il s'agit du certificat de test auto-signé.

Avec Apache 2.2.12 et OpenSSL v0.9.8j et versions ultérieurs, il est possible d'utiliser **TLS Extension Server Name Indication (SNI)** afin d'utiliser des certificats différents pour chaque hôte virtuel.

Par exemple :

```
NameVirtualHost *:443

<VirtualHost *:443>
 ServerName www.yoursite.com
 DocumentRoot /var/www/site
 SSLEngine on
 SSLCertificateFile /path/to/www_yoursite_com.crt
 SSLCertificateKeyFile /path/to/www_yoursite_com.key
 SSLCertificateChainFile /path/to/DigiCertCA.crt
</VirtualHost>

<VirtualHost *:443>
 ServerName www.yoursite2.com
 DocumentRoot /var/www/site2
 SSLEngine on
 SSLCertificateFile /path/to/www_yoursite2_com.crt
 SSLCertificateKeyFile /path/to/www_yoursite2_com.key
 SSLCertificateChainFile /path/to/DigiCertCA.crt
</VirtualHost>
```
