Version : **2026.01**

Dernière mise-à-jour : 2025/12/10 10:48

LDF406 - Sécurité Applicative

Contenu du Module

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.

1.1 - Installation

Netwox s'installe en utilisant APT :

```
root@debian12:~# cd /tmp

root@debian12:/tmp# cd ~

root@debian12:~# apt install netwox -y
```

1.2 - Utilisation

```
root@debian12:~# netwox
Netwox toolbox version 5.39.0. Netwib library version 5.39.0.

######################## 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** :

```
Select a node (key in 03456abcdefghijklmno): 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** :

```
Select a node (key in 0123456abcde): 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** :

```
Select a node (key in 0123456abcd): 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"
```

1.3 - 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 - Greenbone Vulnerability Management (GVM)

2.1 - Présentation

Greenbone Vulnerability Management (GVM), aussi connu sous le nom d'**OpenVAS**, est le successeur libre du scanner **Nessus**, devenu propriétaire. GVM, 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.

2.2 - 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
```

```
[root@centos7 ~]# reboot
```

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
```

2.3 - Installation

Téléchargez et installez **epel-release-7-14.noarch.rpm** :

```
[root@centos7 ~]# wget
https://archives.fedoraproject.org/pub/archive/epel/7/x86_64/Packages/e/epel-release-7-14.noarch.rpm
--2025-12-01 15:29:01--
https://archives.fedoraproject.org/pub/archive/epel/7/x86_64/Packages/e/epel-release-7-14.noarch.rpm
Resolving archives.fedoraproject.org (archives.fedoraproject.org)... 38.145.32.23, 38.145.32.22, 38.145.32.24
Connecting to archives.fedoraproject.org (archives.fedoraproject.org)|38.145.32.23|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 15608 (15K) [application/x-rpm]
Saving to: ‘epel-release-7-14.noarch.rpm’

100%[============================================================================================================
============================================================>] 15,608      --.-K/s   in 0.03s

2025-12-01 15:29:01 (532 KB/s) - ‘epel-release-7-14.noarch.rpm’ saved [15608/15608]

[root@centos7 ~]# yum localinstall epel-release-7-14.noarch.rpm --nogpgcheck
```

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

```
[root@centos7 ~]# yum install openvas-scanner openvas-manager openvas-gsa openvas-cli coreutils openssl
```

2.4 - 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 Mon 2025-12-01 15:45:16 CET; 3s ago
 Main PID: 13037 (redis-server)
   CGroup: /system.slice/redis.service
           └─13037 /usr/bin/redis-server 127.0.0.1:6379

Dec 01 15:45:16 centos7.fenestros.loc systemd[1]: Starting Redis persistent key-value database...
Dec 01 15:45:16 centos7.fenestros.loc systemd[1]: Started 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: Mon Dec  1 15:30:45 CET 2025 on pts/0

[trainee@centos7 ~]$ greenbone-nvt-sync
...
Greenbone community feed server - http://feed.community.greenbone.net/
This service is hosted by Greenbone Networks - http://www.greenbone.net/

All transactions are logged.

If you have any questions, please use the Greenbone community portal.
See https://community.greenbone.net for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be temporarily blocked.


receiving incremental file list
plugin_feed_info.inc
```

```
            330 100%  322.27kB/s    0:00:00 (xfr#1, to-chk=0/1)

sent 57 bytes  received 436 bytes  328.67 bytes/sec
total size is 330  speedup is 0.67
[trainee@centos7 ~]$ exit
[root@centos7 ~]#
```

Important - En cas d'erreur, relancez simplement la commande.

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 41280
drwxr-xr-x.   6 trainee trainee    24576 Dec  1 11:30 2008
drwxr-xr-x.  14 trainee trainee    65536 Dec  1 11:30 2009
drwxr-xr-x.  12 trainee trainee    65536 Dec  1 11:30 2010
drwxr-xr-x.  13 trainee trainee   118784 Dec  1 11:30 2011
drwxr-xr-x.  14 trainee trainee   102400 Dec  1 11:30 2012
drwxr-xr-x.  11 trainee trainee    86016 Dec  1 11:30 2013
drwxr-xr-x.  13 trainee trainee    81920 Dec  1 11:30 2014
drwxr-xr-x.  15 trainee trainee   118784 Dec  1 11:30 2015
drwxr-xr-x.  17 trainee trainee   159744 Dec  1 11:30 2016
drwxr-xr-x.  70 trainee trainee   126976 Dec  1 11:30 2017
drwxr-xr-x. 288 trainee trainee     8192 Dec  1 11:30 2018
drwxr-xr-x. 215 trainee trainee     8192 Dec  1 11:30 2019
drwxr-xr-x. 181 trainee trainee     8192 Dec  1 11:30 2020
drwxr-xr-x. 154 trainee trainee     8192 Dec  1 11:30 2021
```

```
drwxr-xr-x. 149 trainee trainee     4096 Dec  1 11:30 2022
drwx------. 136 trainee trainee     4096 Dec  1 11:30 2023
drwx------. 127 trainee trainee     4096 Dec  1 11:30 2024
drwx------. 132 trainee trainee     4096 Dec  1 11:30 2025
-rw-r--r--.   1 trainee trainee     2311 Dec  1 11:08 adaptbb_detect.nasl
-rw-r--r--.   1 trainee trainee     1786 Dec  1 11:08 afs_version.nasl
-rw-r--r--.   1 trainee trainee     2448 Dec  1 11:08 amanda_detect.nasl
-rw-r--r--.   1 trainee trainee     2432 Dec  1 11:08 amanda_version.nasl
-rw-r--r--.   1 trainee trainee     1492 Dec  1 11:08 aol_installed.nasl
-rw-r--r--.   1 trainee trainee     2746 Dec  1 11:08 apachehttp_config_defaults.nasl
-rw-r--r--.   1 trainee trainee     8186 Dec  1 11:08 apache_ofbiz_http_detect.nasl
-rw-r--r--.   1 trainee trainee     5553 Dec  1 11:08 apache_prds.inc
-rw-r--r--.   1 trainee trainee     4210 Dec  1 11:08 apache_server_info.nasl
-rw-r--r--.   1 trainee trainee     4624 Dec  1 11:08 apache_server_status.nasl
-rw-r--r--.   1 trainee trainee     6726 Dec  1 11:08 apache_SSL_complain.nasl
-rw-r--r--.   1 trainee trainee     2117 Dec  1 11:08 apache_tomcat_config.nasl
-rw-r--r--.   1 trainee trainee     2569 Dec  1 11:08 AproxEngine_detect.nasl
-rw-r--r--.   1 trainee trainee     2496 Dec  1 11:08 arcserve_backup_detect.nasl
-rw-r--r--.   1 trainee trainee     1937 Dec  1 11:08 arkoon.nasl
-rw-r--r--.   1 trainee trainee     6878 Dec  1 11:08 asip-status.nasl
-rw-r--r--.   1 trainee trainee     3797 Dec  1 11:08 atmail_detect.nasl
drwx------.   9 trainee trainee    20480 Dec  1 11:30 attic
-rw-r--r--.   1 trainee trainee     1914 Dec  1 11:08 auth_enabled.nasl
-rw-r--r--.   1 trainee trainee     2016 Dec  1 11:08 aventail_asap_http_detect.nasl
-rw-r--r--.   1 trainee trainee  1638960 Dec  1 11:08 bad_dsa_ssh_host_keys.txt
-rw-r--r--.   1 trainee trainee  1638960 Dec  1 11:08 bad_rsa_ssh_host_keys.txt
-rw-r--r--.   1 trainee trainee    54323 Dec  1 11:08 bad_ssh_host_keys.inc
-rw-r--r--.   1 trainee trainee    15064 Dec  1 11:08 bad_ssh_keys.inc
-rw-r--r--.   1 trainee trainee     2507 Dec  1 11:08 barracuda_im_firewall_detect.nasl
-rw-r--r--.   1 trainee trainee     2827 Dec  1 11:08 base_detect.nasl
-rw-r--r--.   1 trainee trainee     4464 Dec  1 11:08 basilix_detect.nasl
-rw-r--r--.   1 trainee trainee     3144 Dec  1 11:08 bgp_detect.nasl
-rw-r--r--.   1 trainee trainee    23162 Dec  1 11:08 bin.inc
-rw-r--r--.   1 trainee trainee     2745 Dec  1 11:08 bloofoxCMS_detect.nasl
```

```
-rw-r--r--.   1 trainee trainee     1531 Dec  1 11:08 bluecoat_mgnt_console.nasl
-rw-r--r--.   1 trainee trainee     2576 Dec  1 11:08 boastMachine_detect.nasl
-rw-r--r--.   1 trainee trainee     1359 Dec  1 11:08 brother_printers.inc
-rw-r--r--.   1 trainee trainee     3450 Dec  1 11:08 bugbear.nasl
-rw-r--r--.   1 trainee trainee     3639 Dec  1 11:08 bugzilla_detect.nasl
-rw-r--r--.   1 trainee trainee     5301 Dec  1 11:08 byte_func.inc
--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 Mon 2025-12-01 16:45:47 CET; 12s ago
  Process: 8889 ExecStart=/usr/sbin/openvassd $SCANNER_PORT $SCANNER_LISTEN $SCANNER_SRCIP (code=exited,
status=0/SUCCESS)
 Main PID: 8890 (openvassd)
   CGroup: /system.slice/openvas-scanner.service
           ├─8890 openvassd: Reloaded 1200 of 138097 NVTs (0% / ETA: 22:48)
           └─8891 openvassd (Loading Handler)

Dec 01 16:45:47 centos7.fenestros.loc systemd[1]: Starting OpenVAS Scanner...
Dec 01 16:45:47 centos7.fenestros.loc systemd[1]: Started OpenVAS Scanner.
```

Construisez maintenant la base de données :

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

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 'a5b5eaa9-3600-4604-bf20-bc10d7e5455b'.
```

```
[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).

Créez le fichier **greenbone-feed-sync** :

```
[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/
```

Créez le répertoire **/var/lib/openvas/scap-data/** :

```
[root@centos7 ~]# mkdir /var/lib/openvas/scap-data/

[root@centos7 ~]# chown trainee:trainee /var/lib/openvas/scap-data/
```

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

```
[root@centos7 ~]# su - trainee
Last login: Mon Dec  1 17:30:45 CET 2025 on pts/0

[trainee@centos7 ~]$ touch /var/lib/openvas/scap-data/scap.db

[trainee@centos7 ~]$ greenbone-feed-sync --type SCAP
Greenbone community feed server - http://feed.community.greenbone.net/
This service is hosted by Greenbone Networks - http://www.greenbone.net/
```

```
All transactions are logged.

If you have any questions, please use the Greenbone community portal.
See https://community.greenbone.net for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be temporarily blocked.


receiving incremental file list
timestamp
             13 100%   12.70kB/s    0:00:00 (xfr#1, to-chk=0/1)

sent 43 bytes  received 108 bytes  100.67 bytes/sec
total size is 13  speedup is 0.09
Greenbone community feed server - http://feed.community.greenbone.net/
This service is hosted by Greenbone Networks - http://www.greenbone.net/

All transactions are logged.

If you have any questions, please use the Greenbone community portal.
See https://community.greenbone.net for details.

By using this service you agree to our terms and conditions.

Only one sync per time, otherwise the source ip will be temporarily blocked.


receiving incremental file list
./
COPYING
          1,187 100%    1.13MB/s    0:00:00 (xfr#1, to-chk=26/28)
nvdcve-2.0-2002.xml
```

```
     19,533,351 100%   62.30MB/s    0:00:00 (xfr#2, to-chk=25/28)
nvdcve-2.0-2003.xml
      4,744,330 100%   13.55MB/s    0:00:00 (xfr#3, to-chk=24/28)
nvdcve-2.0-2004.xml
      9,416,639 100%   24.47MB/s    0:00:00 (xfr#4, to-chk=23/28)
nvdcve-2.0-2005.xml
     15,701,047 100%   23.22MB/s    0:00:00 (xfr#5, to-chk=22/28)
nvdcve-2.0-2006.xml
     26,320,892 100%   28.82MB/s    0:00:00 (xfr#6, to-chk=21/28)
nvdcve-2.0-2007.xml
     30,567,434 100%   22.08MB/s    0:00:01 (xfr#7, to-chk=20/28)
nvdcve-2.0-2008.xml
     29,775,037 100%   37.41MB/s    0:00:00 (xfr#8, to-chk=19/28)
nvdcve-2.0-2009.xml
     27,996,918 100%   17.06MB/s    0:00:01 (xfr#9, to-chk=18/28)
nvdcve-2.0-2010.xml
     42,684,286 100%   65.87MB/s    0:00:00 (xfr#10, to-chk=17/28)
nvdcve-2.0-2011.xml
     83,905,485 100%   51.13MB/s    0:00:01 (xfr#11, to-chk=16/28)
nvdcve-2.0-2012.xml
     66,859,075 100%  152.18MB/s    0:00:00 (xfr#12, to-chk=15/28)
nvdcve-2.0-2013.xml
     96,064,147 100%   48.94MB/s    0:00:01 (xfr#13, to-chk=14/28)
nvdcve-2.0-2014.xml
     98,694,839 100%   48.34MB/s    0:00:01 (xfr#14, to-chk=13/28)
nvdcve-2.0-2015.xml
    124,671,234 100%  227.33MB/s    0:00:00 (xfr#15, to-chk=12/28)
nvdcve-2.0-2016.xml
    161,692,009 100%  172.29MB/s    0:00:00 (xfr#16, to-chk=11/28)
nvdcve-2.0-2017.xml
    189,948,654 100%  141.52MB/s    0:00:01 (xfr#17, to-chk=10/28)
nvdcve-2.0-2018.xml
    210,761,959 100%  156.30MB/s    0:00:01 (xfr#18, to-chk=9/28)
nvdcve-2.0-2019.xml
```

```
    265,685,784 100%  172.95MB/s    0:00:01 (xfr#19, to-chk=8/28)
nvdcve-2.0-2020.xml
    294,835,369 100%  134.53MB/s    0:00:02 (xfr#20, to-chk=7/28)
nvdcve-2.0-2021.xml
    442,673,740 100%  155.72MB/s    0:00:02 (xfr#21, to-chk=6/28)
nvdcve-2.0-2022.xml
    743,192,055 100%  111.53MB/s    0:00:06 (xfr#22, to-chk=5/28)
nvdcve-2.0-2023.xml
    599,785,077 100%   67.83MB/s    0:00:08 (xfr#23, to-chk=4/28)
nvdcve-2.0-2024.xml
    922,757,332 100%   73.89MB/s    0:00:11 (xfr#24, to-chk=3/28)
nvdcve-2.0-2025.xml
    480,360,705 100%  127.96MB/s    0:00:03 (xfr#25, to-chk=2/28)
official-cpe-dictionary_v2.2.xml
    784,852,577 100%  251.59MB/s    0:00:02 (xfr#26, to-chk=1/28)
timestamp
             13 100%   12.70kB/s    0:00:00 (xfr#27, to-chk=0/28)

sent 2,186,887 bytes  received 11,127,079 bytes  117,303.67 bytes/sec
total size is 5,773,481,175  speedup is 433.64

[trainee@centos7 ~]$ greenbone-scapdata-sync

[trainee@centos7 ~]$ exit
```

Important - En cas d'erreur, relancez simplement la commande.

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).**

Créez le répertoire **/var/lib/openvas/cert-data/** :

```
[root@centos7 ~]# mkdir /var/lib/openvas/cert-data/
```

Créez le fichier **/var/lib/openvas/cert-data/cert.db** :

```
[root@centos7 ~]# touch /var/lib/openvas/cert-data/cert.db
```

Exécutez la commande **greenbone-certdata-sync** :

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

Exécutez encore une fois 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.
        OK: redis-server is present in version v=3.2.12.
        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.
        OK: NVT collection in /var/lib/openvas/plugins contains 138097 NVTs.
        WARNING: Signature checking of NVTs is not enabled in OpenVAS Scanner.
        SUGGEST: Enable signature checking (see http://www.openvas.org/trusted-nvts.html).
        OK: The NVT cache in /var/cache/openvas contains 138097 files for 138097 NVTs.
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 138097 NVTs.
        OK: At least one user exists.
        OK: OpenVAS SCAP database found in /var/lib/openvas/scap-data/scap.db.
        OK: OpenVAS CERT database found in /var/lib/openvas/cert-data/cert.db.
        OK: xsltproc found.
Step 3: Checking user configuration ...
        WARNING: Your password policy is empty.
        SUGGEST: Edit the /etc/openvas/pwpolicy.conf file to set a password policy.
Step 4: Checking Greenbone Security Assistant (GSA) ...
        OK: Greenbone Security Assistant is present in version 6.0.11.
Step 5: Checking OpenVAS CLI ...
        OK: OpenVAS CLI version 1.4.4.
Step 6: Checking Greenbone Security Desktop (GSD) ...
        SKIP: Skipping check for Greenbone Security Desktop.
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!

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: 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 Tue 2025-12-02 11:51:41 CET; 10s ago
  Process: 12237 ExecStart=/usr/sbin/openvasmd $MANAGER_LISTEN $MANAGER_PORT $SCANNER_LISTEN $SCANNER_PORT
$MANAGER_OTP (code=exited, status=0/SUCCESS)
 Main PID: 12238 (openvasmd)
   CGroup: /system.slice/openvas-manager.service
           └─12238 openvasmd

Dec 02 11:51:41 centos7.fenestros.loc systemd[1]: Starting OpenVAS Manager...
Dec 02 11:51:41 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 Tue 2025-12-02 11:53:08 CET; 1s ago
  Process: 12948 ExecStart=/usr/sbin/gsad $GSA_LISTEN $GSA_PORT $MANAGER_LISTEN $MANAGER_PORT $GNUTLSSTRING
(code=exited, status=0/SUCCESS)
 Main PID: 12949 (gsad)
   CGroup: /system.slice/openvas-gsa.service
           ├─12949 /usr/sbin/gsad --port=9443 --mlisten=127.0.0.1 --mport=9390 --gnutls-priorities=SECURE128:-
AES-128-CBC:-CAMELLIA-128-CBC:-VERS-SSL3.0:-VERS-TLS1.0
           └─12950 /usr/sbin/gsad --port=9443 --mlisten=127.0.0.1 --mport=9390 --gnutls-priorities=SECURE128:-
AES-128-CBC:-CAMELLIA-128-CBC:-VERS-SSL3.0:-VERS-TLS1.0

Dec 02 11:53:08 centos7.fenestros.loc systemd[1]: Starting OpenVAS Greenbone Security Assistant...
Dec 02 11:53:08 centos7.fenestros.loc systemd[1]: Started OpenVAS Greenbone Security Assistant.
```

Exécutez encore une fois 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.
        OK: redis-server is present in version v=3.2.12.
        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.
        OK: NVT collection in /var/lib/openvas/plugins contains 138097 NVTs.
        WARNING: Signature checking of NVTs is not enabled in OpenVAS Scanner.
        SUGGEST: Enable signature checking (see http://www.openvas.org/trusted-nvts.html).
        OK: The NVT cache in /var/cache/openvas contains 138097 files for 138097 NVTs.
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 138097 NVTs.
        OK: At least one user exists.
        OK: OpenVAS SCAP database found in /var/lib/openvas/scap-data/scap.db.
        OK: OpenVAS CERT database found in /var/lib/openvas/cert-data/cert.db.
        OK: xsltproc found.
Step 3: Checking user configuration ...
        WARNING: Your password policy is empty.
        SUGGEST: Edit the /etc/openvas/pwpolicy.conf file to set a password policy.
Step 4: Checking Greenbone Security Assistant (GSA) ...
        OK: Greenbone Security Assistant is present in version 6.0.11.
Step 5: Checking OpenVAS CLI ...
```

```
        OK: OpenVAS CLI version 1.4.4.
Step 6: Checking Greenbone Security Desktop (GSD) ...
        SKIP: Skipping check for Greenbone Security Desktop.
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.
        OK: Greenbone Security Assistant is listening on port 80, which is the default port.
Step 8: Checking nmap installation ...
        WARNING: No nmap installation found.
        SUGGEST: You should install nmap for comprehensive network scanning (see http://nmap.org)
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.

If you think it is not OK, 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 les WARNINGS.

Installez les paquets suggérés :

```
[root@centos7 ~]# yum install nmap texlive-latex-bin-bin alien -y
```

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.
        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 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 -y
```

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

```
[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
--2025-12-02 13:35:43--  http://mirrors.ctan.org/macros/latex/contrib/comment/comment.sty
Resolving mirrors.ctan.org (mirrors.ctan.org)... 89.58.7.101, 2a03:4000:5e:d33::1
Connecting to mirrors.ctan.org (mirrors.ctan.org)|89.58.7.101|:80... connected.
HTTP request sent, awaiting response... 307 Temporary Redirect
Location: https://mirror.its.dal.ca/ctan/macros/latex/contrib/comment/comment.sty [following]
--2025-12-02 13:35:43--  https://mirror.its.dal.ca/ctan/macros/latex/contrib/comment/comment.sty
Resolving mirror.its.dal.ca (mirror.its.dal.ca)... 192.75.96.254
Connecting to mirror.its.dal.ca (mirror.its.dal.ca)|192.75.96.254|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 10197 (10.0K) [application/octet-stream]
Saving to: ‘comment.sty’

100%[============================================================================================================
============================================================>] 10,197      --.-K/s   in 0s

2025-12-02 13:35:43 (175 MB/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 comment]# 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.
        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 la ligne **WARNING: Could not find makensis binary, LSC credential package generation for Microsoft Windows targets will not work.**

Téléchargez et installez le fichier **mingw32-nsis-3.01-1.el7.x86_64.rpm** :

```
[root@centos7 ~]# cd ~
```

```
[root@centos7 ~]# wget https://www.dropbox.com/scl/fi/76napuuwlohrzbhlxvduu/mingw32-nsis-3.01-1.el7.x86_64.rpm?rlkey=l0bibrdachsvy7gtui70kwgpd&st=uq4vst8m&dl=0

[root@centos7 ~]# mv mingw32-nsis-3.01-1.el7.x86_64.rpm?rlkey=l0bibrdachsvy7gtui70kwgpd&st=uq4vst8m&dl=0 mingw32-nsis-3.01-1.el7.x86_64.rpm

[root@centos7 ~]# yum localinstall mingw32-nsis-3.01-1.el7.x86_64.rpm --nogpgcheck -y
```

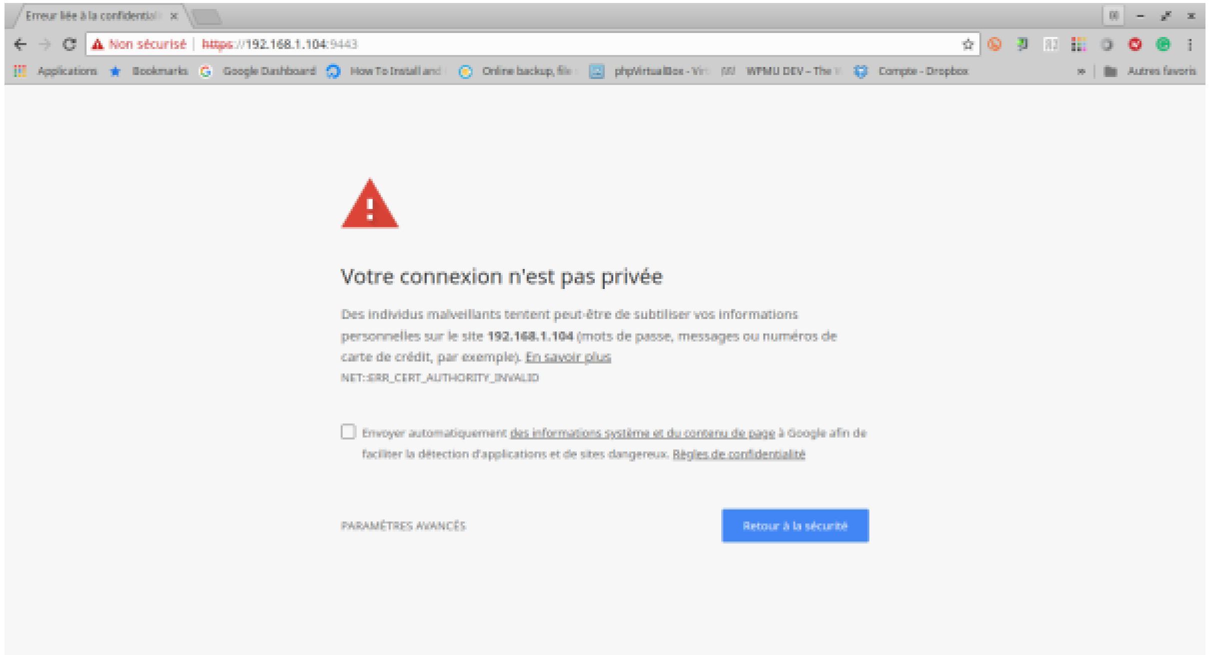
Exécutez une dernière fois la commande **openvas-check-setup** :

```
[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.
...
```

2.5 - Utilisation

Retournez à l'accueil de Guacamole. Connectez-vous à la VM **Gateway_10.0.2.40_VNC** avec le compte **trainee** et le mot de passe **a39dae707d**.

Ouvrez un navigateur web dans la VM et saisissez l'adresse https:>//10.0.2.51:9443. Vous obtiendrez une fenêtre similaire à celle-ci :



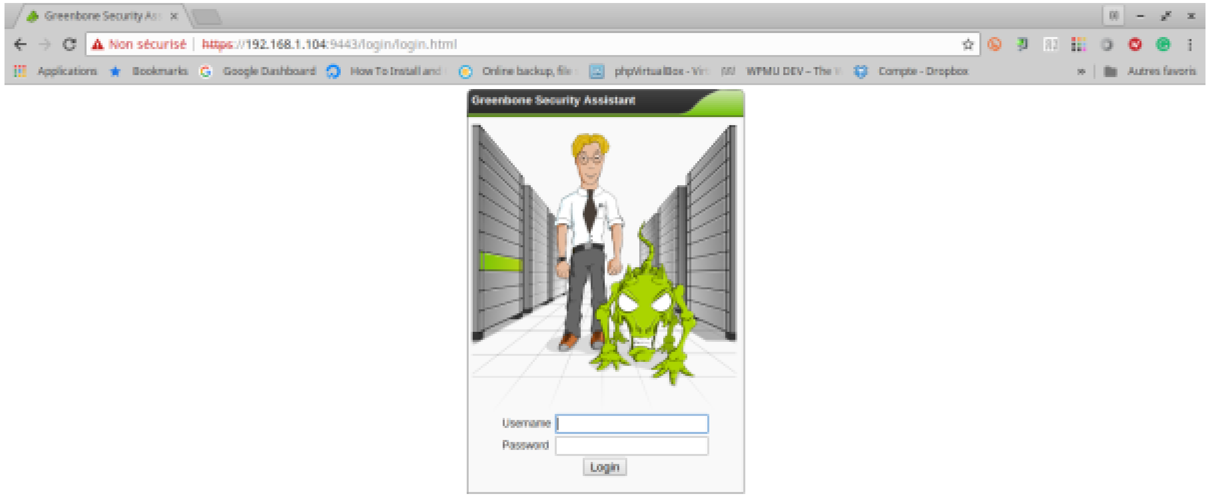
Votre connexion n'est pas privée

Des individus malveillants tentent peut-être de subtiliser vos informations personnelles sur le site **192.168.1.104** (mots de passe, messages ou numéros de carte de crédit, par exemple). En savoir plus

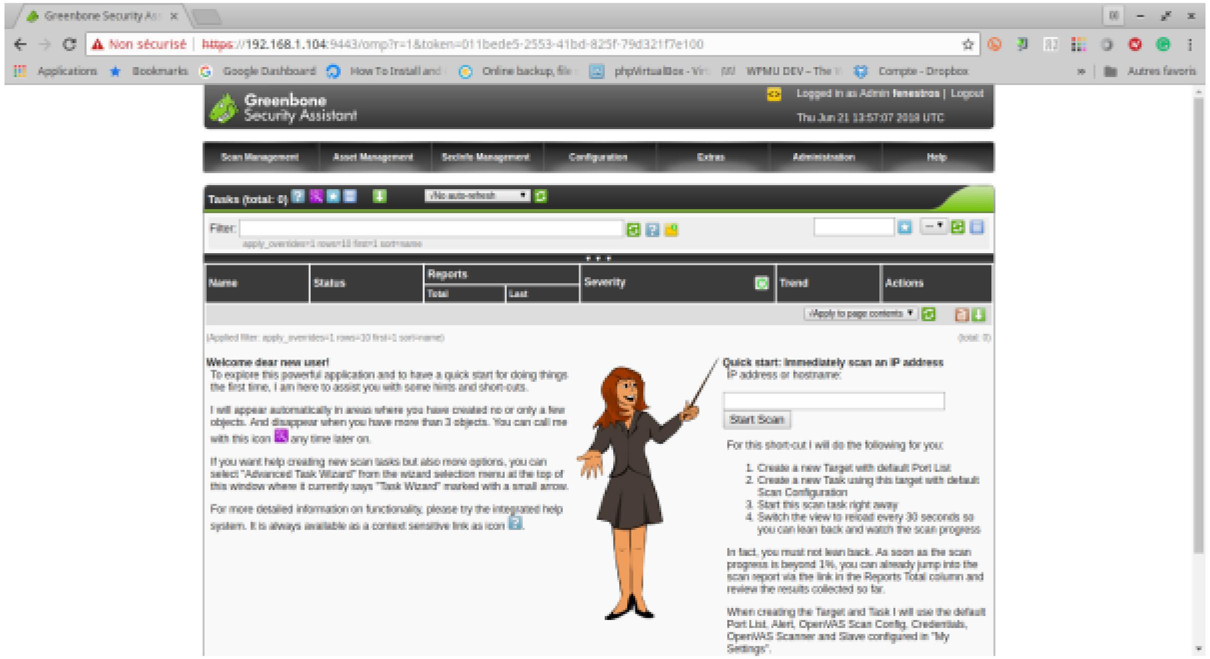
NET::ERR_CERT_AUTHORITY_INVALID

□ Envoyer automatiquement des informations système et du contenu de page à Google afin de faciliter la détection d'applications et de sites dangereux. Règles de confidentialité

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



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


Greenbone Security Assistant
Non sécurisé | https://192.168.1.104:9443/omp?r=1&token=011bede5-2553-41bd-825f-79d321f7e100
Logged in as Admin fenestros | Logout
Thu Jun 21 13:57:07 2018 UTC
Scan Management
Asset Management
SecInfo Management
Configuration
Extras
Administration
Help
Tasks (total: 0)
No auto-refresh
Filter:
apply_overrides=1 rows=10 first=1 sort=name
Name
Status
Reports
Total
Last
Severity
Trend
Actions
Apply to page contents
(Applied filter: apply_overrides=1 rows=10 first=1 sort=name)
(total: 0)

Welcome dear new user!

To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.

For more detailed information on functionality, please try the integrated help system. It is always available as a context sensitive link as icon ?.

Quick start: Immediately scan an IP address

IP address or hostname:

Start Scan

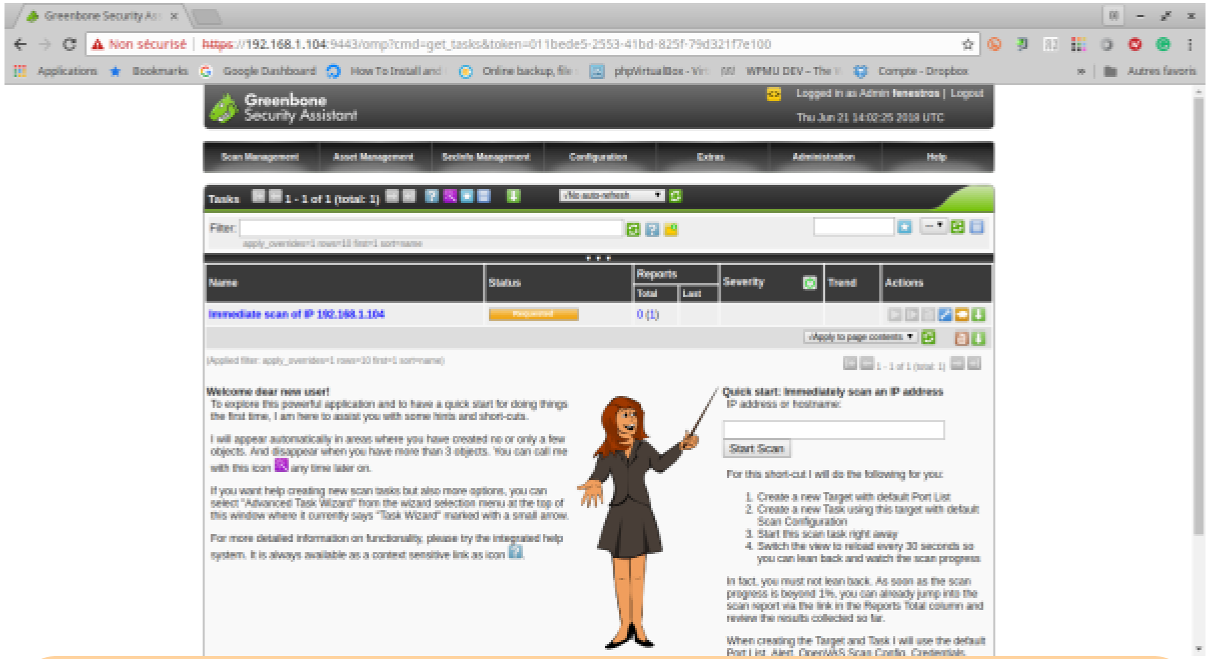
For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the default Port List, Alert, OpenVAS Scan Config, Credentials, OpenVAS Scanner and Slave configured in "My Settings".

Dans la boîte **Quick start**, entrez l'adresse IP 10.0.2.46 et cliquez sur le bouton **Start Scan**. Vous obtiendrez une fenêtre similaire à celle-ci :



Name	Status	Reports		Severity	Trend	Actions
		Total	Last			
Immediate scan of IP 192.168.1.104	Requested	0 (1)				

(Applied filter: apply_overrides=1 rows=10 first=1 sort=name)

Welcome dear new user!

To explore this powerful application and to have a quick start for doing things the first time, I am here to assist you with some hints and short-cuts.

I will appear automatically in areas where you have created no or only a few objects. And disappear when you have more than 3 objects. You can call me with this icon any time later on.

If you want help creating new scan tasks but also more options, you can select "Advanced Task Wizard" from the wizard selection menu at the top of this window where it currently says "Task Wizard" marked with a small arrow.

For more detailed information on functionality, please try the integrated help system. It is always available as a context sensitive link as icon ?.

Quick start: Immediately scan an IP address

IP address or hostname:

For this short-cut I will do the following for you:

1. Create a new Target with default Port List
2. Create a new Task using this target with default Scan Configuration
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress

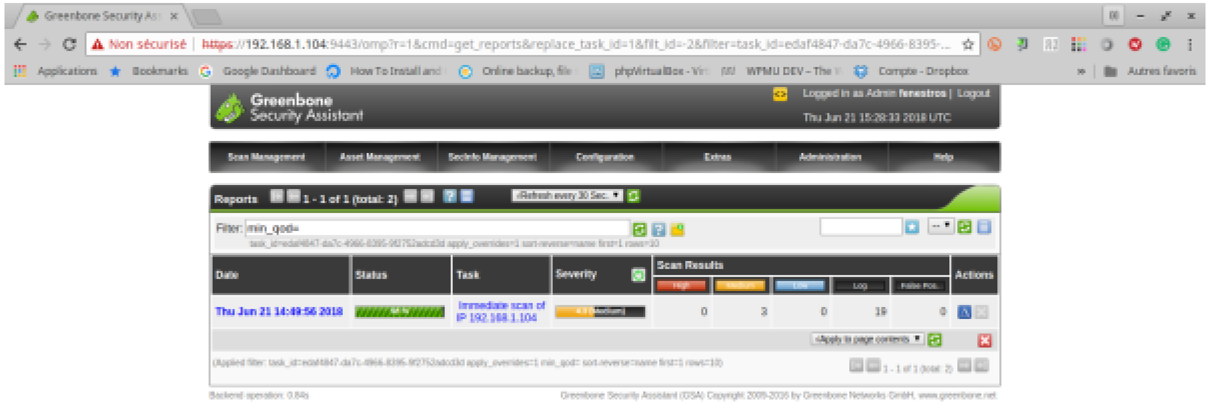
In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.

When creating the Target and Task I will use the default Port List, Alert, OpenVAS Scan Config, Credentials,

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 :



Non sécurisé | https://192.168.1.104:9443/omp?r=1&cmd=get_reports&replace_task_id=1&filt_id=-2&filter=task_id=edaf4847-da7c-4966-8395-...

Logged in as Admin fenestros | Logout

Thu Jun 21 15:28:33 2018 UTC

Reports 1 - 1 of 1 (total: 2)

Filter: min_qod=

task_id=edaf4847-da7c-4966-8395-9f2752adcd3d apply_overrides=1 sort-reverse=name first=1 rows=10

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Thu Jun 21 14:49:56 2018	Done	Immediate scan of IP 192.168.1.104	4.3 (Medium)	0	3	0	19	0	

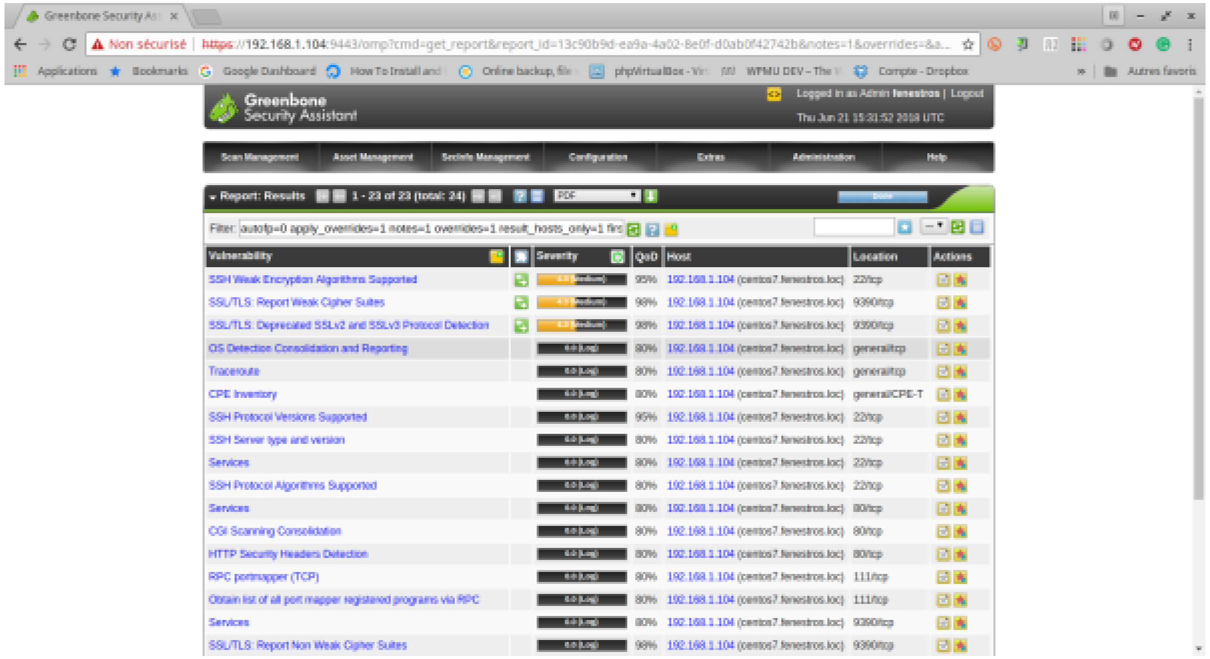
(Applied filter: task_id=edaf4847-da7c-4966-8395-9f2752adcd3d apply_overrides=1 min_qod= sort-reverse=name first=1 rows=10)

1 - 1 of 1 (total: 2)

Backend operation: 0.84s

Greenbone Security Assistant (GSA) Copyright 2009-2016 by Greenbone Networks GmbH, www.greenbone.net

ainsi que les détails de celui-ci :



Greenbone Security Assistant

Logged in as Admin fenestros | Logout

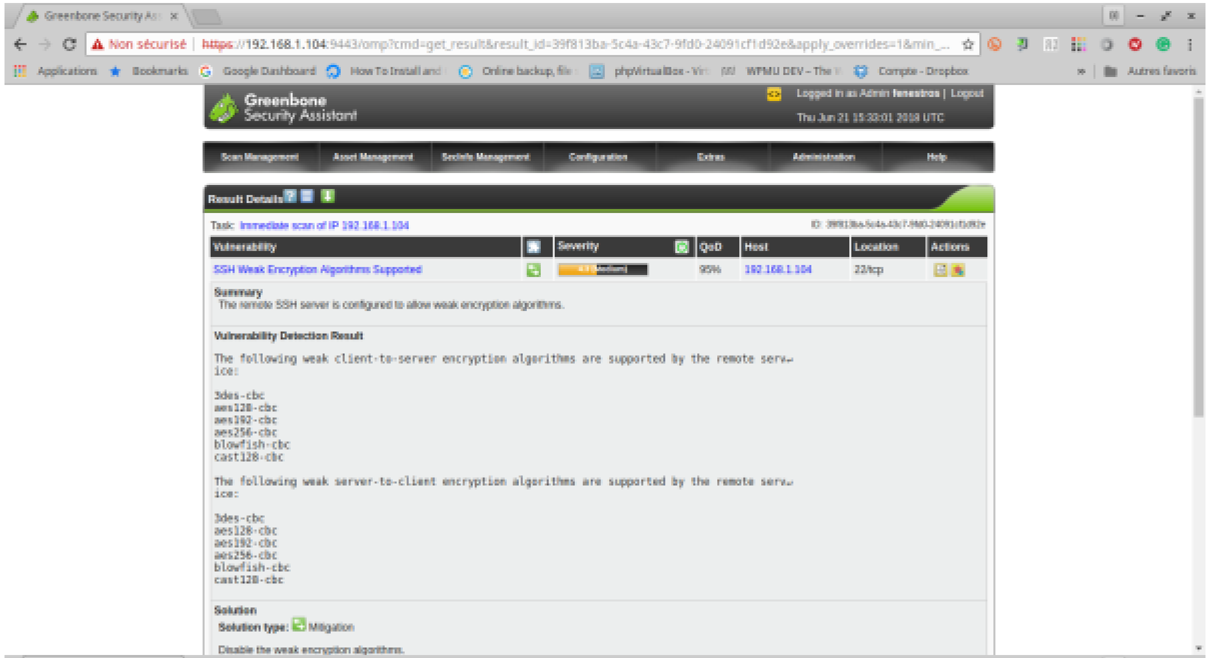
Thu Jun 21 15:31:52 2018 UTC

Report: Results 1 - 23 of 23 (total: 24)

Filter: autofp=0 apply_overrides=1 notes=1 overrides=1 result_hosts_only=1 firs

Vulnerability		Severity	QoD	Host	Location	Actions
SSH Weak Encryption Algorithms Supported		4.3 (Medium)	95%	192.168.1.104 (centos7.fenestros.loc)	22/tcp	
SSL/TLS: Report Weak Cipher Suites		4.3 (Medium)	98%	192.168.1.104 (centos7.fenestros.loc)	9390/tcp	
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection		4.3 (Medium)	98%	192.168.1.104 (centos7.fenestros.loc)	9390/tcp	
OS Detection Consolidation and Reporting		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	general/tcp	
Traceroute		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	general/tcp	
CPE Inventory		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	general/CPE-T	
SSH Protocol Versions Supported		0.0 (Log)	95%	192.168.1.104 (centos7.fenestros.loc)	22/tcp	
SSH Server type and version		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	22/tcp	
Services		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	22/tcp	
SSH Protocol Algorithms Supported		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	22/tcp	
Services		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	80/tcp	
CGI Scanning Consolidation		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	80/tcp	
HTTP Security Headers Detection		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	80/tcp	
RPC portmapper (TCP)		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	111/tcp	
Obtain list of all port mapper registered programs via RPC		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	111/tcp	
Services		0.0 (Log)	80%	192.168.1.104 (centos7.fenestros.loc)	9390/tcp	
SSL/TLS: Report Non Weak Cipher Suites		0.0 (Log)	98%	192.168.1.104 (centos7.fenestros.loc)	9390/tcp	

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



Greenbone Security As ×
Non sécurisé | https://192.168.1.104:9443/omp?cmd=get_result&result_id=39f813ba-5c4a-43c7-9fd0-24091cf1d92e&apply_overrides=1&min_...
Applications Bookmarks Google Dashboard How To Install and Online backup, file phpVirtualBox - Vir WPMU DEV - The Compte - Dropbox Autres favoris
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		4.3 (Medium)	95%	192.168.1.104	22/tcp	

Summary

The remote SSH server is configured to allow weak encryption algorithms.

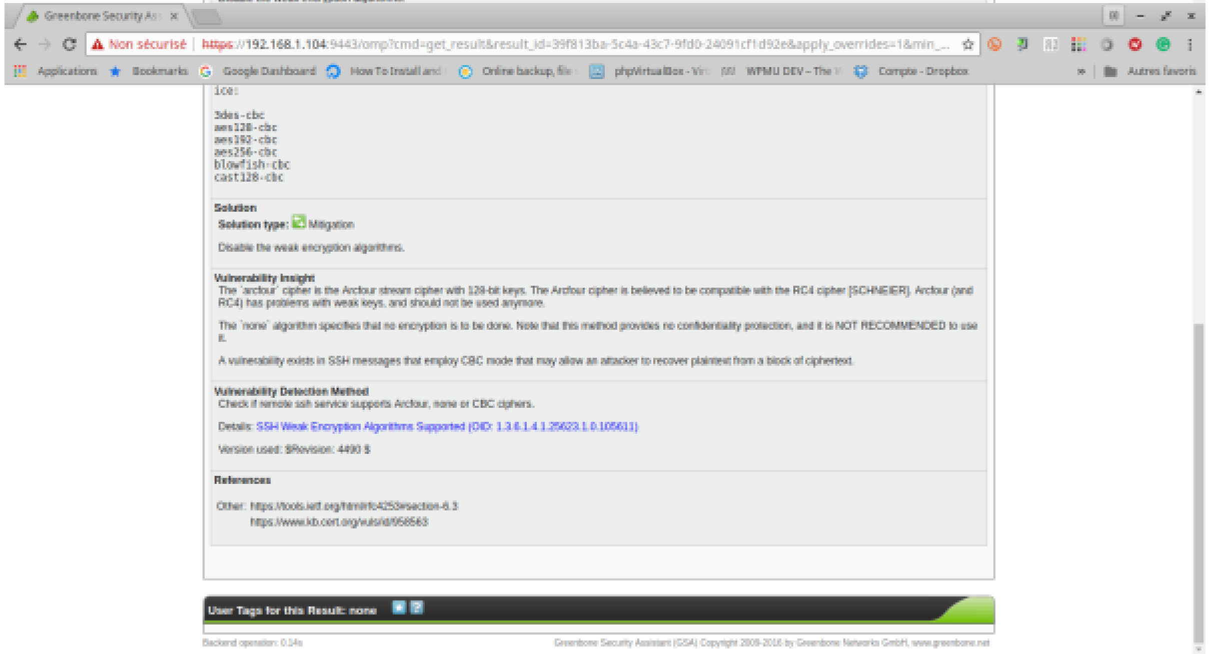
Vulnerability Detection Result

```
The following weak client-to-server encryption algorithms are supported by the remote serv↵
ice:

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 serv↵
ice:

3des-cbc
aes128-cbc
aes192-cbc
aes256-cbc
blowfish-cbc
cast128-cbc
```

Solution

Solution type: Mitigation

Disable the weak encryption algorithms.



Greenbone Security As ×
Non sécurisé | https://192.168.1.104:9443/omp?cmd=get_result&result_id=39f813ba-5c4a-43c7-9fd0-24091cf1d92e&apply_overrides=1&min_...
Applications Bookmarks Google Dashboard How To Install and Online backup, file phpVirtualBox - Vir WPMU DEV - The Compte - Dropbox Autres favoris

```
ice:

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

LAB #3 - Sécuriser le Serveur DNS

3.1 - Le serveur DNS

Le principe du DNS est basé sur l'équivalence entre un **FQDN** (Fully Qualified Domain Name) et une adresse IP. Les humains retiennent plus facilement des noms tels que www.ittraining.team, tandis que les ordinateurs utilisent des chiffres.

Le **DNS** (Domain Name Service) est né peut après l'introduction des FQDN en 1981.

Lorsqu'un ordinateur souhaite communiquer avec un autre par le biais de son nom, par exemple avec www.fenestros.com, il envoie une requête à un serveur DNS. Si le serveur DNS a connaissance de la correspondance entre le nom demandé et le numéro IP, il répond directement. Si ce n'est pas le cas, il démarre un processus de **Recursive Lookup**.

Ce processus tente d'identifier le serveur de domaine responsable pour le **SLD** (Second Level Domain) afin de lui passer la requête. Dans notre exemple, il tenterait d'identifier le serveur de domaine responsable de **ittraining.com**.

Si cette tentative échoue, le serveur DNS cherche le serveur de domaine pour le **TLD** (Top Level Domain) dans son cache afin de lui demander l'adresse du serveur responsable du SLD. Dans notre cas il tenterait trouver l'enregistrement pour le serveur de domaine responsable de **.com**

Si cette recherche échoue, le serveur s'adresse à un **Root Name Server** dont il y en a peu. Si le Root Name Server ne peut pas répondre, le serveur DNS renvoie une erreur à la machine ayant formulé la demande.

Le serveur DNS sert à faire la résolution de noms. Autrement dit de traduire une adresse Internet telle que **www.ittraining.com** en **numéro IP**.

3.2 - Préparation à l'Installation

Le serveur DNS nécessite que la machine sur laquelle il est installé possède un nom FQDN et une adresse IP fixe. Il est également important de noter que le service de bind ne démarrera **pas** dans le cas où le fichier **/etc/hosts** comporte une anomalie. Trois étapes préparatoires sont donc nécessaires :

- Modification de l'adresse IP de la machine en adresse IP fixe
- Définition d'un nom FQDN (Fully Qualified Domain Name)

- Vérification du fichier /etc/hosts

Afin d'étudier ce dernier cas, nous prenons en tant qu'exemple la machine suivante :

- **FQDN** - debian12.ittraining.loc
- **Adresse IP** - 10.0.2.46

Vérifiez la configuration de la VM :

```
root@debian12:~# hostname
debian12

root@debian12:~# hostnamectl set-hostname debian12.ittraining.loc

root@debian12:~# hostname
debian12.ittraining.loc

root@debian12:~# nmcli c show
NAME                UUID                                  TYPE      DEVICE
ip_fixe             33c26470-0968-4646-a88a-a22f10fab6da  ethernet  ens18
lo                  c4172990-a224-464f-a1de-9820ca5e83c8  loopback  lo
Wired connection 1  77c569e6-3176-4c10-8008-40d7634d2504  ethernet  --

root@debian12:~# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: ens18: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 56:a3:fd:18:02:6d brd ff:ff:ff:ff:ff:ff
    altname enp0s18
    inet 10.0.2.46/24 brd 10.0.2.255 scope global noprefixroute ens18
```

```
       valid_lft forever preferred_lft forever
    inet6 fe80::4b88:5cd8:60c9:6e2c/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
root@debian12:~# cat /etc/hosts
127.0.0.1       localhost
10.0.2.46       debian12.ittraining.loc debian12

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
```

Important - La configuration du serveur DNS dépend du nom de votre machine. Dans le cas où vous changeriez ce nom, vous devez reconfigurer votre serveur DNS en éditant les fichiers de configuration directement.

3.3 - Installation

Pour installer le serveur DNS, utilisez la commande **APT**:

```
root@debian12:~# apt install bind9 -y

root@debian12:~# systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-12-07 11:19:19 CET; 44s ago
       Docs: man:named(8)
   Main PID: 32581 (named)
     Status: "running"
      Tasks: 26 (limit: 19123)
     Memory: 116.9M
        CPU: 215ms
     CGroup: /system.slice/named.service
             └─32581 /usr/sbin/named -f -u bind

Dec 07 11:19:19 debian12.ittraining.loc named[32581]: network unreachable resolving '>
Dec 07 11:19:19 debian12.ittraining.loc named[32581]: network unreachable resolving '>
Dec 07 11:19:19 debian12.ittraining.loc named[32581]: network unreachable resolving '>
Dec 07 11:19:19 debian12.ittraining.loc named[32581]: network unreachable resolving '>
Dec 07 11:19:19 debian12.ittraining.loc named[32581]: network unreachable resolving '>
Dec 07 11:19:19 debian12.ittraining.loc named[32581]: network unreachable resolving '>
Dec 07 11:19:19 debian12.ittraining.loc named[32581]: network unreachable resolving '>
Dec 07 11:19:19 debian12.ittraining.loc named[32581]: network unreachable resolving '>
Dec 07 11:19:19 debian12.ittraining.loc named[32581]: managed-keys-zone: Initializing>
Dec 07 11:19:19 debian12.ittraining.loc named[32581]: managed-keys-zone: Initializing>
```

Options de la commande named

Les options de cette commande sont :

```
root@debian12:~# named help
usage: named [-4|-6] [-c conffile] [-d debuglevel] [-D comment] [-E engine]
             [-f|-g] [-L logfile] [-n number_of_cpus] [-p port] [-s]
             [-S sockets] [-t chrootdir] [-u username] [-U listeners]
             [-X lockfile] [-m {usage|trace|record}]
             [-M fill|nofill]
usage: named [-v|-V|-C]
named: extra command line arguments
```

3.4 - Les fichiers de configuration

Sous Debian12, les fichiers de configuration de **bind9** se trouvent dans **/etc/bind** :

```
root@debian12:~# ls -l /etc/bind
total 48
-rw-r--r-- 1 root root 2928 Oct 22 17:38 bind.keys
-rw-r--r-- 1 root root  255 Oct 22 17:38 db.0
-rw-r--r-- 1 root root  271 Oct 22 17:38 db.127
-rw-r--r-- 1 root root  237 Oct 22 17:38 db.255
-rw-r--r-- 1 root root  353 Oct 22 17:38 db.empty
-rw-r--r-- 1 root root  270 Oct 22 17:38 db.local
-rw-r--r-- 1 root bind  458 Oct 22 17:38 named.conf
-rw-r--r-- 1 root bind  498 Oct 22 17:38 named.conf.default-zones
-rw-r--r-- 1 root bind  165 Oct 22 17:38 named.conf.local
-rw-r--r-- 1 root bind  846 Oct 22 17:38 named.conf.options
-rw-r----- 1 bind bind  100 Dec  7 11:19 rndc.key
-rw-r--r-- 1 root root 1317 Oct 22 17:38 zones.rfc1918
```

named.conf

Le fichier de configuration principal du serveur DNS Bind est **/etc/bind/named.conf** :

```

root@debian12:~# cat /etc/bind/named.conf
// This is the primary configuration file for the BIND DNS server named.
//
// Please read /usr/share/doc/bind9/README.Debian for information on the
// structure of BIND configuration files in Debian, *BEFORE* you customize
// this configuration file.
//
// If you are just adding zones, please do that in /etc/bind/named.conf.local

include "/etc/bind/named.conf.options";
include "/etc/bind/named.conf.local";
include "/etc/bind/named.conf.default-zones";
```

Les directives **include**, incluent les fichiers suivants dans la configuration :

```
root@debian12:~# cat /etc/bind/named.conf.options
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and nameservers you want
        // to talk to, you may need to fix the firewall to allow multiple
        // ports to talk.  See http://www.kb.cert.org/vuls/id/800113

        // If your ISP provided one or more IP addresses for stable
        // nameservers, you probably want to use them as forwarders.
        // Uncomment the following block, and insert the addresses replacing
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //========================================================================
        // If BIND logs error messages about the root key being expired,
        // you will need to update your keys.  See https://www.isc.org/bind-keys
        //========================================================================
        dnssec-validation auto;

        listen-on-v6 { any; };
};
```

```
root@debian12:~# cat /etc/bind/named.conf.local
//
// Do any local configuration here
//
```

```
// Consider adding the 1918 zones here, if they are not used in your
// organization
//include "/etc/bind/zones.rfc1918";
```

```
root@debian12:~# cat /etc/bind/named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

Les Sections de Zone

La Valeur Type

Maintenant, étudions les sections de zones. La valeur “type” peut prendre plusieurs valeurs:

- **master**
  - Ce type définit le serveur DNS comme serveur maître ayant **autorité** sur la zone concernée.
- **slave**
  - Ce type définit le serveur DNS comme serveur esclave pour la zone concernée. Ceci implique que la zone est une réplication d'une zone maîtresse. Un type de zone esclave contiendra aussi une directive **masters** indiquant les adresses IP des serveurs DNS maîtres.
- **stub**
  - Ce type définit le serveur DNS comme serveur esclave pour la zone concernée mais uniquement pour les **enregistrements** de type **NS**.
- **forward**
  - Ce type définit le serveur DNS comme serveur de transit pour la zone concernée. Ceci implique que toute requête est retransmise vers un autre serveur.
- **hint**
  - Ce type définit la zone concernée comme une zone racine. Ceci implique que lors du démarrage du serveur, cette zone est utilisée pour récupérer les adresses des serveurs DNS racine.

La valeur “notify” est utilisée pour indiquer si non (no) ou oui (yes) les autres serveurs DNS sont informés de changements dans la zone.

La Valeur File

La deuxième directive dans une section de zone comporte la valeur **file**. Il indique l'emplacement du fichier de zone.

Exemples de Sections de Zone

Chaque section de zone, à l'exception de la zone “.” est associée avec une section de zone inversée.

La zone “.” est configurée dans le fichier **/usr/share/dns/root.hints** :

```
...
```

```
zone "." {
        type hint;
        file "/usr/share/dns/root.hints";
};
...
```

La section de zone fait correspondre un nom avec une adresse IP tandis que la section de zone inversée fait l'inverse. La section inversée a un nom d'un syntaxe spécifique :

```
adresse_réseau_inversée.in-addr.arpa.
```

Par exemple dans le fichier ci-dessus nous trouvons les quatre sections suivantes :

```
...
zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};
```

```
...
```

Sections de Zones de votre Machine

Afin de configurer notre serveur correctement, il est necéssaire d'ajouter à ce fichier deux sections supplémentaires :

- La zone correspondante à notre domaine, ici appelée “ittraining.loc”. Celle-ci fait correspondre le nom de la machine avec son adresse IP:

```
...
zone "ittraining.loc" {
    type master;
    file "/etc/bind/zones/ittraining.loc";
    forwarders { };
};
...
```

- La zone à notre domaine mais dans le sens inverse. A savoir le fichier **db.2.0.10.hosts** qui fait correspondre notre adresse IP avec le nom de la machine.

```
...
zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.2.0.10.hosts";
    forwarders { };
};
...
```

Ajoutez donc ces deux sections au fichier **/etc/bind/named.conf.default-zones** :

```
root@debian12:~# vi /etc/bind/named.conf.default-zones

root@debian12:~# cat /etc/bind/named.conf.default-zones
// prime the server with knowledge of the root servers
```

```
zone "." {
        type hint;
        file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

zone "ittraining.loc" {
    type master;
    file "/etc/bind/zones/ittraining.loc";
    forwarders { };
};
```

```
zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.2.0.10.hosts";
    forwarders { };
};
```

Les fichiers de zone

La fichiers de zone sont composées de lignes d'une forme:

nom	TTL	classe	type	donnée

où

- **nom**
  - Le nom DNS.
- **TTL**
  - La durée de vie en cache de cet enregistrement.
- **classe**
  - Le réseau de transport utilisé. Dans notre cas, le réseau est du TCP. La valeur est donc IN.
- **type**
  - Le type d'enregistrement:
    - SOA - Start of Authority - se trouve au début du fichier et contient des informations générales
    - NS - Name Server - le nom du serveur de nom
    - A - Address - indique une résolution de nom vers une adresse IP. Ne se trouve que dans les fichiers **.hosts**
    - PTR - PoinTeR - indique une résolution d'une adresse IP vers un nom. Ne se trouve que dans les fichiers inversés.
    - MX - Mail eXchange - le nom d'un serveur de mail.
    - CNAME - Canonical Name - un alias d'une machine.
    - HINFO - Hardware Info - fournit des informations sur le matériel de la machine
- **donnée**
  - La donnée de la ressource:
    - Une adresse IP pour un enregistrement de type A
    - Un nom de machine pour un eregistrement de type PTR

ittraining.loc

Ce fichier se trouve dans /etc/bind/zones. C'est le fichier qui définit la correspondance du nom de la machine **debian12.ittraining.loc** avec son numéro IP, à savoir le **10.0.2.46**. On définit dans ce fichier les machines qui doivent être appelées par leur nom :

```
root@debian12:~# mkdir /etc/bind/zones

root@debian12:~# vi /etc/bind/zones/ittraining.loc

root@debian12:~# cat /etc/bind/zones/ittraining.loc
$TTL 3D
@       IN     SOA     debian12.ittraining.loc. root.debian12.ittraining.loc. (
               2025120701       ; Serial
               8H   ; Refresh
               2H   ; Retry
               4W  ; Expire
               1D)  ; Minimum TTL
               IN      NS      debian12.ittraining.loc.
localhost                   A              127.0.0.1
dnsmaster                   IN      CNAME  debian12.ittraining.loc.
debian12.ittraining.loc.    IN      A      10.0.2.46

ftp IN CNAME debian12.ittraining.loc.
www IN CNAME debian12.ittraining.loc.
mail IN CNAME debian12.ittraining.loc.
news IN CNAME debian12.ittraining.loc.
```

Important - Notez le point à la fin de chaque nom de domaine. Notez bien le remplacement du caractère @ dans l'adresse email de l'administrateur de mail par le caractère “.”

La première ligne de ce fichier commence par une ligne semblable à celle-ci:

```
$TTL 3D
```

Cette ligne indique aux autres serveurs DNS pendant combien de temps ils doivent garder en cache les enregistrements de cette zone. La durée peut s'exprimer en jours (**D**), en heures (**H**) ou en secondes (**S**).

La deuxième ligne définit une **classe IN**ternet, un **SOA** (Start Of Authority), le nom du serveur primaire et l'adresse de l'administrateur de mail :

```
@       IN     SOA     debian12.ittraining.loc. root.debian12.ittraining.loc. (
```

Le caractère **@** correspond au nom de la zone et est une abréviation pour le nom de la zone décrit par le fichier de la zone, soit dans ce cas db.**ittraining.loc**.hosts, et présent dans le fichier /etc/bind/named.conf.default-zones :

```
zone "ittraining.loc" {
    type master;
    file "/etc/bind/zones/ittraining.loc";
    forwarders { };
};
```

Le **numéro de série** doit être modifié chaque fois que le fichier est changé. Il faut noter que dans le cas de plusieurs changements dans la même journée il est nécessaire d'incrémenter les deux derniers chiffres du numéro de série. Par exemple, dans le cas de deux changements en date du 07/12/2025, le premier fichier comportera une ligne Serial avec la valeur 2025120701 tandis que le deuxième changement comportera le numéro de série 2025120702 :

```
2025120701       ; Serial
```

La ligne suivante indique le temps de rafraîchissement, soit 8 heures. Ce temps correspond à la durée entre les mises à jour d'un autre serveur :

```
       8H ; Refresh
```

La ligne suivante indique le temps entre de nouveaux essaies de mise à jour d'un autre serveur dans le cas où la durée du Refresh a été dépassée :

```
       2H ; Retry
```

La ligne suivante indique le temps d'expiration, c'est-à-dire la durée d'autorité de l'enregistrement. Cette directive est utilisée seulement par un serveur esclave :

```
       4W ; Expire
```

La ligne suivante indique le temps minimum pour la valeur TTL, soit un jour:

```
       1D) ; Minimum TTL
```

Cette ligne identifie notre serveur de noms :

```
IN NS debian12.ittraining.loc.
```

Dans le cas où notre serveur était également un serveur mail. Nous trouverions aussi une entrée du type SMTP (MX) :

```
IN MX 10 mail.ittraining.loc.
```

Ci-dessous on définit avec une entrée du type A, les machines que l'on souhaite appeler par leur nom, à savoir **debian12.ittraining.loc** et **localhost** :

```
localhost                   A              127.0.0.1
...
debian12.ittraining.loc.    IN      A      10.0.2.46
```

Ci-dessous on définit des **Alias** avec des entrées du type CNAME. Les alias servent à identifier une machine.

```
dnsmaster                   IN      CNAME  debian12.ittraining.loc.
```

Nous pourrions aussi trouver ici des entrées telles:

```
ftp IN CNAME debian12.ittraining.loc.
www IN CNAME debian12.ittraining.loc.
```

```
mail IN CNAME debian12.ittraining.loc.
news IN CNAME debian12.ittraining.loc.
```

db.2.0.10.hosts

Ce fichier se trouve dans /etc/bind/zones/. C'est le fichier qui définit la correspondance de l'adresse IP de la machine, à savoir le **10.0.2.46** avec le nom **debian12.ittraining.loc**. Le chiffre **46** dans la dernière ligne correspond au 10.0.2.**46**:

```
root@debian12:~# vi /etc/bind/zones/db.2.0.10.hosts

root@debian12:~# cat /etc/bind/zones/db.2.0.10.hosts
$TTL 3D
@       IN      SOA     debian12.ittraining.loc.        debian12.ittraining.loc. (
                2025120701 ; Serial
                10800   ; Refresh
                3600    ; Retry
                604800  ; Expire
                86400) ; Minimum TTL
                NS      debian12.ittraining.loc.
46       IN      PTR     debian12.ittraining.loc.
```

Modifiez maintenant les permissions sur les fichiers de configuration :

```
root@debian12:~# ls -l /etc/bind/zones/*
-rw-r--r-- 1 root bind 362 Dec  7 12:16 /etc/bind/zones/db.2.0.10.hosts
-rw-r--r-- 1 root bind 634 Dec  7 12:06 /etc/bind/zones/ittraining.loc

root@debian12:~# chmod g+w /etc/bind/zones/*

root@debian12:~# ls -l /etc/bind/zones/*
-rw-rw-r-- 1 root bind 362 Dec  7 12:16 /etc/bind/zones/db.2.0.10.hosts
-rw-rw-r-- 1 root bind 634 Dec  7 12:06 /etc/bind/zones/ittraining.loc
```

3.5 - Utilisation

Modifiez maintenant le fichier **/etc/resolv.conf** afin d'utiliser votre propre serveur DNS :

```
root@debian12:~# vi /etc/resolv.conf

root@debian12:~# cat /etc/resolv.conf
# Generated by NetworkManager
search ittraining.loc
nameserver 127.0.0.1
nameserver 8.8.8.8
```

Dernièrement, redémarrez le service named :

```
root@debian12:~# systemctl restart named

root@debian12:~# systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-12-07 12:19:11 CET; 7s ago
       Docs: man:named(8)
   Main PID: 32731 (named)
     Status: "running"
      Tasks: 18 (limit: 19123)
     Memory: 109.1M
        CPU: 86ms
     CGroup: /system.slice/named.service
             └─32731 /usr/sbin/named -f -u bind

Dec 07 12:19:11 debian12.ittraining.loc named[32731]: network unreachable resolving './DNSKEY/IN':
2801:1b8:10::b#53
Dec 07 12:19:11 debian12.ittraining.loc named[32731]: network unreachable resolving './NS/IN': 2801:1b8:10::b#53
Dec 07 12:19:11 debian12.ittraining.loc named[32731]: network unreachable resolving './DNSKEY/IN':
```

```
2001:500:1::53#53
Dec 07 12:19:11 debian12.ittraining.loc named[32731]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Dec 07 12:19:11 debian12.ittraining.loc named[32731]: network unreachable resolving './DNSKEY/IN':
2001:500:2f::f#53
Dec 07 12:19:11 debian12.ittraining.loc named[32731]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Dec 07 12:19:11 debian12.ittraining.loc named[32731]: network unreachable resolving './DNSKEY/IN':
2001:503:c27::2:30#53
Dec 07 12:19:11 debian12.ittraining.loc named[32731]: network unreachable resolving './NS/IN':
2001:503:c27::2:30#53
Dec 07 12:19:12 debian12.ittraining.loc named[32731]: managed-keys-zone: Key 20326 for zone . is now trusted
(acceptance timer complete)
Dec 07 12:19:12 debian12.ittraining.loc named[32731]: managed-keys-zone: Key 38696 for zone . is now trusted
(acceptance timer complete)
```

Testez maintenant votre serveur :

```
root@debian12:/etc/bind/zones# nslookup debian12.ittraining.loc
Server:         127.0.0.1
Address:        127.0.0.1#53

Name:   debian12.ittraining.loc
Address: 10.0.2.46

root@debian12:~# dig ittraining.loc

; <<>> DiG 9.18.41-1~deb12u1-Debian <<>> ittraining.loc
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 51890
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 74a7e4078e44bf490100000069356348f4e348254883e231 (good)
```

```
;; QUESTION SECTION:
;ittraining.loc.                        IN      A

;; AUTHORITY SECTION:
ittraining.loc.         86400   IN      SOA     debian12.ittraining.loc. root.debian12.ittraining.loc. 2025120701 28800 7200 2419200 86400

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Dec 07 12:21:44 CET 2025
;; MSG SIZE  rcvd: 121

root@debian12:~# dig -x 10.0.2.46

; <<>> DiG 9.18.41-1~deb12u1-Debian <<>> -x 10.0.2.46
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 5254
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: b019ecafc27e89760100000693563584aff28c151c1bd67 (good)
;; QUESTION SECTION:
;46.2.0.10.in-addr.arpa.                IN      PTR

;; ANSWER SECTION:
46.2.0.10.in-addr.arpa. 259200  IN      PTR     debian12.ittraining.loc.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Dec 07 12:22:00 CET 2025
;; MSG SIZE  rcvd: 116
```

Important - Notez l'utilisation de l'option **-x** de la commande **dig** pour tester la zone à l'envers.

3.6 - Créer les Pairs de Clefs

Utilisez la commande **dnssec-keygen** pour créer la ZSK :

```
root@debian12:~# cd /etc/bind/zones/

root@debian12:/etc/bind/zones# dnssec-keygen -b 2048 -a RSASHA256 ittraining.loc
Generating key
pair............+.....+...+....+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....+........+.
..+...+....+...+........+.......+.....+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*.....
...+.........+..............+....+..+...+.+......+...+..+...+..........+...+.....+...+......+.+........+.+.......
..+..+.........+......+...+......+.........+..........+......+.....+...+.+.........+...+.....+....+...+..........
..+........+.+...........+...+...+...+........................+...+.......+......+.....+.+....................+..
..+.....+......................+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
..+......+........+.......+.....+......+...+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*....
...+......+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*................+.+............+.....
+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++
Kittraining.loc.+008+18528
```

Important - L'option **-a RSASHA256** force l'utilisation de l'algorithme SHA2 au lieu de SHA1.

```
root@debian12:/etc/bind/zones# ls -l
total 24
```

```
-rw-rw-r-- 1 root bind  362 Dec  7 12:16 db.2.0.10.hosts
-rw-rw-r-- 1 root bind  747 Dec  7 13:13 ittraining.loc
-rw-r--r-- 1 root bind  612 Dec  7 13:28 Kittraining.loc.+008+18528.key
-rw------- 1 root bind 1776 Dec  7 13:28 Kittraining.loc.+008+18528.private
```

Important - Dans le nom de chaque fichier, **008** indique l'utilisation de SHA2. Dans le cas de l'utilisation de SHA1, la valeur serait **005**. La valeur **18528** est l'identifiant du pair de clefs.

Utilisez la commande **dnssec-keygen** pour créer la KSK :

```
root@debian12:/etc/bind/zones# dnssec-keygen -b 4096 -f KSK -a RSASHA256 ittraining.loc
Generating key
pair..+.....+....+......+......+.....+....+...+.....+......+......................+........+....+...+...+........
.+..+...+.+..+++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++++*...+.....+.+...........+++++++++++
++++++++++++++++++++++++++++++++++++++++++++++++++++++*.........+.......+......+..+......+.......+.........+.....
.........+.........+.+..+....+.....+....+..+.......+...+..+......+..........+...........+.+....................+.
..+......+.........+.........+.+......+........+...+............+..........+...+...+....................+....+...
.....+...+....+..................+..............+.........+.......+...+..+.......++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++++++++++
..+..+....+..+.......+..+......+.........+....+..+..........+.....+.......+++++++++++++++++++++++++++++++++++++++
++++++++++++++++++++++++++*..+.......+........+.+.....+.......+........+.......+..+.+......+..............+.+....
..+.........+...+......+.........+...+.................+................+......+.....+....+++++++++++++++++++++++
++++++++++++++++++++++++++++++++++++++++++*...........+....+...+............+..............+..........+..........
.......+.............+.........+..+...+.+..+.........+...+.............+...+.....+....+..+...+......+.......+...+
.........+...+.....+.........+....+...........+......+.......+...........+.+.........+.....+.+.....+.............
.....+.+..+.........+.........+.......+........+...................+.....++++++++++++++++++++++++++++++++++++++++
+++++++++++++++++++++++++
Kittraining.loc.+008+63515
```

Important - L'option **-f** indique le type de pair de clefs, soit KSK.

Constatez la présence des pairs de clefs :

```
root@debian12:/etc/bind/zones# ls -l
total 24
-rw-rw-r-- 1 root bind  362 Dec  7 12:16 db.2.0.10.hosts
-rw-rw-r-- 1 root bind  747 Dec  7 13:13 ittraining.loc
-rw-r--r-- 1 root bind  612 Dec  7 13:28 Kittraining.loc.+008+18528.key
-rw------- 1 root bind 1776 Dec  7 13:28 Kittraining.loc.+008+18528.private
-rw-r--r-- 1 root bind  957 Dec  7 13:28 Kittraining.loc.+008+63515.key
-rw------- 1 root bind 3316 Dec  7 13:28 Kittraining.loc.+008+63515.private
```

3.7 - Modifier la Configuration de Bind

Ajoutez les deux clefs publiques dans la configuration du fichier de zone **/etc/bind/zones/ittraining.loc** :

```
root@debian12:/etc/bind/zones# vi ittraining.loc

root@debian12:/etc/bind/zones# cat ittraining.loc
$TTL 3D
@       IN     SOA     debian12.ittraining.loc. root.debian12.ittraining.loc. (
               2025120702       ; Serial
               8H   ; Refresh
               2H   ; Retry
               4W  ; Expire
               1D)  ; Minimum TTL
               IN      NS      debian12.ittraining.loc.
localhost                   A              127.0.0.1
dnsmaster                   IN      CNAME  debian12.ittraining.loc.
debian12.ittraining.loc.    IN      A      10.0.2.46
```

```
ftp IN CNAME debian12.ittraining.loc.
www IN CNAME debian12.ittraining.loc.
mail IN CNAME debian12.ittraining.loc.
news IN CNAME debian12.ittraining.loc.

$include /etc/bind/zones/Kittraining.loc.+008+18528.key
$include /etc/bind/zones/Kittraining.loc.+008+63515.key
```

Important - N'oubliez pas de changer la valeur **serial**.

Redémarrez le service **named** :

```
root@debian12:/etc/bind/zones# systemctl restart named

root@debian12:/etc/bind/zones# systemctl status  named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-12-07 13:32:03 CET; 7s ago
       Docs: man:named(8)
   Main PID: 32952 (named)
     Status: "running"
      Tasks: 18 (limit: 19123)
     Memory: 113.1M
        CPU: 83ms
     CGroup: /system.slice/named.service
             └─32952 /usr/sbin/named -f -u bind

Dec 07 13:32:03 debian12.ittraining.loc named[32952]: network unreachable resolving './DNSKEY/IN':
2001:503:ba3e::2:30#53
Dec 07 13:32:03 debian12.ittraining.loc named[32952]: network unreachable resolving './NS/IN':
2001:503:ba3e::2:30#53
```

```
Dec 07 13:32:03 debian12.ittraining.loc named[32952]: network unreachable resolving './DNSKEY/IN':
2001:7fe::53#53
Dec 07 13:32:03 debian12.ittraining.loc named[32952]: network unreachable resolving './NS/IN': 2001:7fe::53#53
Dec 07 13:32:03 debian12.ittraining.loc named[32952]: network unreachable resolving './DNSKEY/IN':
2001:500:9f::42#53
Dec 07 13:32:03 debian12.ittraining.loc named[32952]: network unreachable resolving './NS/IN': 2001:500:9f::42#53
Dec 07 13:32:03 debian12.ittraining.loc named[32952]: network unreachable resolving './DNSKEY/IN':
2001:503:c27::2:30#53
Dec 07 13:32:03 debian12.ittraining.loc named[32952]: network unreachable resolving './NS/IN':
2001:503:c27::2:30#53
Dec 07 13:32:03 debian12.ittraining.loc named[32952]: managed-keys-zone: Key 20326 for zone . is now trusted
(acceptance timer complete)
Dec 07 13:32:03 debian12.ittraining.loc named[32952]: managed-keys-zone: Key 38696 for zone . is now trusted
(acceptance timer complete)
```

Intérogez le DNS local pour obtenir les clefs publiques :

```
root@debian12:/etc/bind/zones# dig @debian12.ittraining.loc DNSKEY ittraining.loc

; <<>> DiG 9.18.41-1~deb12u1-Debian <<>> @debian12.ittraining.loc DNSKEY ittraining.loc
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 58210
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 74f4778aedb99b4d01000000693576d3fe2e16da8329795a (good)
;; QUESTION SECTION:
;ittraining.loc.                        IN      DNSKEY

;; ANSWER SECTION:
ittraining.loc.         259200  IN      DNSKEY  256 3 8 AwEAAZ+2bRM+yedcAeqUR6AdkSzyIeQg1kH4021as3WvYGlOLqeUnfbe
```

```
gNewRYifndXx/b1t84A9L6IZH1ZamuSNxNi7Y0+FZbyq4DJmFnHA68Ao 5zmOhK76mrQf6SjzQHZWzwtoG0DAApTggaRxhmezzjkSr3WNadIoFg4F
XU5UaV4ePU5hhPn+zi34SUYvgPTZsSWb/solo0yna80RBxI+hgRxoaPp jV/v4mEVVS9Fjpvc6SxJ/ZZbtUMJi5lTUCvko+Ny9cuXZ5auW4b2qp4u
Sk6NuywMawQafxBaxZ/9KuhxqO4qp2n1pl+gBatqb/XPydE41z6ONkT2 YnDOLQVZxLM=
ittraining.loc.         259200  IN      DNSKEY  257 3 8 AwEAAcRrC7vljqlLFZGQbLUBpMs29NWyiJ8158xqL0GdZuRslhAqy4q2
JisfBS1gKm27J4y2s8zrDhKLAnEqWpIydvRkZd+a6oTJAomfAF9bxHAe xxEyLK7Xd4ATGiXRUv2vALQq1e6XejBhVr10gmbKdQW+SxayYnwQ0G8h
1VFJ2wtAJZdNn/exhmgxxmUwxeJWLmUf37VOkycwn4RbwWZY3rBIOi2V mCigGe1cDpZoNb2FCTKLjEj5ZRz0ieM9SXXLkZEvGd77xAvoV8+JTTX5
BjlP6Hfso+C/NZUchvoNYisqWSPzffyrsaOzumMtuIsKJX2PaADSmFg8 os/b16zqtPbd+lPhQdsR+RE9V5R0YJhNPnsoG0Vy/mfQCCcP7VIC97iB
aYSz/u5KFhsS5E0AIJt8rJwGrb2eqZYTFe2Mdtth1FjgIk7DCvFm2GYM zZ0F15WqcBpJGEDof0/HWSpMfjbnc20QAojLYmuek5XE9lWlZLrk9tby
q4R7dZrUdDez3oShtJ/rXTA8AxOzcftLsoCZHy+bMfy5RxThidWQYJGE dQsnk3IgJ1pgzSjdB4nXQkyxMBpRzjyxPw9k1a4oLxYrdLQnHkm5RdWA
b5k6Csu2xmSKaQUy9oyLaCRrkd9BnpJPELjRmXIdmyswevjmUr9qwLtk L1W/qxN3it6Ribh3

;; Query time: 4 msec
;; SERVER: 10.0.2.46#53(debian12.ittraining.loc) (UDP)
;; WHEN: Sun Dec 07 13:45:07 CET 2025
;; MSG SIZE  rcvd: 879
```

3.8 - Signer la Zone

Les clefs étant maintenant insérées dans la configuration, il convient de signer la zone en utilisant la commande **dnssec-signzone**. L'option **-S** signifie **smart signing** permet de trouver automatiquement les fichiers de clefs pour la zone et détermine comment ils doivent être utilisés :

```
root@debian12:/etc/bind/zones# dnssec-signzone -S ittraining.loc
Verifying the zone using the following algorithms:
- RSASHA256
Zone fully signed:
Algorithm: RSASHA256: KSKs: 1 active, 0 stand-by, 0 revoked
                      ZSKs: 1 active, 0 stand-by, 0 revoked
ittraining.loc.signed

root@debian12:/etc/bind/zones# ls -l | grep signed
-rw-r--r-- 1 root bind 12407 Dec  7 13:39 ittraining.loc.signed
```

Consultez le fichier **ittraining.loc.signed** :

```
root@debian12:/etc/bind/zones# more ittraining.loc.signed
; File written on Sun Dec  7 13:39:03 2025
; dnssec_signzone version 9.18.41-1~deb12u1-Debian
ittraining.loc.         259200  IN SOA  debian12.ittraining.loc. root.debian12.ittraining.loc. (
                                        2025120703 ; serial
                                        28800      ; refresh (8 hours)
                                        7200       ; retry (2 hours)
                                        2419200    ; expire (4 weeks)
                                        86400      ; minimum (1 day)
                                        )
                        259200  RRSIG   SOA 8 2 259200 (
                                        20260106113903 20251207113903 18528 ittraining.loc.
                                        ANlboBzlffzcYC1G10cQuxvRP3XC5bvDP1+v
                                        Baxfh/B4BxgYGeQoDih2uGqLxzDExRWix2a2
                                        B95uAkDGClaGdlFkYtU4voIQJWuAx0Goo6Xa
                                        omEyrIdLGqoj9e2vdn6j2lVpJik9YgCTxP2G
                                        ShVYc632XsAFPXN6SJrR3QdKo1x6KM1uPYdd
                                        OxAX9fGNYj59ZXG84slUxreDejoqn2k8Rx68
                                        gxuzkIY3oM5aUtbvL8bwjflk121mWxQ4vVhW
                                        R/KNk9SEc6AbZSqJXwmlY/vReOA+pvPCdLYJ
                                        7Wf+S9kr1i1xT1y078Iqz2twASWBjBnP/adG
                                        QtKpn9SvKUEzICTaNA== )
                        259200  NS      debian12.ittraining.loc.
                        259200  RRSIG   NS 8 2 259200 (
                                        20260106113903 20251207113903 18528 ittraining.loc.
                                        CGtE8nZ2F0JQLAmbyPgrqKLDXjyWg2hZmEcf
                                        22h2zAxJZWjNWB7k5aLHA6weKkvo7mTnH7sS
                                        pEazWPhaDzmW2BLfdBjeaSZzj+mMWUiXVnUq
                                        LYAMLRXGD1NAPcuSQlyzDpN0JZXwWfQFTpzT
                                        DJttJyChcQgyJmvaJEhIhQK5gRFMaT+Ww1zg
                                        pvAke0HlkSEz9mQxIhff5FqSL00Zyn5mnLBB
                                        N6X1XKQXL/mUJ8nb9X70n9b/qsYqAQdFFxzS
                                        6lz+kMr/D1AhzabDGkeD/+xlXSPMygYc4I6b
                                        eYZKmEsD8HOdYJb5JlWicP7cheeKonPXxjrZ
                                        TQqLDJFaRETE+IDnLQ== )
                        86400   NSEC    debian12.ittraining.loc. NS SOA RRSIG NSEC DNSKEY
                        86400   RRSIG   NSEC 8 2 86400 (
                                        20260106113903 20251207113903 18528 ittraining.loc.
                                        dDLcoBI/agA+tHni16R8aWdWHBqPPfBjbFRZ
                                        775fNQI/d20d47vFx/u2rx+WzenCSZBOpU/J
                                        2b8Q2Dm26f218L1KYF7NF7dew2s5OUIkfM+V
                                        iZIqBSAFYyAbLYRCfbQA6DxsIgDT6T/x7jLf
                                        +jYHNeASGauWunufrSLvbqdsIE0z+JH+3AVE
                                        JaLTeXYL6I+/U4vn+EwVOiOuVv3eOt8d1d5a
                                        0lqDK8qRlcbhFF1ngOJHe+Fa5ect9kqnbjCa
                                        7mwOOmp4v4JA6Myvvut7OEDI5mQItd9HApPl
                                        eM0kvui7mioUEUCM2EXRPtJYXVAELUnqGz1S
                                        hn6EYefpcWvUDo8veg== )
                        259200  DNSKEY  256 3 8 (
                                        AwEAAZ+2bRM+yedcAeqUR6AdkSzyIeQg1kH4
                                        021as3WvYGlOLqeUnfbegNewRYifndXx/b1t
                                        84A9L6IZH1ZamuSNxNi7Y0+FZbyq4DJmFnHA
                                        68Ao5zmOhK76mrQf6SjzQHZWzwtoG0DAApTg
                                        gaRxhmezzjkSr3WNadIoFg4FXU5UaV4ePU5h
                                        hPn+zi34SUYvgPTZsSWb/solo0yna80RBxI+
                                        hgRxoaPpjV/v4mEVVS9Fjpvc6SxJ/ZZbtUMJ
--More--(18%)
```

Consultez la section RRSIG du SOA :

```
...
                        259200  RRSIG   SOA 8 2 259200 (
                                        20260106113903 20251207113903 18528 ittraining.loc.
                                        ANlboBzlffzcYC1G10cQuxvRP3XC5bvDP1+v
                                        Baxfh/B4BxgYGeQoDih2uGqLxzDExRWix2a2
                                        B95uAkDGClaGdlFkYtU4voIQJWuAx0Goo6Xa
                                        omEyrIdLGqoj9e2vdn6j2lVpJik9YgCTxP2G
                                        ShVYc632XsAFPXN6SJrR3QdKo1x6KM1uPYdd
                                        OxAX9fGNYj59ZXG84slUxreDejoqn2k8Rx68
                                        gxuzkIY3oM5aUtbvL8bwjflk121mWxQ4vVhW
                                        R/KNk9SEc6AbZSqJXwmlY/vReOA+pvPCdLYJ
                                        7Wf+S9kr1i1xT1y078Iqz2twASWBjBnP/adG
                                        QtKpn9SvKUEzICTaNA== )
...
```

Dans cette section on constate :

- L'ID de la clef **18528** utilisée pour la signature, soit la ZSK
- La date et l'heure de la signature **20251207113903**
- La date et l'heure de l'expiration de la signature **20260106113903**

Configurez Bind pour qu'il utilise le fichier signé :

```
root@debian12:/etc/bind/zones# vi ../named.conf.default-zones
root@debian12:/etc/bind/zones# cat ../named.conf.default-zones
// prime the server with knowledge of the root servers
zone "." {
        type hint;
        file "/usr/share/dns/root.hints";
};

// be authoritative for the localhost forward and reverse zones, and for
// broadcast zones as per RFC 1912

zone "localhost" {
        type master;
        file "/etc/bind/db.local";
};

zone "127.in-addr.arpa" {
        type master;
        file "/etc/bind/db.127";
};

zone "0.in-addr.arpa" {
        type master;
        file "/etc/bind/db.0";
};

zone "255.in-addr.arpa" {
        type master;
        file "/etc/bind/db.255";
};

zone "ittraining.loc" {
    type master;
    file "/etc/bind/zones/ittraining.loc.signed";
    forwarders { };
};

zone "2.0.10.in-addr.arpa" {
    type master;
    file "/etc/bind/zones/db.2.0.10.hosts";
    forwarders { };
};
```

Redémarrez le service **named** :

```
root@debian12:/etc/bind/zones# systemctl restart named

root@debian12:/etc/bind/zones# systemctl status named
● named.service - BIND Domain Name Server
     Loaded: loaded (/lib/systemd/system/named.service; enabled; preset: enabled)
     Active: active (running) since Sun 2025-12-07 14:02:52 CET; 7s ago
       Docs: man:named(8)
   Main PID: 33227 (named)
```

```
     Status: "running"
      Tasks: 18 (limit: 19123)
     Memory: 109.0M
        CPU: 88ms
     CGroup: /system.slice/named.service
             └─33227 /usr/sbin/named -f -u bind

Dec 07 14:02:52 debian12.ittraining.loc named[33227]: network unreachable resolving './DNSKEY>
Dec 07 14:02:52 debian12.ittraining.loc named[33227]: network unreachable resolving './NS/IN'>
Dec 07 14:02:52 debian12.ittraining.loc named[33227]: network unreachable resolving './DNSKEY>
Dec 07 14:02:52 debian12.ittraining.loc named[33227]: network unreachable resolving './NS/IN'>
Dec 07 14:02:52 debian12.ittraining.loc named[33227]: network unreachable resolving './DNSKEY>
Dec 07 14:02:52 debian12.ittraining.loc named[33227]: network unreachable resolving './NS/IN'>
Dec 07 14:02:52 debian12.ittraining.loc named[33227]: network unreachable resolving './DNSKEY>
Dec 07 14:02:52 debian12.ittraining.loc named[33227]: network unreachable resolving './NS/IN'>
Dec 07 14:02:52 debian12.ittraining.loc named[33227]: managed-keys-zone: Key 20326 for zone .>
Dec 07 14:02:52 debian12.ittraining.loc named[33227]: managed-keys-zone: Key 38696 for zone .>
```

Demandez l'enregistrement SOA du DNS local :

```
root@debian12:/etc/bind/zones# dig @debian12.ittraining.loc ittraining.loc SOA

; <<>> DiG 9.18.41-1~deb12u1-Debian <<>> @debian12.ittraining.loc ittraining.loc SOA
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 42848
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: a42dbdb3e931b5b40100000069357b611d705b9c213bca01 (good)
;; QUESTION SECTION:
;ittraining.loc.                        IN      SOA
```

```
;; ANSWER SECTION:
ittraining.loc.         259200  IN      SOA     debian12.ittraining.loc. root.debian12.ittraining.loc. 2025120703
28800 7200 2419200 86400

;; Query time: 0 msec
;; SERVER: 10.0.2.46#53(debian12.ittraining.loc) (UDP)
;; WHEN: Sun Dec 07 14:04:33 CET 2025
;; MSG SIZE  rcvd: 121
```

Demandez l'enregistrement SOA et sa signature du DNS local :

```
root@debian12:/etc/bind/zones# dig @debian12.ittraining.loc ittraining.loc SOA +dnssec

; <<>> DiG 9.18.41-1~deb12u1-Debian <<>> @debian12.ittraining.loc ittraining.loc SOA +dnssec
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56632
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: 14cfa09283a1f49801000000069357b95d90b040d04f37247 (good)
;; QUESTION SECTION:
;ittraining.loc.                        IN      SOA

;; ANSWER SECTION:
ittraining.loc.         259200  IN      SOA     debian12.ittraining.loc. root.debian12.ittraining.loc. 2025120703
28800 7200 2419200 86400
ittraining.loc.         259200  IN      RRSIG   SOA 8 2 259200 20260106113903 20251207113903 18528
ittraining.loc. ANlboBzlffzcYC1G10cQuxvRP3XC5bvDP1+vBaxfh/B4BxgYGeQoDih2
uGqLxzDExRWix2a2B95uAkDGClaGdlFkYtU4voIQJWuAx0Goo6XaomEy rIdLGqoj9e2vdn6j2lVpJik9YgCTxP2GShVYc632XsAFPXN6SJrR3QdK
o1x6KM1uPYddOxAX9fGNYj59ZXG84slUxreDejoqn2k8Rx68gxuzkIY3 oM5aUtbvL8bwjflk121mWxQ4vVhWR/KNk9SEc6AbZSqJXwmlY/vReOA+
pvPCdLYJ7Wf+S9kr1i1xT1y078Iqz2twASWBjBnP/adGQtKpn9SvKUEz ICTaNA==
;; Query time: 0 msec
;; SERVER: 10.0.2.46#53(debian12.ittraining.loc) (UDP)
;; WHEN: Sun Dec 07 14:05:25 CET 2025
;; MSG SIZE  rcvd: 423
```

3.9 - La chaîne de confiance DNS

Créez le DSSet à partir de la clef publique KSK :

```
root@debian12:/etc/bind/zones# dnssec-dsfromkey -2 Kittraining.loc.+008+63515.key
ittraining.loc. IN DS 63515 8 2 909F3FC8A2B34083B1268C0FE7FDAA851252626CDCDF4D8B51D97CB98C62FDA4

root@debian12:/etc/bind/zones# ls -l | grep dsset
-rw-r--r-- 1 root bind    99 Dec  7 13:39 dsset-ittraining.loc.

root@debian12:/etc/bind/zones# cat dsset-ittraining.loc.
ittraining.loc.         IN DS 63515 8 2 909F3FC8A2B34083B1268C0FE7FDAA851252626CDCDF4D8B51D97CB9 8C62FDA4
```

Il conviendrait maintenant d'insérer un enregistrement DSSet dans le DNS du domaine parent, dans notre cas **.loc**. Cet enregistrement comportera l'ID de la clef, soit **63515**, ainsi que le hash **909F3FC8A2B34083B1268C0FE7FDAA851252626CDCDF4D8B51D97CB98C62FDA4**

Quand DNSSEC ne peut pas être validé, le résultat routorné par la commande dig est **SERVFAIL** :

```
root@debian12:/etc/bind/zones# dig www.dnssec-failed.org +dnssec

; <<>> DiG 9.18.41-1~deb12u1-Debian <<>> www.dnssec-failed.org +dnssec
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 42077
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags: do; udp: 1232
; COOKIE: 5321c94da922f6ca010000006935867f45a42de06e00bfa1 (good)
;; QUESTION SECTION:
;www.dnssec-failed.org.         IN      A

;; Query time: 140 msec
;; SERVER: 127.0.0.1#53(127.0.0.1) (UDP)
;; WHEN: Sun Dec 07 14:51:59 CET 2025
;; MSG SIZE  rcvd: 78
```

LAB #4 - Sécuriser Apache

Connectez-vous à votre VM **CentOS7_10.0.2.51_SSH**.

4.1 - 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.
```

4.2 - 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.
```

4.3 - 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:

```
10.0.2.51       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.
```

4.4 - 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** :

```
10.0.2.51            www.homeland.net
10.0.2.51            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
10.0.2.51 - - [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
```

4.5 - 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 ».

4.6 - 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 !

4.7 - 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
```

4.8 - 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>
```

Reconnectez-vous à votre VM **Debian12_10.0.2.46_SSH**.
