Version : **2022.01**

Dernière mise-à-jour : 2022/11/24 11:19

Topic 212: System Security

Contenu du Module

Netfilter et Firewalld

Le contre-mesure est principalement l'utilisation d'un pare-feu.

Le Pare-feu Netfilter/iptables

Netfilter est composé de 5 *hooks* :

- NF_IP_PRE_ROUTING
- NF_IP_LOCAL_IN
- NF_IP_LOCAL_OUT
- NF_IP_FORWARD
- NF_IP_POSTROUTING

Ces hooks sont utilisés par deux branches, la première est celle concernée par les paquets qui entrent vers des services locaux :

- NF_IP_PRE_ROUTING > NF_IP_LOCAL_IN > NF_IP_LOCAL_OUT > NF_IP_POSTROUTING

tandis que la deuxième concerne les paquets qui traversent la passerelle:

- NF_IP_PRE_ROUTING > NF_IP_FORWARD > NF_IP_POSTROUTING

Si IPTABLES a été compilé en tant que module, son utilisation nécessite le chargement de plusieurs modules supplémentaires en fonction de la situation:

- iptable_filter
- iptable_mangle
- iptable_net
- etc

Netfilter est organisé en **tables**. La commande **iptables** de netfilter permet d'insérer des **policies** dans les **chaines**:

- La table **FILTER**
  - La chaîne INPUT
    - Concerne les paquets entrants
      - Policies: ACCEPT, DROP, REJECT
  - La chaîne OUTPUT
    - Concerne les paquets sortants
      - Policies: ACCEPT, DROP, REJECT
  - La chaîne FORWARD
    - Concerne les paquets traversant le par-feu.
      - Policies: ACCEPT, DROP, REJECT

Si aucune table n'est précisée, c'est la table FILTER qui s'applique par défaut.

- La table **NAT**
  - La chaîne PREROUTING
    - Permet de faire la translation d'adresse de destination
      - Cibles: SNAT, DNAT, MASQUERADE
  - La chaîne POSTROUTING
    - Permet de faire la translation d'adresse de la source
      - Cibles: SNAT, DNAT, MASQUERADE
  - Le cas spécifique OUTPUT
    - Permet la modification de la destination des paquets générés localement

- La table **MANGLE**
  - Permet le marquage de paquets générés localement (OUTPUT) et entrants (PREROUTING)

Les **policies** sont:

- ACCEPT
  - Permet d'accepter le paquet concerné
- DROP
  - Permet de rejeter le paquet concerné sans générer un message d'erreur
- REJECT
  - Permet de rejeter le paquet concerné en générant une message d'erreur

Les **cibles** sont:

- SNAT
  - Permet de modifier l'adresse source du paquet concerné
- DNAT
  - Permet de modifier l'adresse de destination du paquet concerné
- MASQUERADE
  - Permet de remplacer l'adresse IP privée de l'expéditeur par un socket public de la passerelle.

IPTABLES peut être configuré soit par des outils tels shorewall, soit en utilisant des lignes de commandes ou un script. Dans ce dernier cas, la ligne prend la forme:

```
# IPTABLES --action CHAINE --option1 --option2
```

Les actions sont:

Action	Abréviation	Déscription
- -append	-A	Ajouter une règle à la fin de la chaîne spécifiée
- -delete	-D	Supprimer une règle en spécifiant son numéro ou la règle à supprimer
- -replace	-R	Permet de remplacer la règle spécifée par son numéro
- -insert	-I	Permet d'insérer une règle à l'endroit spécifié
- -list	-L	Permet d'afficher des règles

Action	Abréviation	Déscription
- -flush	-F	Permet de vider toutes les règles d'une chaîne

Les options sont:

Option	Abréviation	Déscription
- -protocol	-p	Permet de spécifier un protocol - tcp, udp, icmp, all
- -source	-s	Permet de spécifier une adresse source
- -destination	-d	Permet de spécifier une adresse de destination
- -in-interface	-i	Permet de spécifier une interface réseau d'entrée
- -out-interface	-o	Permet de spécifier une interface réseau de sortie
- -fragment	-f	Permet de ne spécifier que les paquets fragmentés
- -source-port	-sport	Permet de spécifier un port source ou une plage de ports source
- -destination-port	-dport	Permet de spécifier un port de destination ou une plage de ports de destination
- -tcp-flags	s/o	Permet de spécifier un flag TCP à matcher - SYN, ACK, FIN, RST, URG, PSH, ALL, NONE
- -icmp-type	s/o	Permet de spécifier un type de paquet ICMP
- -mac-source	s/o	Permet de spécifier une adresse MAC

Les options spécifiques à NET sont:

- -to-destination	s/o	Permet de spécifier l'adresse de destination d'une translation
- -to-source	s/o	Permet spécifier l'adresse source d'une translation

Les options spécifiques aux LOGS sont:

- -log-level	s/o	Permet de spécifier le niveau de logs
- -log-prefix	s/o	Permet de spécifier un préfix pour les logs

L'option spécifique au STATEFUL est:

- -state	s/o	Permet de spécifier l'état du paquet à vérifier

Ce dernier cas fait référence au STATEFUL. Le STATEFUL est la capacité du par-feu à enregistrer dans une table spécifique, l'état des différentes

connexions. Cette table s'appelle une **table d'état**. Le principe du fonctionnement de STATEFUL est simple, à savoir, si le paquet entrant appartient à une communication déjà établie, celui-ci n'est pas vérifié.

Il existe 4 états:

- NEW
  - Le paquet concerne une nouvelle connexion et contient donc un flag SYN à 1
- ESTABLISHED
  - Le paquet concerne une connexion déjà établie. Le paquet ne doit contenir **ni** flag SYN à 1, **ni** flag FIN à 1
- RELATED
  - Le paquet est d'une connexion qui présente une relation avec une autre connexion
- INVALID
  - La paquet provient d'une connexion anormale.

LAB #1 - Configuration par Scripts sous RHEL/CentOS 6 et versions Antérieures

Dans l'exemple suivant, expliquez le fonctionnement du script en détaillant les règles écrites :

```
#!/bin/bash
#####################################
# proxy server IP
PROXY_SERVER="192.168.1.2"
# Interface connected to Internet
INTERNET="eth1"
# Interface connected to LAN
LAN_IN="eth0"
# Local Interface
LOCAL="lo"
# Squid port
PROXY_PORT="8080"
# DO NOT MODIFY BELOW
# Clean old firewall
iptables -F
```

```
iptables -X
iptables -t nat -F
iptables -t nat -X
iptables -t mangle -F
iptables -t mangle -X
# Load IPTABLES modules for NAT and IP conntrack support
modprobe ip_conntrack
modprobe ip_conntrack_ftp
# For win xp ftp client
modprobe ip_nat_ftp
echo 1 > /proc/sys/net/ipv4/ip_forward
# Setting default filter policy
iptables -P INPUT DROP
iptables -P OUTPUT ACCEPT
# Unlimited access to loop back
iptables -A INPUT -i lo -j ACCEPT
iptables -A OUTPUT -o lo -j ACCEPT
# Allow UDP, DNS and Passive FTP
iptables -A INPUT -i $INTERNET -m state --state ESTABLISHED,RELATED -j ACCEPT
# set this system as a router for Rest of LAN
iptables --table nat --append POSTROUTING --out-interface $INTERNET -j MASQUERADE
iptables --append FORWARD --in-interface $LAN_IN -j ACCEPT
# unlimited access to LAN
iptables -A INPUT -i $LAN_IN -j ACCEPT
iptables -A OUTPUT -o $LAN_IN -j ACCEPT
# DNAT port 80 request comming from LAN systems to squid 3128 ($SQUID_PORT) aka transparent proxy
iptables -t nat -A PREROUTING -i $LAN_IN -p tcp --dport 80 -j DNAT --to $PROXY_SERVER:$PROXY_PORT
# iptables -t nat -A PREROUTING -i br0 -p tcp --dport 80 -j REDIRECT --to-port 3128
# if it is same system
iptables -t nat -A PREROUTING -i $INTERNET -p tcp --dport 80 -j REDIRECT --to-port $PROXY_PORT
# DROP everything and Log it
iptables -A INPUT -j LOG
iptables -A INPUT -j DROP
```

LAB #2 - La Configuration par firewalld sous RHEL/CentOS 7

firewalld est à Netfilter ce que NetworkManager est au réseau. firewalld utilise des **zones** - des jeux de règles pré-définis dans lesquels sont placés les interfaces :

- **trusted** - un réseau fiable. Dans ce cas tous les ports sont autorisés,
- **work**, **home**, **internal** - un réseau partiellement fiable. Dans ce cas quelques ports sont autorisés,
- **dmz**, **public**, **external** - un réseau non fiable. Dans ce cas peu de ports sont autorisés,
- **block**, **drop** - tout est interdit. La zone drop n'envoie pas de messages d'erreurs.

Important - Une interface ne peut être que dans une zone à la fois tandis que plusieurs interfaces peuvent être dans la même zone.

Le service firewalld doit toujours être lancé :

```
[root@centos7 ~]# systemctl status firewalld.service
firewalld.service - firewalld - dynamic firewall daemon
   Loaded: loaded (/usr/lib/systemd/system/firewalld.service; enabled)
   Active: active (running) since Tue 2015-07-07 15:53:56 CEST; 1 day 21h ago
 Main PID: 493 (firewalld)
   CGroup: /system.slice/firewalld.service
           └─493 /usr/bin/python -Es /usr/sbin/firewalld --nofork --nopid

Jul 07 15:53:56 centos7.fenestros.loc systemd[1]: Started firewalld - dynamic firewall daemon.
```

2.1 - La Configuration de Base de firewalld

La configuration par défaut de firewalld se trouve dans **/usr/lib/firewalld** :

```
[root@centos7 ~]# ls -l /usr/lib/firewalld/
total 12
drwxr-x---. 2 root root 4096 Jun  4 09:52 icmptypes
drwxr-x---. 2 root root 4096 Jun  4 09:52 services
drwxr-x---. 2 root root 4096 Jun  4 09:52 zones
[root@centos7 ~]# ls -l /usr/lib/firewalld/zones
total 36
-rw-r-----. 1 root root 299 Mar  6 00:35 block.xml
-rw-r-----. 1 root root 293 Mar  6 00:35 dmz.xml
-rw-r-----. 1 root root 291 Mar  6 00:35 drop.xml
-rw-r-----. 1 root root 304 Mar  6 00:35 external.xml
-rw-r-----. 1 root root 400 Mar  6 00:35 home.xml
-rw-r-----. 1 root root 415 Mar  6 00:35 internal.xml
-rw-r-----. 1 root root 315 Mar  6 00:35 public.xml
-rw-r-----. 1 root root 162 Mar  6 00:35 trusted.xml
-rw-r-----. 1 root root 342 Mar  6 00:35 work.xml
[root@centos7 ~]# ls -l /usr/lib/firewalld/services
total 192
-rw-r-----. 1 root root 412 Mar  6 00:35 amanda-client.xml
-rw-r-----. 1 root root 320 Mar  6 00:35 bacula-client.xml
-rw-r-----. 1 root root 346 Mar  6 00:35 bacula.xml
-rw-r-----. 1 root root 305 Mar  6 00:35 dhcpv6-client.xml
-rw-r-----. 1 root root 234 Mar  6 00:35 dhcpv6.xml
-rw-r-----. 1 root root 227 Mar  6 00:35 dhcp.xml
-rw-r-----. 1 root root 346 Mar  6 00:35 dns.xml
-rw-r-----. 1 root root 374 Mar  6 00:35 ftp.xml
-rw-r-----. 1 root root 476 Mar  6 00:35 high-availability.xml
-rw-r-----. 1 root root 448 Mar  6 00:35 https.xml
-rw-r-----. 1 root root 353 Mar  6 00:35 http.xml
-rw-r-----. 1 root root 372 Mar  6 00:35 imaps.xml
-rw-r-----. 1 root root 454 Mar  6 00:35 ipp-client.xml
-rw-r-----. 1 root root 427 Mar  6 00:35 ipp.xml
-rw-r-----. 1 root root 517 Mar  6 00:35 ipsec.xml
-rw-r-----. 1 root root 233 Mar  6 00:35 kerberos.xml
```

```
-rw-r-----. 1 root root 221 Mar  6 00:35 kpasswd.xml
-rw-r-----. 1 root root 232 Mar  6 00:35 ldaps.xml
-rw-r-----. 1 root root 199 Mar  6 00:35 ldap.xml
-rw-r-----. 1 root root 385 Mar  6 00:35 libvirt-tls.xml
-rw-r-----. 1 root root 389 Mar  6 00:35 libvirt.xml
-rw-r-----. 1 root root 424 Mar  6 00:35 mdns.xml
-rw-r-----. 1 root root 211 Mar  6 00:35 mountd.xml
-rw-r-----. 1 root root 190 Mar  6 00:35 ms-wbt.xml
-rw-r-----. 1 root root 171 Mar  6 00:35 mysql.xml
-rw-r-----. 1 root root 324 Mar  6 00:35 nfs.xml
-rw-r-----. 1 root root 389 Mar  6 00:35 ntp.xml
-rw-r-----. 1 root root 335 Mar  6 00:35 openvpn.xml
-rw-r-----. 1 root root 433 Mar  6 00:35 pmcd.xml
-rw-r-----. 1 root root 474 Mar  6 00:35 pmproxy.xml
-rw-r-----. 1 root root 544 Mar  6 00:35 pmwebapis.xml
-rw-r-----. 1 root root 460 Mar  6 00:35 pmwebapi.xml
-rw-r-----. 1 root root 357 Mar  6 00:35 pop3s.xml
-rw-r-----. 1 root root 181 Mar  6 00:35 postgresql.xml
-rw-r-----. 1 root root 261 Mar  6 00:35 proxy-dhcp.xml
-rw-r-----. 1 root root 446 Mar  6 00:35 radius.xml
-rw-r-----. 1 root root 517 Mar  6 00:35 RH-Satellite-6.xml
-rw-r-----. 1 root root 214 Mar  6 00:35 rpc-bind.xml
-rw-r-----. 1 root root 384 Mar  6 00:35 samba-client.xml
-rw-r-----. 1 root root 461 Mar  6 00:35 samba.xml
-rw-r-----. 1 root root 550 Mar  6 00:35 smtp.xml
-rw-r-----. 1 root root 463 Mar  6 00:35 ssh.xml
-rw-r-----. 1 root root 393 Mar  6 00:35 telnet.xml
-rw-r-----. 1 root root 301 Mar  6 00:35 tftp-client.xml
-rw-r-----. 1 root root 437 Mar  6 00:35 tftp.xml
-rw-r-----. 1 root root 211 Mar  6 00:35 transmission-client.xml
-rw-r-----. 1 root root 475 Mar  6 00:35 vnc-server.xml
-rw-r-----. 1 root root 310 Mar  6 00:35 wbem-https.xml
[root@centos7 ~]# ls -l /usr/lib/firewalld/icmptypes/
total 36
```

```
-rw-r-----. 1 root root 222 Mar  6 00:35 destination-unreachable.xml
-rw-r-----. 1 root root 173 Mar  6 00:35 echo-reply.xml
-rw-r-----. 1 root root 210 Mar  6 00:35 echo-request.xml
-rw-r-----. 1 root root 225 Mar  6 00:35 parameter-problem.xml
-rw-r-----. 1 root root 185 Mar  6 00:35 redirect.xml
-rw-r-----. 1 root root 227 Mar  6 00:35 router-advertisement.xml
-rw-r-----. 1 root root 223 Mar  6 00:35 router-solicitation.xml
-rw-r-----. 1 root root 248 Mar  6 00:35 source-quench.xml
-rw-r-----. 1 root root 253 Mar  6 00:35 time-exceeded.xml
```

Ces fichiers sont au format **xml**, par exemple :

```
[root@centos7 ~]# cat /usr/lib/firewalld/zones/home.xml
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Home</short>
  <description>For use in home areas. You mostly trust the other computers on networks to not harm your computer.
Only selected incoming connections are accepted.</description>
  <service name="ssh"/>
  <service name="ipp-client"/>
  <service name="mdns"/>
  <service name="samba-client"/>
  <service name="dhcpv6-client"/>
</zone>
```

La configuration de firewalld ainsi que les définitions et règles personnalisées se trouvent dans **/etc/firewalld** :

```
[root@centos7 ~]# ls -l /etc/firewalld/
total 8
-rw-r-----. 1 root root 1026 Mar  6 00:35 firewalld.conf
drwxr-x---. 2 root root    6 Mar  6 00:35 icmptypes
-rw-r-----. 1 root root  271 Mar  6 00:35 lockdown-whitelist.xml
drwxr-x---. 2 root root    6 Mar  6 00:35 services
drwxr-x---. 2 root root   23 Mar  6 00:35 zones
```

```
[root@centos7 ~]# ls -l /etc/firewalld/zones/
total 4
-rw-r--r--. 1 root root 315 Mar  8 14:05 public.xml
[root@centos7 ~]# ls -l /etc/firewalld/services/
total 0
[root@centos7 ~]# ls -l /etc/firewalld/icmptypes/
total 0
```

Le fichier de configuration de firewalld est **/etc/firewalld/firewalld.conf** :

```
[root@centos7 ~]# cat /etc/firewalld/firewalld.conf
# firewalld config file

# default zone
# The default zone used if an empty zone string is used.
# Default: public
DefaultZone=public

# Minimal mark
# Marks up to this minimum are free for use for example in the direct
# interface. If more free marks are needed, increase the minimum
# Default: 100
MinimalMark=100

# Clean up on exit
# If set to no or false the firewall configuration will not get cleaned up
# on exit or stop of firewalld
# Default: yes
CleanupOnExit=yes

# Lockdown
# If set to enabled, firewall changes with the D-Bus interface will be limited
# to applications that are listed in the lockdown whitelist.
# The lockdown whitelist file is lockdown-whitelist.xml
```

```
# Default: no
Lockdown=no

# IPv6_rpfilter
# Performs a reverse path filter test on a packet for IPv6. If a reply to the
# packet would be sent via the same interface that the packet arrived on, the
# packet will match and be accepted, otherwise dropped.
# The rp_filter for IPv4 is controlled using sysctl.
# Default: yes
IPv6_rpfilter=yes
```

2.2 - La Commande firewall-cmd

firewalld s'appuie sur netfilter. Pour cette raison, l'utilisation de firewall-cmd est incompatible avec l'utilisation des commandes iptables et system-config-firewall.

Important - firewall-cmd est le front-end de firewalld en ligne de commande. Il existe aussi la commande **firewall-config** qui lance un outi de configuration graphique.

Pour obtenir la liste de toutes les zones prédéfinies, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --get-zones
block dmz drop external home internal public trusted work
```

Pour obtenir la liste de toutes les services prédéfinis, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --get-services
RH-Satellite-6 amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns ftp high-availability http https
imaps ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt libvirt-tls mdns mountd ms-wbt mysql nfs ntp
```

```
openvpn pmcd pmproxy pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba samba-client smtp ssh
telnet tftp tftp-client transmission-client vnc-server wbem-https
```

Pour obtenir la liste de toutes les types ICMP prédéfinis, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --get-icmptypes
destination-unreachable echo-reply echo-request parameter-problem redirect router-advertisement router-
solicitation source-quench time-exceeded
```

Pour obtenir la liste des zones de la configuration courante, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --get-active-zones
public
  interfaces: eth0
```

Pour obtenir la liste des zones de la configuration courante pour une interface spécifique, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --get-zone-of-interface=eth0
public
```

Pour obtenir la liste des services autorisés pour la zone public, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=public --list-services
dhcpv6-client ssh
```

Pour obtenir toute la configuration pour la zone public, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=public --list-all
public (default, active)
  interfaces: eth0
  sources:
  services: dhcpv6-client ssh
  ports:
```

```
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

Pour obtenir la liste complète de toutes les zones et leurs configurations, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --list-all-zones
block
  interfaces:
  sources:
  services:
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
dmz
  interfaces:
  sources:
  services: ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
drop
  interfaces:
  sources:
  services:
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
```

```
  rich rules:
external
  interfaces:
  sources:
  services: ssh
  ports:
  masquerade: yes
  forward-ports:
  icmp-blocks:
  rich rules:
home
  interfaces:
  sources:
  services: dhcpv6-client ipp-client mdns samba-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
internal
  interfaces:
  sources:
  services: dhcpv6-client ipp-client mdns samba-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
public (default, active)
  interfaces: eth0
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
```

```
  forward-ports:
  icmp-blocks:
  rich rules:
trusted
  interfaces:
  sources:
  services:
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
work
  interfaces:
  sources:
  services: dhcpv6-client ipp-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

Pour changer la zone par défaut de public à work, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --set-default-zone=work
success
[root@centos7 ~]# firewall-cmd --get-active-zones
work
  interfaces: eth0
```

Pour ajouter l'interface ip_fixe à la zone work, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --add-interface=ip_fixe
success
```

```
[root@centos7 ~]# firewall-cmd --get-active-zones
work
  interfaces: eth0 ip_fixe
```

Pour supprimer l'interface ip_fixe à la zone work, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --remove-interface=ip_fixe
success
[root@centos7 ~]# firewall-cmd --get-active-zones
work
  interfaces: eth0
```

Pour ajouter le service **http** à la zone **work**, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --add-service=http
success
[root@centos7 ~]# firewall-cmd --zone=work --list-services
dhcpv6-client http ipp-client ssh
```

Pour supprimer le service **http** de la zone **work**, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --remove-service=http
success
[root@centos7 ~]# firewall-cmd --zone=work --list-services
dhcpv6-client ipp-client ssh
```

Pour ajouter un nouveau bloc ICMP, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --add-icmp-block=echo-reply
success
[root@centos7 ~]# firewall-cmd --zone=work --list-icmp-blocks
echo-reply
```

Pour supprimer un bloc ICMP, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --remove-icmp-block=echo-reply
success
[root@centos7 ~]# firewall-cmd --zone=work --list-icmp-blocks
[root@centos7 ~]#
```

Pour ajouter le port 591/tcp à la zone work, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --add-port=591/tcp
success
[root@centos7 ~]# firewall-cmd --zone=work --list-ports
591/tcp
```

Pour supprimer le port 591/tcp à la zone work, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --zone=work --remove-port=591/tcp
success
[root@centos7 ~]# firewall-cmd --zone=work --list-ports
[root@centos7 ~]#
```

Pour créer un nouveau service, il convient de :

- copier un fichier existant se trouvant dans le répertoire **/usr/lib/firewalld/services** vers **/etc/firewalld/services**,
- modifier le fichier,
- recharger la configuration de firewalld,
- vérifier que firewalld voit le nouveau service.

Par exemple :

```
[root@centos7 ~]# cp /usr/lib/firewalld/services/http.xml /etc/firewalld/services/filemaker.xml
[root@centos7 ~]#
[root@centos7 ~]# cat /etc/firewalld/services/filemaker.xml
<?xml version="1.0" encoding="utf-8"?>
```

```
<service>
  <short>FileMakerPro</short>
  <description>fichier de service firewalld pour FileMaker Pro</description>
  <port protocol="tcp" port="591"/>
</service>
[root@centos7 ~]#
[root@centos7 ~]# firewall-cmd --reload
success
[root@centos7 ~]#
[root@centos7 ~]# firewall-cmd --get-services
RH-Satellite-6 amanda-client bacula bacula-client dhcp dhcpv6 dhcpv6-client dns filemaker ftp high-availability
http https imaps ipp ipp-client ipsec kerberos kpasswd ldap ldaps libvirt libvirt-tls mdns mountd ms-wbt mysql
nfs ntp openvpn pmcd pmproxy pmwebapi pmwebapis pop3s postgresql proxy-dhcp radius rpc-bind samba samba-client
smtp ssh telnet tftp tftp-client transmission-client vnc-server wbem-https
```

2.3 - La Configuration Avancée de firewalld

La configuration de base de firewalld ne permet que la configuration des zones, services, blocs ICMP et les ports non-standard. Cependant firewalld peut également être configuré avec des **Rich Rules** ou ***Règles Riches***. Rich Rules ou Règles Riches évaluent des **critères** pour ensuite entreprendre une **action**.

Les **Critères** sont :

- **source address=“<adresse_IP>“**
- **destination address=”<adresse_IP>“**,
- **rule port port=”<numéro_du_port>“**,
- **service name=<nom_d'un_sevice_prédéfini>**.

Les **Actions** sont :

- **accept**,
- **reject**,
    - une Action reject peut être associée avec un message d'erreur spécifique par la clause **type=”<type_d'erreur>**,

- **drop**.

Saisissez la commande suivante pour ouvrir le port 80 :

```
[root@centos7 ~]# firewall-cmd --add-rich-rule='rule port port="80" protocol="tcp" accept'
success
```

Important - Notez que la Rich Rule doit être entourée de caractères '.

Saisissez la commande suivante pour visualiser la règle iptables pour IPv4 :

```
[root@centos7 ~]# iptables -L -n | grep 80
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80 ctstate NEW
```

Saisissez la commande suivante pour visualiser la règle iptables pour IPv6 :

```
[root@centos7 ~]# ip6tables -L -n | grep 80
ACCEPT     udp      ::/0                 fe80::/64           udp dpt:546 ctstate NEW
ACCEPT     tcp      ::/0                 ::/0                tcp dpt:80 ctstate NEW
```

Important - Notez que la Rich Rule a créé deux règles, une pour IPv4 et une deuxième pour IPv6. Une règle peut être créée pour IPv4 seul en incluant le Critère **family=ipv4**. De la même façon, une règle peut être créée pour IPv6 seul en incluant le Critère **family=ipv6**.

Cette nouvelle règle est écrite en mémoire mais non pas sur disque. Pour l'écrire sur disque dans le fichier zone se trouvant dans **/etc/firewalld**, il faut ajouter l'option **–permanent** :

```
[root@centos7 ~]# firewall-cmd --add-rich-rule='rule port port="80" protocol="tcp" accept' --permanent
success
[root@centos7 ~]#
[root@centos7 ~]# cat /etc/firewalld/zones/work.xml
<?xml version="1.0" encoding="utf-8"?>
<zone>
  <short>Work</short>
  <description>For use in work areas. You mostly trust the other computers on networks to not harm your computer.
Only selected incoming connections are accepted.</description>
  <service name="ipp-client"/>
  <service name="dhcpv6-client"/>
  <service name="ssh"/>
  <rule>
    <port protocol="tcp" port="80"/>
    <accept/>
  </rule>
</zone>
```

Important - Attention ! La règle ajoutée avec l'option –permanent n'est pas prise en compte imédiatement mais uniquement au prochain redémmarge. Pour qu'une règle soit appliquée immédiatement **et** être écrite sur disque, il faut saisir la commande deux fois dont une avec l'option –permanent et l'autre sans l'option –permanent.

Pour visualiser cette règle dans la configuration de firewalld, il convient de saisir la commande suivante :

```
[root@centos7 ~]# firewall-cmd --list-all-zones
...
work (default, active)
  interfaces: eth0
  sources:
```

```
  services: dhcpv6-client ipp-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
    rule port port="80" protocol="tcp" accept
```

Notez que la Rich Rule est créée dans la Zone par Défaut. Il est possible de créer une Rich Rule dans une autre zone en utilisant l'option **–zone=<zone>** de la commande firewall-cmd :

```
[root@centos7 ~]# firewall-cmd --zone=public --add-rich-rule='rule port port="80" protocol="tcp" accept'
success
[root@centos7 ~]# firewall-cmd --list-all-zones
...
public
  interfaces:
  sources:
  services: dhcpv6-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
    rule port port="80" protocol="tcp" accept
trusted
  interfaces:
  sources:
  services:
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
```

```
work (default, active)
  interfaces: eth0
  sources:
  services: dhcpv6-client ipp-client ssh
  ports:
  masquerade: no
  forward-ports:
  icmp-blocks:
  rich rules:
    rule port port="80" protocol="tcp" accept
```

Pour supprimer une Rich Rule, il faut copier la ligne entière la concernant qui se trouve dans la sortie de la commande **firewall-cmd –list-all-zones** :

```
[root@centos7 ~]# firewall-cmd --zone=public --remove-rich-rule='rule port port="80" protocol="tcp" accept'
success
```

2.4 - Le mode Panic de firewalld

Le mode Panic de firewalld permet de bloquer tout le trafic avec une seule commande. Pour connaître l'état du mode Panic, utilisez la commande suivante :

```
[root@centos7 ~]# firewall-cmd --query-panic
no
```

Pour activer le mode Panic, il convient de saisir la commande suivante :

```
[root@centos7 ~]# firewall-cmd --panic-on
success
[root@centos7 ~]# firewall-cmd --query-panic
yes
```

Pour désactiver le mode Panic, il convient de saisir la commande suivante :

```
[root@centos7 ~]# firewall-cmd --panic-off
success
[root@centos7 ~]# firewall-cmd --query-panic
no
```

LAB #3 - Utilisation de nmap et de netcat

3.1 - nmap

Installation

Sous RHEL/CentOS 7, **nmap** n'est pas installé par défaut :

```
[root@centos7 ~]# which nmap
/usr/bin/which: no nmap in (/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/root/bin)
```

Installez donc nmap en utilisant yum :

```
[root@centos7 ~]# yum install nmap
Loaded plugins: fastestmirror, langpacks
Repodata is over 2 weeks old. Install yum-cron? Or run: yum makecache fast
adobe-linux-x86_64                                       | 2.9 kB     00:00
base                                                     | 3.6 kB     00:00
extras                                                   | 3.4 kB     00:00
updates                                                  | 3.4 kB     00:00
(1/3): adobe-linux-x86_64/primary_db                       | 2.7 kB   00:00
(2/3): extras/7/x86_64/primary_db                          | 191 kB   00:00
(3/3): updates/7/x86_64/primary_db                         | 7.8 MB   00:04
Determining fastest mirrors
 * base: ftp.rezopole.net
```

```
 * extras: ftp.rezopole.net
 * updates: ftp.rezopole.net
Resolving Dependencies
--> Running transaction check
---> Package nmap.x86_64 2:6.40-7.el7 will be installed
--> Processing Dependency: nmap-ncat = 2:6.40-7.el7 for package: 2:nmap-6.40-7.el7.x86_64
--> Running transaction check
---> Package nmap-ncat.x86_64 2:6.40-7.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved

================================================================================
 Package            Arch            Version                 Repository     Size
================================================================================
Installing:
 nmap               x86_64          2:6.40-7.el7            base          4.0 M
Installing for dependencies:
 nmap-ncat          x86_64          2:6.40-7.el7            base          201 k

Transaction Summary
================================================================================
Install  1 Package (+1 Dependent package)

Total download size: 4.2 M
Installed size: 17 M
Is this ok [y/d/N]: y
```

Les options de cette commande sont :

```
[root@centos7 ~]# nmap --help
Nmap 6.40 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
```

```
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
```

```
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-args-file=filename: provide NSE script args in a file
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
  --script-help=<Lua scripts>: Show help about scripts.
           <Lua scripts> is a comma separted list of script-files or
           script-categories.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
```

```
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
```

```
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Utilisation

Pour connaître la liste des ports ouverts sur votre machine virtuelle, saisissez la commande suivante :

```
[root@centos7 ~]# nmap 127.0.0.1

Starting Nmap 6.40 ( http://nmap.org ) at 2017-08-05 14:17 CEST
Nmap scan report for localhost.localdomain (127.0.0.1)
Host is up (-2100s latency).
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
25/tcp  open  smtp
111/tcp open  rpcbind
631/tcp open  ipp

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

Important - Pour connaître les ports ouverts sur une machine distante, la procédure est identique sauf que vous devez utiliser l'adresse IP de votre cible.

Fichiers de Configuration

nmap utilise un fichier spécifique pour identifier les ports. Ce fichier est **/usr/share/nmap/nmap-services**:

```
[root@centos7 ~]# more /usr/share/nmap/nmap-services
# THIS FILE IS GENERATED AUTOMATICALLY FROM A MASTER - DO NOT EDIT.
# EDIT /nmap-private-dev/nmap-services-all IN SVN INSTEAD.
# Well known service port numbers -*- mode: fundamental; -*-
# From the Nmap Security Scanner ( http://nmap.org )
#
# $Id: nmap-services 31220 2013-07-03 04:30:43Z david $
#
# Derived from IANA data and our own research
#
# This collection of service data is (C) 1996-2011 by Insecure.Com
# LLC.  It is distributed under the Nmap Open Source license as
# provided in the COPYING file of the source distribution or at
# http://nmap.org/data/COPYING .  Note that this license
# requires you to license your own work under a compatable open source
# license.  If you wish to embed Nmap technology into proprietary
# software, we sell alternative licenses (contact sales@insecure.com).
# Dozens of software vendors already license Nmap technology such as
# host discovery, port scanning, OS detection, and version detection.
# For more details, see http://nmap.org/book/man-legal.html
#
# Fields in this file are: Service name, portnum/protocol, open-frequency, optional comments
#
tcpmux  1/tcp    0.001995    # TCP Port Service Multiplexer [rfc-1078]
tcpmux  1/udp    0.001236    # TCP Port Service Multiplexer
compressnet 2/tcp    0.000013    # Management Utility
compressnet 2/udp    0.001845    # Management Utility
compressnet 3/tcp    0.001242    # Compression Process
compressnet 3/udp    0.001532    # Compression Process
```

```
unknown 4/tcp    0.000477
rje 5/udp    0.000593    # Remote Job Entry
unknown 6/tcp    0.000502
echo    7/sctp    0.000000
echo    7/tcp    0.004855
echo    7/udp    0.024679
unknown 8/tcp    0.000013
--More--(0%)
```

Le répertoire **/usr/share/nmap** contient d'autres fichiers importants :

```
[root@centos7 ~]# ls -l /usr/share/nmap
total 6548
-rw-r--r--. 1 root root   10546 Nov 20  2015 nmap.dtd
-rw-r--r--. 1 root root  455371 Nov 20  2015 nmap-mac-prefixes
-rw-r--r--. 1 root root 3694559 Nov 20  2015 nmap-os-db
-rw-r--r--. 1 root root   11749 Nov 20  2015 nmap-payloads
-rw-r--r--. 1 root root    6631 Nov 20  2015 nmap-protocols
-rw-r--r--. 1 root root   49243 Nov 20  2015 nmap-rpc
-rw-r--r--. 1 root root 1727204 Nov 20  2015 nmap-service-probes
-rw-r--r--. 1 root root  622039 Nov 20  2015 nmap-services
-rw-r--r--. 1 root root   31935 Nov 20  2015 nmap.xsl
drwxr-xr-x. 3 root root    4096 Aug  5 14:16 nselib
-rw-r--r--. 1 root root   47190 Nov 20  2015 nse_main.lua
drwxr-xr-x. 2 root root   20480 Aug  5 14:16 scripts
```

Voici la liste des fichiers les plus importants :

Fichier	**Description**
/usr/share/nmap/nmap-protocols	Contient la liste des protocols reconnus par **nmap**.
/usr/share/nmap/nmap-service-probes	Contient les règles de balayage utilisées par **nmap** pour identifier le service actif sur un port donné.
/usr/share/nmap/nmap-mac-prefixes	Contient une liste de préfix d'adresses MAC par fabricant reconnu par **nmap**.
/usr/share/nmap/nmap-rpc	Contient une liste des services RPC reconnus par **nmap**.

Scripts

nmap utilise des scripts pour accomplir certaines tâches allant de la découverte simple de ports ouverts jusqu'à l'intrusion :

```
[root@centos7 ~]# ls /usr/share/nmap/scripts/
acarsd-info.nse                        http-domino-enum-passwords.nse          ndmp-version.nse
address-info.nse                       http-drupal-enum-users.nse              nessus-brute.nse
afp-brute.nse                          http-drupal-modules.nse                 nessus-xmlrpc-brute.nse
afp-ls.nse                             http-email-harvest.nse                  netbus-auth-bypass.nse
afp-path-vuln.nse                      http-enum.nse                           netbus-brute.nse
afp-serverinfo.nse                     http-exif-spider.nse                    netbus-info.nse
afp-showmount.nse                      http-favicon.nse                        netbus-version.nse
ajp-auth.nse                           http-fileupload-exploiter.nse           nexpose-brute.nse
ajp-brute.nse                          http-form-brute.nse                     nfs-ls.nse
ajp-headers.nse                        http-form-fuzzer.nse                    nfs-showmount.nse
ajp-methods.nse                        http-frontpage-login.nse                nfs-statfs.nse
ajp-request.nse                        http-generator.nse                      nping-brute.nse
amqp-info.nse                          http-git.nse                            nrpe-enum.nse
asn-query.nse                          http-gitweb-projects-enum.nse           ntp-info.nse
auth-owners.nse                        http-google-malware.nse                 ntp-monlist.nse
auth-spoof.nse                         http-grep.nse                           omp2-brute.nse
backorifice-brute.nse                  http-headers.nse                        omp2-enum-targets.nse
backorifice-info.nse                   http-huawei-hg5xx-vuln.nse              openlookup-info.nse
banner.nse                             http-icloud-findmyiphone.nse            openvas-otp-brute.nse
bitcoin-getaddr.nse                    http-icloud-sendmsg.nse                 oracle-brute.nse
bitcoin-info.nse                       http-iis-webdav-vuln.nse                oracle-brute-stealth.nse
bitcoinrpc-info.nse                    http-joomla-brute.nse                   oracle-enum-users.nse
bittorrent-discovery.nse               http-litespeed-sourcecode-download.nse  oracle-sid-brute.nse
bjnp-discover.nse                      http-majordomo2-dir-traversal.nse       ovs-agent-version.nse
broadcast-ataoe-discover.nse           http-malware-host.nse                   p2p-conficker.nse
broadcast-avahi-dos.nse                http-methods.nse                        path-mtu.nse
broadcast-bjnp-discover.nse            http-method-tamper.nse                  pcanywhere-brute.nse
broadcast-db2-discover.nse             http-open-proxy.nse                     pgsql-brute.nse
```

```
broadcast-dhcp6-discover.nse
broadcast-dhcp-discover.nse
broadcast-dns-service-discovery.nse
broadcast-dropbox-listener.nse
broadcast-eigrp-discovery.nse
broadcast-igmp-discovery.nse
broadcast-listener.nse
broadcast-ms-sql-discover.nse
broadcast-netbios-master-browser.nse
broadcast-networker-discover.nse
broadcast-novell-locate.nse
broadcast-pc-anywhere.nse
broadcast-pc-duo.nse
broadcast-pim-discovery.nse
broadcast-ping.nse
broadcast-pppoe-discover.nse
broadcast-rip-discover.nse
broadcast-ripng-discover.nse
broadcast-sybase-asa-discover.nse
broadcast-tellstick-discover.nse
broadcast-upnp-info.nse
broadcast-versant-locate.nse
broadcast-wake-on-lan.nse
broadcast-wpad-discover.nse
broadcast-wsdd-discover.nse
broadcast-xdmcp-discover.nse
cassandra-brute.nse
cassandra-info.nse
cccam-version.nse
citrix-brute-xml.nse
citrix-enum-apps.nse
citrix-enum-apps-xml.nse
citrix-enum-servers.nse
citrix-enum-servers-xml.nse
http-open-redirect.nse
http-passwd.nse
http-phpmyadmin-dir-traversal.nse
http-phpself-xss.nse
http-php-version.nse
http-proxy-brute.nse
http-put.nse
http-qnap-nas-info.nse
http-rfi-spider.nse
http-robots.txt.nse
http-robtex-reverse-ip.nse
http-robtex-shared-ns.nse
http-sitemap-generator.nse
http-slowloris-check.nse
http-slowloris.nse
http-sql-injection.nse
http-stored-xss.nse
http-title.nse
http-tplink-dir-traversal.nse
http-trace.nse
http-traceroute.nse
http-unsafe-output-escaping.nse
http-userdir-enum.nse
http-vhosts.nse
http-virustotal.nse
http-vlcstreamer-ls.nse
http-vmware-path-vuln.nse
http-vuln-cve2009-3960.nse
http-vuln-cve2010-0738.nse
http-vuln-cve2010-2861.nse
http-vuln-cve2011-3192.nse
http-vuln-cve2011-3368.nse
http-vuln-cve2012-1823.nse
http-vuln-cve2013-0156.nse
pjl-ready-message.nse
pop3-brute.nse
pop3-capabilities.nse
pptp-version.nse
qscan.nse
quake3-info.nse
quake3-master-getservers.nse
rdp-enum-encryption.nse
rdp-vuln-ms12-020.nse
realvnc-auth-bypass.nse
redis-brute.nse
redis-info.nse
resolveall.nse
reverse-index.nse
rexec-brute.nse
riak-http-info.nse
rlogin-brute.nse
rmi-dumpregistry.nse
rmi-vuln-classloader.nse
rpcap-brute.nse
rpcap-info.nse
rpc-grind.nse
rpcinfo.nse
rsync-brute.nse
rsync-list-modules.nse
rtsp-methods.nse
rtsp-url-brute.nse
samba-vuln-cve-2012-1182.nse
script.db
servicetags.nse
sip-brute.nse
sip-call-spoof.nse
sip-enum-users.nse
sip-methods.nse
```

```
couchdb-databases.nse
couchdb-stats.nse
creds-summary.nse
cups-info.nse
cups-queue-info.nse
cvs-brute.nse
cvs-brute-repository.nse
daap-get-library.nse
daytime.nse
db2-das-info.nse
db2-discover.nse
dhcp-discover.nse
dict-info.nse
distcc-cve2004-2687.nse
dns-blacklist.nse
dns-brute.nse
dns-cache-snoop.nse
dns-check-zone.nse
dns-client-subnet-scan.nse
dns-fuzz.nse
dns-ip6-arpa-scan.nse
dns-nsec3-enum.nse
dns-nsec-enum.nse
dns-nsid.nse
dns-random-srcport.nse
dns-random-txid.nse
dns-recursion.nse
dns-service-discovery.nse
dns-srv-enum.nse
dns-update.nse
dns-zeustracker.nse
dns-zone-transfer.nse
domcon-brute.nse
domcon-cmd.nse
http-waf-detect.nse
http-waf-fingerprint.nse
http-wordpress-brute.nse
http-wordpress-enum.nse
http-wordpress-plugins.nse
iax2-brute.nse
iax2-version.nse
icap-info.nse
ike-version.nse
imap-brute.nse
imap-capabilities.nse
informix-brute.nse
informix-query.nse
informix-tables.nse
ip-forwarding.nse
ip-geolocation-geobytes.nse
ip-geolocation-geoplugin.nse
ip-geolocation-ipinfodb.nse
ip-geolocation-maxmind.nse
ipidseq.nse
ipv6-node-info.nse
ipv6-ra-flood.nse
irc-botnet-channels.nse
irc-brute.nse
irc-info.nse
irc-sasl-brute.nse
irc-unrealircd-backdoor.nse
iscsi-brute.nse
iscsi-info.nse
isns-info.nse
jdwp-exec.nse
jdwp-info.nse
jdwp-inject.nse
jdwp-version.nse
skypev2-version.nse
smb-brute.nse
smb-check-vulns.nse
smb-enum-domains.nse
smb-enum-groups.nse
smb-enum-processes.nse
smb-enum-sessions.nse
smb-enum-shares.nse
smb-enum-users.nse
smb-flood.nse
smb-ls.nse
smb-mbenum.nse
smb-os-discovery.nse
smb-print-text.nse
smb-psexec.nse
smb-security-mode.nse
smb-server-stats.nse
smb-system-info.nse
smbv2-enabled.nse
smb-vuln-ms10-054.nse
smb-vuln-ms10-061.nse
smtp-brute.nse
smtp-commands.nse
smtp-enum-users.nse
smtp-open-relay.nse
smtp-strangeport.nse
smtp-vuln-cve2010-4344.nse
smtp-vuln-cve2011-1720.nse
smtp-vuln-cve2011-1764.nse
sniffer-detect.nse
snmp-brute.nse
snmp-hh3c-logins.nse
snmp-interfaces.nse
snmp-ios-config.nse
```

```
domino-enum-users.nse                krb5-enum-users.nse                  snmp-netstat.nse
dpap-brute.nse                       ldap-brute.nse                       snmp-processes.nse
drda-brute.nse                       ldap-novell-getpass.nse              snmp-sysdescr.nse
drda-info.nse                        ldap-rootdse.nse                     snmp-win32-services.nse
duplicates.nse                       ldap-search.nse                      snmp-win32-shares.nse
eap-info.nse                         lexmark-config.nse                   snmp-win32-software.nse
epmd-info.nse                        llmnr-resolve.nse                    snmp-win32-users.nse
eppc-enum-processes.nse              lltd-discovery.nse                   socks-auth-info.nse
finger.nse                           maxdb-info.nse                       socks-brute.nse
firewalk.nse                         mcafee-epo-agent.nse                 socks-open-proxy.nse
firewall-bypass.nse                  membase-brute.nse                    ssh2-enum-algos.nse
flume-master-info.nse                membase-http-info.nse                ssh-hostkey.nse
ftp-anon.nse                         memcached-info.nse                   sshv1.nse
ftp-bounce.nse                       metasploit-info.nse                  ssl-cert.nse
ftp-brute.nse                        metasploit-msgrpc-brute.nse          ssl-date.nse
ftp-libopie.nse                      metasploit-xmlrpc-brute.nse          ssl-enum-ciphers.nse
ftp-proftpd-backdoor.nse             mmouse-brute.nse                     ssl-google-cert-catalog.nse
ftp-vsftpd-backdoor.nse              mmouse-exec.nse                      ssl-known-key.nse
ftp-vuln-cve2010-4221.nse            modbus-discover.nse                  sslv2.nse
ganglia-info.nse                     mongodb-brute.nse                    stun-info.nse
giop-info.nse                        mongodb-databases.nse                stun-version.nse
gkrellm-info.nse                     mongodb-info.nse                     stuxnet-detect.nse
gopher-ls.nse                        mrinfo.nse                           svn-brute.nse
gpsd-info.nse                        msrpc-enum.nse                       targets-asn.nse
hadoop-datanode-info.nse             ms-sql-brute.nse                     targets-ipv6-multicast-echo.nse
hadoop-jobtracker-info.nse           ms-sql-config.nse                    targets-ipv6-multicast-invalid-
dst.nse
hadoop-namenode-info.nse             ms-sql-dac.nse                       targets-ipv6-multicast-mld.nse
hadoop-secondary-namenode-info.nse   ms-sql-dump-hashes.nse               targets-ipv6-multicast-slaac.nse
hadoop-tasktracker-info.nse          ms-sql-empty-password.nse            targets-sniffer.nse
hbase-master-info.nse                ms-sql-hasdbaccess.nse               targets-traceroute.nse
hbase-region-info.nse                ms-sql-info.nse                      teamspeak2-version.nse
hddtemp-info.nse                     ms-sql-query.nse                     telnet-brute.nse
hostmap-bfk.nse                      ms-sql-tables.nse                    telnet-encryption.nse
```

```
hostmap-ip2hosts.nse                ms-sql-xp-cmdshell.nse          tftp-enum.nse
hostmap-robtex.nse                  mtrace.nse                      tls-nextprotoneg.nse
http-adobe-coldfusion-apsa1301.nse  murmur-version.nse              traceroute-geolocation.nse
http-affiliate-id.nse               mysql-audit.nse                 unusual-port.nse
http-apache-negotiation.nse         mysql-brute.nse                 upnp-info.nse
http-auth-finder.nse                mysql-databases.nse             url-snarf.nse
http-auth.nse                       mysql-dump-hashes.nse           ventrilo-info.nse
http-awstatstotals-exec.nse         mysql-empty-password.nse        versant-info.nse
http-axis2-dir-traversal.nse        mysql-enum.nse                  vmauthd-brute.nse
http-backup-finder.nse              mysql-info.nse                  vnc-brute.nse
http-barracuda-dir-traversal.nse    mysql-query.nse                 vnc-info.nse
http-brute.nse                      mysql-users.nse                 voldemort-info.nse
http-cakephp-version.nse            mysql-variables.nse             vuze-dht-info.nse
http-chrono.nse                     mysql-vuln-cve2012-2122.nse     wdb-version.nse
http-coldfusion-subzero.nse         nat-pmp-info.nse                whois.nse
http-comments-displayer.nse         nat-pmp-mapport.nse             wsdd-discover.nse
http-config-backup.nse              nbstat.nse                      x11-access.nse
http-cors.nse                       ncp-enum-users.nse              xdmcp-discover.nse
http-date.nse                       ncp-serverinfo.nse              xmpp-brute.nse
http-default-accounts.nse           ndmp-fs-info.nse                xmpp-info.nse
```

Les scripts sont regroupés dans des catégories : **auth**, **broadcast**, **brute**, **default**, **discovery**, **dos**, **exploit**, **external**, **fuzzer**, **intrusive**, **malware**, **safe**, **version** and **vuln**.

Important - Pour plus d'informations concernant ces catégories, consultez cette page.

La catégorie la plus utilisée est **default** qui est appelée par l'utilisation de l'option **-sC**. Cette catégorie contient une liste de scripts par défaut.

```
[root@centos7 ~]# nmap -v -sC localhost
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2017-08-05 14:20 CEST
NSE: Loaded 95 scripts for scanning.
NSE: Script Pre-scanning.
Initiating SYN Stealth Scan at 14:20
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 22/tcp on 127.0.0.1
adjust_timeouts2: packet supposedly had rtt of -1500757317045342 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -1500757317045342 microseconds.  Ignoring time.
Discovered open port 25/tcp on 127.0.0.1
adjust_timeouts2: packet supposedly had rtt of -1500757317045486 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -1500757317045486 microseconds.  Ignoring time.
Discovered open port 111/tcp on 127.0.0.1
adjust_timeouts2: packet supposedly had rtt of -1500757317045504 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -1500757317045504 microseconds.  Ignoring time.
Discovered open port 631/tcp on 127.0.0.1
adjust_timeouts2: packet supposedly had rtt of -1500757274107480 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -1500757274107480 microseconds.  Ignoring time.
Completed SYN Stealth Scan at 14:20, 0.01s elapsed (1000 total ports)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 14:20
Completed NSE at 14:20, 0.28s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.0000060s latency).
rDNS record for 127.0.0.1: localhost.localdomain
Not shown: 996 closed ports
PORT    STATE SERVICE
22/tcp  open  ssh
| ssh-hostkey: 2048 17:21:e0:43:b1:66:22:22:b6:f8:2b:cc:08:68:38:59 (RSA)
|_256 19:cd:05:58:af:2c:10:82:52:ba:e3:31:df:bd:72:54 (ECDSA)
25/tcp  open  smtp
|_smtp-commands: centos7.fenestros.loc, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BITMIME,
DSN,
111/tcp open  rpcbind
| rpcinfo:
```

```
|   program version   port/proto  service
|   100000  2,3,4        111/tcp  rpcbind
|_  100000  2,3,4        111/udp  rpcbind
631/tcp open  ipp
| http-methods: GET HEAD OPTIONS POST PUT
| Potentially risky methods: PUT
|_See http://nmap.org/nsedoc/scripts/http-methods.html
| http-robots.txt: 1 disallowed entry
|_/
|_http-title: Home - CUPS 1.6.3

NSE: Script Post-scanning.
Initiating NSE at 14:20
Completed NSE at 14:20, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
           Raw packets sent: 1000 (44.000KB) | Rcvd: 2004 (84.176KB)
```

Attention - La catégorie par défaut **default** contient certains scripts de la catégorie **intrusive**. Vous ne devez donc jamais utiliser cette option sur un réseau sans avoir obtenu un accord au préalable.

3.2 - netcat

netcat est un couteau suisse. Il permet non seulement de scanner des ports mais aussi de lancer la connexion lors de la découverte d'un port ouvert.

Les options de cette commande sont :

```
[root@centos7 ~]# nc --help
Ncat 6.40 ( http://nmap.org/ncat )
```

```
Usage: ncat [options] [hostname] [port]

Options taking a time assume seconds. Append 'ms' for milliseconds,
's' for seconds, 'm' for minutes, or 'h' for hours (e.g. 500ms).
  -4                         Use IPv4 only
  -6                         Use IPv6 only
  -U, --unixsock             Use Unix domain sockets only
  -C, --crlf                 Use CRLF for EOL sequence
  -c, --sh-exec <command>    Executes the given command via /bin/sh
  -e, --exec <command>       Executes the given command
      --lua-exec <filename>  Executes the given Lua script
  -g hop1[,hop2,...]         Loose source routing hop points (8 max)
  -G <n>                     Loose source routing hop pointer (4, 8, 12, ...)
  -m, --max-conns <n>        Maximum <n> simultaneous connections
  -h, --help                 Display this help screen
  -d, --delay <time>         Wait between read/writes
  -o, --output <filename>    Dump session data to a file
  -x, --hex-dump <filename>  Dump session data as hex to a file
  -i, --idle-timeout <time>  Idle read/write timeout
  -p, --source-port port     Specify source port to use
  -s, --source addr          Specify source address to use (doesn't affect -l)
  -l, --listen               Bind and listen for incoming connections
  -k, --keep-open            Accept multiple connections in listen mode
  -n, --nodns                Do not resolve hostnames via DNS
  -t, --telnet               Answer Telnet negotiations
  -u, --udp                  Use UDP instead of default TCP
      --sctp                 Use SCTP instead of default TCP
  -v, --verbose              Set verbosity level (can be used several times)
  -w, --wait <time>          Connect timeout
      --append-output        Append rather than clobber specified output files
      --send-only            Only send data, ignoring received; quit on EOF
      --recv-only            Only receive data, never send anything
      --allow                Allow only given hosts to connect to Ncat
      --allowfile            A file of hosts allowed to connect to Ncat
```

```
      --deny                  Deny given hosts from connecting to Ncat
      --denyfile              A file of hosts denied from connecting to Ncat
      --broker                Enable Ncat's connection brokering mode
      --chat                  Start a simple Ncat chat server
      --proxy <addr[:port]>   Specify address of host to proxy through
      --proxy-type <type>     Specify proxy type ("http" or "socks4")
      --proxy-auth <auth>     Authenticate with HTTP or SOCKS proxy server
      --ssl                   Connect or listen with SSL
      --ssl-cert              Specify SSL certificate file (PEM) for listening
      --ssl-key               Specify SSL private key (PEM) for listening
      --ssl-verify            Verify trust and domain name of certificates
      --ssl-trustfile         PEM file containing trusted SSL certificates
      --version               Display Ncat's version information and exit

See the ncat(1) manpage for full options, descriptions and usage examples
```

Utilisation

Dans l'exemple qui suite, un scan est lancé sur le port 80 puis sur le port 25 :

```
[root@centos7 ~]# nc 127.0.0.1 80 -w 1 -vv
Ncat: Version 6.40 ( http://nmap.org/ncat )
libnsock nsi_new2(): nsi_new (IOD #1)
libnsock nsock_connect_tcp(): TCP connection requested to 127.0.0.1:80 (IOD #1) EID 8
libnsock nsock_trace_handler_callback(): Callback: CONNECT ERROR [Connection refused (111)] for EID 8
[127.0.0.1:80]
Ncat: Connection refused.

[root@centos7 ~]# nc 127.0.0.1 25 -w 1 -vv
Ncat: Version 6.40 ( http://nmap.org/ncat )
libnsock nsi_new2(): nsi_new (IOD #1)
libnsock nsock_connect_tcp(): TCP connection requested to 127.0.0.1:25 (IOD #1) EID 8
libnsock nsock_trace_handler_callback(): Callback: CONNECT SUCCESS for EID 8 [127.0.0.1:25]
```

```
Ncat: Connected to 127.0.0.1:25.
libnsock nsi_new2(): nsi_new (IOD #2)
libnsock nsock_read(): Read request from IOD #1 [127.0.0.1:25] (timeout: -1ms) EID 18
libnsock nsock_readbytes(): Read request for 0 bytes from IOD #2 [peer unspecified] EID 26
libnsock nsock_trace_handler_callback(): Callback: READ SUCCESS for EID 18 [127.0.0.1:25] (41 bytes): 220
centos7.fenestros.loc ESMTP Postfix..
220 centos7.fenestros.loc ESMTP Postfix
libnsock nsock_readbytes(): Read request for 0 bytes from IOD #1 [127.0.0.1:25] EID 34
^C
```

Important - Notez que **netcat** se connecte au port 25 qui est ouvert.

LAB #4 - Mise en place du Système de Prévention d'Intrusion Fail2Ban

Fail2Ban est un **S**ystème de **P**révention d'**I**ntrusion. Fail2Ban lit les logs de divers services (SSH, Apache, FTP...) à la recherche d'erreurs d'authentification répétées et ajoute une règle à iptables pour bannir l'adresse IP de la source.

4.1 - Installation

Sous RHEL/CentOS 7, beaucoup d'outils de sécurité ne se trouvent pas dans leurs versions les plus récentes dans les dépôts de base. Installez donc le dépôt Fedora **epel** :

```
[root@centos7 ~]# yum -y install epel-release
```

Ensuite installez Fail2Ban :

```
[root@centos6 ~]# yum install fail2ban
```

4.2 - Configuration

La configuration de Fail2Ban se trouve dans le fichier **/etc/fail2ban/jail.conf** :

```
[root@centos7 ~]# more /etc/fail2ban/jail.conf
#
# WARNING: heavily refactored in 0.9.0 release.  Please review and
#          customize settings for your setup.
#
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in jail.local file,
#           or separate .conf files under jail.d/ directory, e.g.:
#
# HOW TO ACTIVATE JAILS:
#
# YOU SHOULD NOT MODIFY THIS FILE.
#
# It will probably be overwritten or improved in a distribution update.
#
# Provide customizations in a jail.local file or a jail.d/customisation.local.
# For example to change the default bantime for all jails and to enable the
# ssh-iptables jail the following (uncommented) would appear in the .local file.
# See man 5 jail.conf for details.
#
# [DEFAULT]
# bantime = 3600
#
# [sshd]
# enabled = true
#
# See jail.conf(5) man page for more information
```

```
# Comments: use '#' for comment lines and ';' (following a space) for inline comments


[INCLUDES]

#before = paths-distro.conf
--More--(4%)
```

Dans ce fichier se trouvent des sections pour configurer l'action de Fail2Ban pour chaque service :

```
...
[sshd]

port    = ssh
logpath = %(sshd_log)s
...
```

Ces sections, appelées des Prisons (*Jails* en anglais), peuvent contenir des directives telles que :

Directive	**Description**
enabled	Indique si oui (true) ou non (false) le prison est activé.
port	Le port à bloquer dans iptables.
filter	Le nom du filtre, une expression régulière, associé au prison et utilisé pour trouver une activité suspect. Le nom dans ce champs, sans l'extention .conf, fait référence à un fichier dans le répertoire **/etc/fail2ban/filter.d/**. Par exemple la valeur **sshd** fait reférence au fichier **/etc/fail2ban/filter.d/sshd.conf**.
logpath	Le nom et le chemin du journal à examiner.
maxretry	Le nombre maximal de tentatives.
action	Spécifie l'action à entreprendre lors d'une corréspondance du **filter**. Le nom dans ce champs, sans l'extention .conf, fait référence à un fichier dans le répertoire **/etc/fail2ban/action.d/**. Par exemple la valeur **iptables** fait reférence au fichier **/etc/fail2ban/action.d/iptables.conf**.

Il n'est pas recommendé de modifier ce fichier afin de ne pas voir ses modifications ecrasées lors de la prochaine mise-à-jour de Fail2Ban. Fail2Ban nous donne la possibilité de créer le fichier **/etc/fail2ban/jail.local** pour contenir nos modifications. Créez donc ce fichier avec le contenu ci-dessous :

```
[root@centos7 ~]# vi /etc/fail2ban/jail.local
[root@centos7 ~]# cat /etc/fail2ban/jail.local
[DEFAULT]
ignoreip = 127.0.0.1 172.YY+20.0.3
findtime = 3600
bantime = 86400
maxretry = 5

[sshd]
enabled = true
```

Il est à noter que les directives dans le fichier **jail.conf** sont surchargées par celles dans les fichiers suivantes et dans l'ordre suivant :

- **/etc/fail2ban/jail.d/*.conf** dans l'ordre alphabétique,
- **/etc/fail2ban/jail.local**,
- **/etc/fail2ban/jail.d/*.local** dans l'ordre alphabétique.

Important - Notez que la définition des variables dans la section **[DEFAULT]** du fichier **/etc/fail2ban/jail.local** s'appliquent à toutes les sections de prisons actives dans les fichiers **/etc/fail2ban/jail.local** et **/etc/fail2ban/jail.conf** sauf si dans la section du prison elle-même, la variable est redéfinie.

Dans ce fichier, les directives sont donc :

Directive	Description
ignoreip	Liste des adresses IP, séparées par un **espace**, qui ne sont pas concernées par l'action de Fail2Ban ou une liste d'adresses de réseaux, exprimées au format CIDR.
findtime	L'intervale de temps en secondes, avant l'heure actuelle, pendant laquelle des authentifications infructueueses sont prises en compte pour le calcul de banir l'adresse IP ou non.
bantime	La durée de vie des règles, en secondes, inscrites dans le pare-feu iptables.

Directive	Description
maxretry	Le nombre maximal de tentatives. La règle sera donc inscrite dans le pare-feu lors de la sixième tentative.

4.3 - Le répertoire /etc/fail2ban

Le répertoire **/etc/fail2ban/** contient des fichiers et répertoires importants pour le fonctionnement de Fail2Ban :

```
[root@centos7 ~]# ls -l /etc/fail2ban/
total 68
drwxr-xr-x. 2 root root  4096 Jun  8 22:51 action.d
-rw-r--r--. 1 root root  2328 May 11  2017 fail2ban.conf
drwxr-xr-x. 2 root root     6 Jul 13  2017 fail2ban.d
drwxr-xr-x. 3 root root  4096 Jun  8 22:51 filter.d
-rw-r--r--. 1 root root 21502 Jul 13  2017 jail.conf
drwxr-xr-x. 2 root root    30 Jun  8 22:51 jail.d
-rw-r--r--. 1 root root   110 Jun  8 22:54 jail.local
-rw-r--r--. 1 root root  2375 May 11  2017 paths-common.conf
-rw-r--r--. 1 root root   642 May 11  2017 paths-debian.conf
-rw-r--r--. 1 root root  1070 May 11  2017 paths-fedora.conf
-rw-r--r--. 1 root root  1156 May 11  2017 paths-freebsd.conf
-rw-r--r--. 1 root root   975 May 11  2017 paths-opensuse.conf
-rw-r--r--. 1 root root   290 May 11  2017 paths-osx.conf
```

Le fichier fail2ban.conf

Ce fichier définit les configurations globales de Fail2Ban, telles le **pidfile**, le **socket** et le niveau syslog de journalisation :

```
[root@centos7 ~]# cat /etc/fail2ban/fail2ban.conf
# Fail2Ban main configuration file
#
# Comments: use '#' for comment lines and ';' (following a space) for inline comments
#
```

```
# Changes:  in most of the cases you should not modify this
#           file, but provide customizations in fail2ban.local file, e.g.:
#
# [Definition]
# loglevel = DEBUG
#

[Definition]

# Option: loglevel
# Notes.: Set the log level output.
#         CRITICAL
#         ERROR
#         WARNING
#         NOTICE
#         INFO
#         DEBUG
# Values: [ LEVEL ]  Default: ERROR
#
loglevel = INFO

# Option: logtarget
# Notes.: Set the log target. This could be a file, SYSLOG, STDERR or STDOUT.
#         Only one log target can be specified.
#         If you change logtarget from the default value and you are
#         using logrotate -- also adjust or disable rotation in the
#         corresponding configuration file
#         (e.g. /etc/logrotate.d/fail2ban on Debian systems)
# Values: [ STDOUT | STDERR | SYSLOG | FILE ]  Default: STDERR
#
logtarget = /var/log/fail2ban.log

# Option: syslogsocket
# Notes: Set the syslog socket file. Only used when logtarget is SYSLOG
```

```
#        auto uses platform.system() to determine predefined paths
# Values: [ auto | FILE ]  Default: auto
syslogsocket = auto

# Option: socket
# Notes.: Set the socket file. This is used to communicate with the daemon. Do
#         not remove this file when Fail2ban runs. It will not be possible to
#         communicate with the server afterwards.
# Values: [ FILE ]  Default: /var/run/fail2ban/fail2ban.sock
#
socket = /var/run/fail2ban/fail2ban.sock

# Option: pidfile
# Notes.: Set the PID file. This is used to store the process ID of the
#         fail2ban server.
# Values: [ FILE ]  Default: /var/run/fail2ban/fail2ban.pid
#
pidfile = /var/run/fail2ban/fail2ban.pid

# Options: dbfile
# Notes.: Set the file for the fail2ban persistent data to be stored.
#         A value of ":memory:" means database is only stored in memory
#         and data is lost when fail2ban is stopped.
#         A value of "None" disables the database.
# Values: [ None :memory: FILE ] Default: /var/lib/fail2ban/fail2ban.sqlite3
dbfile = /var/lib/fail2ban/fail2ban.sqlite3

# Options: dbpurgeage
# Notes.: Sets age at which bans should be purged from the database
# Values: [ SECONDS ] Default: 86400 (24hours)
dbpurgeage = 86400
```

Le répertoire /etc/fail2ban/filter.d/

Ce répertoire contient les fichiers appelés par les directives **filter** dans les sections des prisons :

```
[root@centos7 ~]# ls -l /etc/fail2ban/filter.d/
total 344
-rw-r--r--. 1 root root  442 May 11  2017 3proxy.conf
-rw-r--r--. 1 root root 3241 May 11  2017 apache-auth.conf
-rw-r--r--. 1 root root 2745 May 11  2017 apache-badbots.conf
-rw-r--r--. 1 root root 1273 May 11  2017 apache-botsearch.conf
-rw-r--r--. 1 root root  813 May 11  2017 apache-common.conf
-rw-r--r--. 1 root root  268 May 11  2017 apache-fakegooglebot.conf
-rw-r--r--. 1 root root  487 May 11  2017 apache-modsecurity.conf
-rw-r--r--. 1 root root  596 May 11  2017 apache-nohome.conf
-rw-r--r--. 1 root root 1187 May 11  2017 apache-noscript.conf
-rw-r--r--. 1 root root 2000 May 11  2017 apache-overflows.conf
-rw-r--r--. 1 root root  346 May 11  2017 apache-pass.conf
-rw-r--r--. 1 root root 1014 May 11  2017 apache-shellshock.conf
-rw-r--r--. 1 root root 3418 May 11  2017 assp.conf
-rw-r--r--. 1 root root 2443 May 11  2017 asterisk.conf
-rw-r--r--. 1 root root  520 May 11  2017 botsearch-common.conf
-rw-r--r--. 1 root root 1863 May 11  2017 common.conf
-rw-r--r--. 1 root root  252 May 11  2017 counter-strike.conf
-rw-r--r--. 1 root root  393 May 11  2017 courier-auth.conf
-rw-r--r--. 1 root root  490 May 11  2017 courier-smtp.conf
-rw-r--r--. 1 root root  444 May 11  2017 cyrus-imap.conf
-rw-r--r--. 1 root root  345 May 11  2017 directadmin.conf
-rw-r--r--. 1 root root 1942 May 11  2017 domino-smtp.conf
-rw-r--r--. 1 root root 1875 May 11  2017 dovecot.conf
-rw-r--r--. 1 root root 1696 May 11  2017 dropbear.conf
-rw-r--r--. 1 root root  557 May 11  2017 drupal-auth.conf
-rw-r--r--. 1 root root 1282 May 11  2017 ejabberd-auth.conf
-rw-r--r--. 1 root root  516 May 11  2017 exim-common.conf
```

```
-rw-r--r--. 1 root root 1847 May 11  2017 exim.conf
-rw-r--r--. 1 root root 2158 May 11  2017 exim-spam.conf
-rw-r--r--. 1 root root  963 May 11  2017 freeswitch.conf
-rw-r--r--. 1 root root 1209 May 11  2017 froxlor-auth.conf
-rw-r--r--. 1 root root  236 May 11  2017 groupoffice.conf
-rw-r--r--. 1 root root  322 May 11  2017 gssftpd.conf
-rw-r--r--. 1 root root  512 May 11  2017 guacamole.conf
-rw-r--r--. 1 root root 1158 May 11  2017 haproxy-http-auth.conf
-rw-r--r--. 1 root root  404 May 11  2017 horde.conf
drwxr-xr-x. 2 root root   33 Jun  8 22:51 ignorecommands
-rw-r--r--. 1 root root  482 May 11  2017 kerio.conf
-rw-r--r--. 1 root root  323 May 11  2017 lighttpd-auth.conf
-rw-r--r--. 1 root root 2279 May 11  2017 mongodb-auth.conf
-rw-r--r--. 1 root root  773 May 11  2017 monit.conf
-rw-r--r--. 1 root root  652 May 11  2017 murmur.conf
-rw-r--r--. 1 root root  890 May 11  2017 mysqld-auth.conf
-rw-r--r--. 1 root root  400 May 11  2017 nagios.conf
-rw-r--r--. 1 root root 1594 May 11  2017 named-refused.conf
-rw-r--r--. 1 root root  528 May 11  2017 nginx-botsearch.conf
-rw-r--r--. 1 root root  442 May 11  2017 nginx-http-auth.conf
-rw-r--r--. 1 root root 1427 May 11  2017 nginx-limit-req.conf
-rw-r--r--. 1 root root  707 May 11  2017 nsd.conf
-rw-r--r--. 1 root root  459 May 11  2017 openhab.conf
-rw-r--r--. 1 root root  495 May 11  2017 openwebmail.conf
-rw-r--r--. 1 root root 1905 May 11  2017 oracleims.conf
-rw-r--r--. 1 root root  814 May 11  2017 pam-generic.conf
-rw-r--r--. 1 root root  568 May 11  2017 perdition.conf
-rw-r--r--. 1 root root  834 May 11  2017 php-url-fopen.conf
-rw-r--r--. 1 root root  188 May 11  2017 portsentry.conf
-rw-r--r--. 1 root root 1289 May 11  2017 postfix.conf
-rw-r--r--. 1 root root  454 May 11  2017 postfix-rbl.conf
-rw-r--r--. 1 root root  482 May 11  2017 postfix-sasl.conf
-rw-r--r--. 1 root root 1216 May 11  2017 proftpd.conf
-rw-r--r--. 1 root root 2409 May 11  2017 pure-ftpd.conf
```

```
-rw-r--r--. 1 root root  795 May 11  2017 qmail.conf
-rw-r--r--. 1 root root 1286 May 11  2017 recidive.conf
-rw-r--r--. 1 root root 1367 May 11  2017 roundcube-auth.conf
-rw-r--r--. 1 root root  821 May 11  2017 screensharingd.conf
-rw-r--r--. 1 root root  517 May 11  2017 selinux-common.conf
-rw-r--r--. 1 root root  570 May 11  2017 selinux-ssh.conf
-rw-r--r--. 1 root root  396 Jul 13  2017 sendmail-auth.conf
-rw-r--r--. 1 root root 2472 Jul 13  2017 sendmail-reject.conf
-rw-r--r--. 1 root root  371 May 11  2017 sieve.conf
-rw-r--r--. 1 root root  706 May 11  2017 slapd.conf
-rw-r--r--. 1 root root  472 May 11  2017 sogo-auth.conf
-rw-r--r--. 1 root root 1094 May 11  2017 solid-pop3d.conf
-rw-r--r--. 1 root root  206 May 11  2017 squid.conf
-rw-r--r--. 1 root root  199 May 11  2017 squirrelmail.conf
-rw-r--r--. 1 root root  186 May 11  2017 sshd-aggressive.conf
-rw-r--r--. 1 root root 4487 May 11  2017 sshd.conf
-rw-r--r--. 1 root root  476 May 11  2017 sshd-ddos.conf
-rw-r--r--. 1 root root  363 May 11  2017 stunnel.conf
-rw-r--r--. 1 root root  649 May 11  2017 suhosin.conf
-rw-r--r--. 1 root root  821 May 11  2017 tine20.conf
-rw-r--r--. 1 root root  374 May 11  2017 uwimap-auth.conf
-rw-r--r--. 1 root root  637 May 11  2017 vsftpd.conf
-rw-r--r--. 1 root root  444 May 11  2017 webmin-auth.conf
-rw-r--r--. 1 root root  520 May 11  2017 wuftpd.conf
-rw-r--r--. 1 root root  503 May 11  2017 xinetd-fail.conf
```

Le répertoire /etc/fail2ban/action.d/

Ce répertoire contient les fichiers appelés par les directives **action** dans les sections des prisons :

```
[root@centos7 ~]# ls -l /etc/fail2ban/action.d/
total 244
-rw-r--r--. 1 root root   587 May 11  2017 apf.conf
```

```
-rw-r--r--. 1 root root   629 May 11  2017 badips.conf
-rw-r--r--. 1 root root 10620 May 11  2017 badips.py
-rw-r--r--. 2 root root 11791 Jul 13  2017 badips.pyc
-rw-r--r--. 2 root root 11791 Jul 13  2017 badips.pyo
-rw-r--r--. 1 root root  2631 May 11  2017 blocklist_de.conf
-rw-r--r--. 1 root root  1931 May 11  2017 cloudflare.conf
-rw-r--r--. 1 root root  7524 May 11  2017 dshield.conf
-rw-r--r--. 1 root root  1133 May 11  2017 dummy.conf
-rw-r--r--. 1 root root  1538 May 11  2017 firewallcmd-allports.conf
-rw-r--r--. 1 root root  1530 May 11  2017 firewallcmd-ipset.conf
-rw-r--r--. 1 root root  2088 May 11  2017 firewallcmd-multiport.conf
-rw-r--r--. 1 root root  2005 May 11  2017 firewallcmd-new.conf
-rw-r--r--. 1 root root  3223 May 11  2017 firewallcmd-rich-logging.conf
-rw-r--r--. 1 root root  2689 May 11  2017 firewallcmd-rich-rules.conf
-rw-r--r--. 1 root root  1437 May 11  2017 iptables-allports.conf
-rw-r--r--. 1 root root  1868 May 11  2017 iptables-common.conf
-rw-r--r--. 1 root root  1350 May 11  2017 iptables.conf
-rw-r--r--. 1 root root  1828 May 11  2017 iptables-ipset-proto4.conf
-rw-r--r--. 1 root root  1755 May 11  2017 iptables-ipset-proto6-allports.conf
-rw-r--r--. 1 root root  1798 May 11  2017 iptables-ipset-proto6.conf
-rw-r--r--. 1 root root  1431 May 11  2017 iptables-multiport.conf
-rw-r--r--. 1 root root  1910 May 11  2017 iptables-multiport-log.conf
-rw-r--r--. 1 root root  1508 May 11  2017 iptables-new.conf
-rw-r--r--. 1 root root  2282 May 11  2017 iptables-xt_recent-echo.conf
-rw-r--r--. 1 root root  1556 May 11  2017 mail.conf
-rw-r--r--. 1 root root  5233 May 11  2017 mynetwatchman.conf
-rw-r--r--. 1 root root  1493 May 11  2017 netscaler.conf
-rw-r--r--. 1 root root   489 May 11  2017 nftables-allports.conf
-rw-r--r--. 1 root root  3680 May 11  2017 nftables-common.conf
-rw-r--r--. 1 root root   496 May 11  2017 nftables-multiport.conf
-rw-r--r--. 1 root root  1436 May 11  2017 npf.conf
-rw-r--r--. 1 root root  3146 May 11  2017 nsupdate.conf
-rw-r--r--. 1 root root  1023 May 11  2017 route.conf
-rw-r--r--. 1 root root  2762 May 11  2017 sendmail-buffered.conf
```

```
-rw-r--r--. 1 root root  1818 May 11  2017 sendmail-common.conf
-rw-r--r--. 1 root root   798 May 11  2017 sendmail.conf
-rw-r--r--. 1 root root  1692 May 11  2017 sendmail-geoip-lines.conf
-rw-r--r--. 1 root root   918 May 11  2017 sendmail-whois.conf
-rw-r--r--. 1 root root   993 May 11  2017 sendmail-whois-ipjailmatches.conf
-rw-r--r--. 1 root root   974 May 11  2017 sendmail-whois-ipmatches.conf
-rw-r--r--. 1 root root  1207 May 11  2017 sendmail-whois-lines.conf
-rw-r--r--. 1 root root   938 May 11  2017 sendmail-whois-matches.conf
-rw-r--r--. 1 root root  2981 May 11  2017 shorewall-ipset-proto6.conf
-rw-r--r--. 1 root root  6021 May 11  2017 smtp.py
-rw-r--r--. 2 root root  5921 Jul 13  2017 smtp.pyc
-rw-r--r--. 2 root root  5921 Jul 13  2017 smtp.pyo
-rw-r--r--. 1 root root  1330 May 11  2017 symbiosis-blacklist-allports.conf
-rw-r--r--. 1 root root  6018 May 11  2017 xarf-login-attack.conf
```

4.4 - Commandes

Fail2Ban est constitué de deux commandes :

```
[root@centos7 ~]# which fail2ban-client
/bin/fail2ban-client
[root@centos7 ~]# which fail2ban-server
/bin/fail2ban-server
```

L'exécutable **fail2ban-server** est responsable de l'examen des fichiers de journalisation ainsi que les commandes de blocage/déblocage. La commande fail2ban-client est utilisée pour configurer le **fail2ban-server**.

Les options de la commande **fail2ban-server** sont :

```
[root@centos7 ~]# fail2ban-server --help
Usage: /bin/fail2ban-server [OPTIONS]

Fail2Ban v0.9.7 reads log file that contains password failure report
```

```
and bans the corresponding IP addresses using firewall rules.

Only use this command for debugging purpose. Start the server with
fail2ban-client instead. The default behaviour is to start the server
in background.

Options:
    -b                  start in background
    -f                  start in foreground
    -s <FILE>           socket path
    -p <FILE>           pidfile path
    -x                  force execution of the server (remove socket file)
    -h, --help          display this help message
    -V, --version       print the version

Report bugs to https://github.com/fail2ban/fail2ban/issues
```

Les options de la commande **fail2ban-client** sont :

```
[root@centos7 ~]# fail2ban-client --help
Usage: /bin/fail2ban-client [OPTIONS] <COMMAND>

Fail2Ban v0.9.7 reads log file that contains password failure report
and bans the corresponding IP addresses using firewall rules.

Options:
    -c <DIR>               configuration directory
    -s <FILE>              socket path
    -p <FILE>              pidfile path
    -d                     dump configuration. For debugging
    -i                     interactive mode
    -v                     increase verbosity
    -q                     decrease verbosity
    -x                     force execution of the server (remove socket file)
```

```
    -b                      start server in background (default)
    -f                      start server in foreground (note that the client forks once itself)
    -h, --help              display this help message
    -V, --version           print the version

Command:
                                            BASIC
    start                                   starts the server and the jails
    reload                                  reloads the configuration
    reload <JAIL>                           reloads the jail <JAIL>
    stop                                    stops all jails and terminate the
                                            server
    status                                  gets the current status of the
                                            server
    ping                                    tests if the server is alive
    help                                    return this output
    version                                 return the server version

                                            LOGGING
    set loglevel <LEVEL>                    sets logging level to <LEVEL>.
                                            Levels: CRITICAL, ERROR, WARNING,
                                            NOTICE, INFO, DEBUG
    get loglevel                            gets the logging level
    set logtarget <TARGET>                  sets logging target to <TARGET>.
                                            Can be STDOUT, STDERR, SYSLOG or a
                                            file
    get logtarget                           gets logging target
    set syslogsocket auto|<SOCKET>          sets the syslog socket path to
                                            auto or <SOCKET>. Only used if
                                            logtarget is SYSLOG
    get syslogsocket                        gets syslog socket path
    flushlogs                               flushes the logtarget if a file
                                            and reopens it. For log rotation.
```

```
                                        DATABASE
set dbfile <FILE>                       set the location of fail2ban
                                        persistent datastore. Set to
                                        "None" to disable
get dbfile                              get the location of fail2ban
                                        persistent datastore
set dbpurgeage <SECONDS>                sets the max age in <SECONDS> that
                                        history of bans will be kept
get dbpurgeage                          gets the max age in seconds that
                                        history of bans will be kept


                                        JAIL CONTROL
add <JAIL> <BACKEND>                    creates <JAIL> using <BACKEND>
start <JAIL>                            starts the jail <JAIL>
stop <JAIL>                             stops the jail <JAIL>. The jail is
                                        removed
status <JAIL> [FLAVOR]                  gets the current status of <JAIL>,
                                        with optional flavor or extended
                                        info


                                        JAIL CONFIGURATION
set <JAIL> idle on|off                  sets the idle state of <JAIL>
set <JAIL> addignoreip <IP>             adds <IP> to the ignore list of
                                        <JAIL>
set <JAIL> delignoreip <IP>             removes <IP> from the ignore list
                                        of <JAIL>
set <JAIL> addlogpath <FILE> ['tail']   adds <FILE> to the monitoring list
                                        of <JAIL>, optionally starting at
                                        the 'tail' of the file (default
                                        'head').
set <JAIL> dellogpath <FILE>            removes <FILE> from the monitoring
                                        list of <JAIL>
set <JAIL> logencoding <ENCODING>       sets the <ENCODING> of the log
                                        files for <JAIL>
```

```
    set <JAIL> addjournalmatch <MATCH>        adds <MATCH> to the journal filter
                                              of <JAIL>
    set <JAIL> deljournalmatch <MATCH>        removes <MATCH> from the journal
                                              filter of <JAIL>
    set <JAIL> addfailregex <REGEX>           adds the regular expression
                                              <REGEX> which must match failures
                                              for <JAIL>
    set <JAIL> delfailregex <INDEX>           removes the regular expression at
                                              <INDEX> for failregex
    set <JAIL> ignorecommand <VALUE>          sets ignorecommand of <JAIL>
    set <JAIL> addignoreregex <REGEX>         adds the regular expression
                                              <REGEX> which should match pattern
                                              to exclude for <JAIL>
    set <JAIL> delignoreregex <INDEX>         removes the regular expression at
                                              <INDEX> for ignoreregex
    set <JAIL> findtime <TIME>                sets the number of seconds <TIME>
                                              for which the filter will look
                                              back for <JAIL>
    set <JAIL> bantime <TIME>                 sets the number of seconds <TIME>
                                              a host will be banned for <JAIL>
    set <JAIL> datepattern <PATTERN>          sets the <PATTERN> used to match
                                              date/times for <JAIL>
    set <JAIL> usedns <VALUE>                 sets the usedns mode for <JAIL>
    set <JAIL> banip <IP>                     manually Ban <IP> for <JAIL>
    set <JAIL> unbanip <IP>                   manually Unban <IP> in <JAIL>
    set <JAIL> maxretry <RETRY>               sets the number of failures
                                              <RETRY> before banning the host
                                              for <JAIL>
    set <JAIL> maxlines <LINES>               sets the number of <LINES> to
                                              buffer for regex search for <JAIL>
    set <JAIL> addaction <ACT>[ <PYTHONFILE> <JSONKWARGS>]
                                              adds a new action named <ACT> for
                                              <JAIL>. Optionally for a Python
                                              based action, a <PYTHONFILE> and
```

```
                                            <JSONKWARGS> can be specified,
                                            else will be a Command Action
    set <JAIL> delaction <ACT>              removes the action <ACT> from
                                            <JAIL>

                                            COMMAND ACTION CONFIGURATION
    set <JAIL> action <ACT> actionstart <CMD>
                                            sets the start command <CMD> of
                                            the action <ACT> for <JAIL>
    set <JAIL> action <ACT> actionstop <CMD> sets the stop command <CMD> of the
                                            action <ACT> for <JAIL>
    set <JAIL> action <ACT> actioncheck <CMD>
                                            sets the check command <CMD> of
                                            the action <ACT> for <JAIL>
    set <JAIL> action <ACT> actionban <CMD>  sets the ban command <CMD> of the
                                            action <ACT> for <JAIL>
    set <JAIL> action <ACT> actionunban <CMD>
                                            sets the unban command <CMD> of
                                            the action <ACT> for <JAIL>
    set <JAIL> action <ACT> timeout <TIMEOUT>
                                            sets <TIMEOUT> as the command
                                            timeout in seconds for the action
                                            <ACT> for <JAIL>

                                            GENERAL ACTION CONFIGURATION
    set <JAIL> action <ACT> <PROPERTY> <VALUE>
                                            sets the <VALUE> of <PROPERTY> for
                                            the action <ACT> for <JAIL>
    set <JAIL> action <ACT> <METHOD>[ <JSONKWARGS>]
                                            calls the <METHOD> with
                                            <JSONKWARGS> for the action <ACT>
                                            for <JAIL>

                                            JAIL INFORMATION
```

```
    get <JAIL> logpath                      gets the list of the monitored
                                            files for <JAIL>
    get <JAIL> logencoding                  gets the encoding of the log files
                                            for <JAIL>
    get <JAIL> journalmatch                 gets the journal filter match for
                                            <JAIL>
    get <JAIL> ignoreip                     gets the list of ignored IP
                                            addresses for <JAIL>
    get <JAIL> ignorecommand                gets ignorecommand of <JAIL>
    get <JAIL> failregex                    gets the list of regular
                                            expressions which matches the
                                            failures for <JAIL>
    get <JAIL> ignoreregex                  gets the list of regular
                                            expressions which matches patterns
                                            to ignore for <JAIL>
    get <JAIL> findtime                     gets the time for which the filter
                                            will look back for failures for
                                            <JAIL>
    get <JAIL> bantime                      gets the time a host is banned for
                                            <JAIL>
    get <JAIL> datepattern                  gets the patern used to match
                                            date/times for <JAIL>
    get <JAIL> usedns                       gets the usedns setting for <JAIL>
    get <JAIL> maxretry                     gets the number of failures
                                            allowed for <JAIL>
    get <JAIL> maxlines                     gets the number of lines to buffer
                                            for <JAIL>
    get <JAIL> actions                      gets a list of actions for <JAIL>

                                            COMMAND ACTION INFORMATION
    get <JAIL> action <ACT> actionstart     gets the start command for the
                                            action <ACT> for <JAIL>
    get <JAIL> action <ACT> actionstop      gets the stop command for the
                                            action <ACT> for <JAIL>
```

```
    get <JAIL> action <ACT> actioncheck      gets the check command for the
                                             action <ACT> for <JAIL>
    get <JAIL> action <ACT> actionban        gets the ban command for the
                                             action <ACT> for <JAIL>
    get <JAIL> action <ACT> actionunban      gets the unban command for the
                                             action <ACT> for <JAIL>
    get <JAIL> action <ACT> timeout          gets the command timeout in
                                             seconds for the action <ACT> for
                                             <JAIL>

                                             GENERAL ACTION INFORMATION
    get <JAIL> actionproperties <ACT>        gets a list of properties for the
                                             action <ACT> for <JAIL>
    get <JAIL> actionmethods <ACT>           gets a list of methods for the
                                             action <ACT> for <JAIL>
    get <JAIL> action <ACT> <PROPERTY>       gets the value of <PROPERTY> for
                                             the action <ACT> for <JAIL>

Report bugs to https://github.com/fail2ban/fail2ban/issues
```

4.5 - Activer et Démarrer le Serveur

Pour prendre en compte la configuration dans le fichier **/etc/fail2ban/jail.local**, activez et démarrez le server :

```
[root@centos7 ~]# systemctl status fail2ban
● fail2ban.service - Fail2Ban Service
   Loaded: loaded (/usr/lib/systemd/system/fail2ban.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:fail2ban(1)

[root@centos7 ~]# systemctl enable fail2ban

Created symlink from /etc/systemd/system/multi-user.target.wants/fail2ban.service to
```

```
/usr/lib/systemd/system/fail2ban.service.

[root@centos7 ~]# systemctl start fail2ban

[[root@centos7 ~]# ps aux | grep fail2ban-server
root     19229  0.5  2.3 399480 11532 ?        Sl   23:37   0:00 /usr/bin/python2 -s /usr/bin/fail2ban-server -s
/var/run/fail2ban/fail2ban.sock -p /var/run/fail2ban/fail2ban.pid -x -b
root     20004  0.0  0.1 112660   988 pts/1    S+   23:39   0:00 grep --color=auto fail2ban-server
```

Utiliser la Commande Fail2Ban-server

Pour connaître le status de Fail2Ban-server, saisissez la commande suivante :

```
[root@centos7 ~]# fail2ban-client status
Status
|- Number of jail:  1
`- Jail list:   sshd
```

Il est aussi possible de se renseigner sur le statut d'un prison particulier :

```
[root@centos7 ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed: 0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned: 0
   `- Banned IP list:
```

La commande **fail2ban-client** peut être utilisée pour contrôler un prison :

```
[root@centos7 ~]# fail2ban-client stop sshd
Jail stopped

[root@centos7 ~]# fail2ban-client status sshd
ERROR  NOK: ('sshd',)
Sorry but the jail 'sshd' does not exist

[root@centos7 ~]# fail2ban-client reload

[root@centos7 ~]# fail2ban-client status sshd
Status for the jail: sshd
|- Filter
|  |- Currently failed: 0
|  |- Total failed: 0
|  `- Journal matches:  _SYSTEMD_UNIT=sshd.service + _COMM=sshd
`- Actions
   |- Currently banned: 0
   |- Total banned: 0
   `- Banned IP list:
```

Ajouter un Prison

Installez maintenant le serveur Apache si ce n'est pas déjà fait :

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

Activez et démarrez le service Apache si ce n'est pas déjà lancé :

```
[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.

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

Modifiez maintenant votre fichier **/etc/fail2ban/jail.local** :

```
[root@centos7 ~]# vi /etc/fail2ban/jail.local
[root@centos7 ~]# cat /etc/fail2ban/jail.local
[DEFAULT]
ignoreip = 127.0.0.1 10.0.2.51
findtime = 3600
bantime = 86400
maxretry = 5

[sshd]
enabled = true

[apache-auth]
enabled = true
```

Appliquez la nouvelle configuration et constatez le résultat :

```
[root@centos7 ~]# fail2ban-client reload
[root@centos7 ~]# fail2ban-client status
Status
|- Number of jail:  2
`- Jail list:   apache-auth, sshd
```

LAB #5 - Mise en place de SSH et SCP

5.1 - Introduction

La commande **ssh** est le successeur et la remplaçante de la commande **rlogin**. Il permet d'établir des connexions sécurisées avec une machine distante. SSH comporte cinq acteurs :

- Le **serveur SSH**
  - le démon sshd, qui s'occupe des authentifications et autorisations des clients,
- Le **client SSH**
  - ssh ou scp, qui assure la connexion et le dialogue avec le serveur,
- La **session** qui représente la connexion courante et qui commence juste après l'authentification réussie,
- Les **clefs**
  - **Couple de clef utilisateur asymétriques** et persistantes qui assurent l'identité d'un utilisateur et qui sont stockés sur disque dur,
  - **Clef hôte asymétrique et persistante** garantissant l'identité du serveur er qui est conservé sur disque dur
  - **Clef serveur asymétrique et temporaire** utilisée par le protocole SSH1 qui sert au chiffrement de la clé de session,
  - **Clef de session symétrique qui est générée aléatoirement** et qui permet le chiiffrement de la communication entre le client et le serveur. Elle est détruite en fin de session. SSH-1 utilise une seule clef tandis que SSH-2 utilise une clef par direction de la communication,
- La **base de données des hôtes connus** qui stocke les clés des connexions précédentes.

SSH fonctionne de la manière suivante pour la la mise en place d'un canal sécurisé:

- Le client contacte le serveur sur son port 22,
- Les client et le serveur échangent leur version de SSH. En cas de non-compatibilité de versions, l'un des deux met fin au processus,
- Le serveur SSH s'identifie auprès du client en lui fournissant :
  - Sa clé hôte,
  - Sa clé serveur,
  - Une séquence aléatoire de huit octets à inclure dans les futures réponses du client,
  - Une liste de méthodes de chiffrement, compression et authentification,
- Le client et le serveur produisent un identifiant identique, un haché MD5 long de 128 bits contenant la clé hôte, la clé serveur et la séquence aléatoire,
- Le client génère sa clé de session symétrique et la chiffre deux fois de suite, une fois avec la clé hôte du serveur et la deuxième fois avec la clé serveur. Le client envoie cette clé au serveur accompagnée de la séquence aléatoire et un choix d'algorithmes supportés,

- Le serveur déchiffre la clé de session,
- Le client et le serveur mettent en place le canal sécurisé.

SSH-1

SSH-1 utilise une paire de clefs de type RSA1. Il assure l'intégrité des données par une **Contrôle de Redondance Cyclique** (CRC) et est un bloc dit **monolithique**.

Afin de s'identifier, le client essaie chacune des six méthodes suivantes :

- **Kerberos**,
- **Rhosts**,
- **RhostsRSA**,
- Par **clef asymétrique**,
- **TIS**,
- Par **mot de passe**.

SSH-2

SSH-2 utilise **DSA** ou **RSA**. Il assure l'intégrité des données par l'algorithme **HMAC**. SSH-2 est organisé en trois **couches** :

- **SSH-TRANS** – Transport Layer Protocol,
- **SSH-AUTH** – Authentification Protocol,
- **SSH-CONN** – Connection Protocol.

SSH-2 diffère de SSH-1 essentiellement dans la phase authentification.

Trois méthodes d'authentification :

- Par **clef asymétrique**,
  - Identique à SSH-1 sauf avec l'algorithme DSA,
- **RhostsRSA**,
- Par **mot de passe**.

Les options de cette commande sont :

```
[root@centos7 ~]# ssh --help
unknown option -- -
usage: ssh [-1246AaCfGgKkMNnqsTtVvXxYy] [-b bind_address] [-c cipher_spec]
           [-D [bind_address:]port] [-E log_file] [-e escape_char]
           [-F configfile] [-I pkcs11] [-i identity_file]
           [-J [user@]host[:port]] [-L address] [-l login_name] [-m mac_spec]
           [-O ctl_cmd] [-o option] [-p port] [-Q query_option] [-R address]
           [-S ctl_path] [-W host:port] [-w local_tun[:remote_tun]]
           [user@]hostname [command]
```

5.2 - L'authentification par mot de passe

L'utilisateur fournit un mot de passe au client ssh. Le client ssh le transmet de façon sécurisée au serveur ssh puis le serveur vérifie le mot de passe et l'accepte ou non.

Avantage:

- Aucune configuration de clef asymétrique n'est nécessaire.

Inconvénients:

- L'utilisateur doit fournir à chaque connexion un identifiant et un mot de passe,
- Moins sécurisé qu'un système par clef asymétrique.

5.3 - L'authentification par clef asymétrique

- Le **client** envoie au serveur une requête d'authentification par clé asymétrique qui contient le module de la clé à utiliser,
- Le **serveur** recherche une correspondance pour ce module dans le fichier des clés autorisés **~/.ssh/authorized_keys**,
  - Dans le cas où une correspondance n'est pas trouvée, le serveur met fin à la communication,
  - Dans le cas contraire le serveur génère une chaîne aléatoire de 256 bits appelée un **challenge** et la chiffre avec la **clé publique du**

client,

- Le **client** reçoit le challenge et le déchiffre avec la partie privée de sa clé. Il combine le challenge avec l'identifiant de session et chiffre le résultat. Ensuite il envoie le résultat chiffré au serveur.
- Le **serveur** génère le même haché et le compare avec celui reçu du client. Si les deux hachés sont identiques, l'authentification est réussie.

Installation

Pour installer/mettre à jour le serveur **sshd**, utilisez **yum** :

```
[root@centos7 ~]# yum install openssh-server
Loaded plugins: fastestmirror, langpacks
Loading mirror speeds from cached hostfile
 * base: centos.mirror.fr.planethoster.net
 * extras: ftp.ciril.fr
 * updates: centos.mirrors.ovh.net
Package openssh-server-6.6.1p1-25.el7_2.x86_64 already installed and latest version
Nothing to do
```

Important - Pour les stations de travail, installez le client : **openssh-clients**.

Les options de la commande sont :

```
SYNOPSIS
     sshd [-46DdeiqTt] [-b bits] [-C connection_spec] [-f config_file] [-g login_grace_time] [-h host_key_file]
[-k key_gen_time] [-o option] [-p port]  [-u len]
```

Configuration

Serveur

La configuration du serveur s'effectue dans le fichier **/etc/ssh/sshd_config** :

```
[root@centos7 ~]# cat /etc/ssh/sshd_config
#   $OpenBSD: sshd_config,v 1.93 2014/01/10 05:59:19 djm Exp $

# This is the sshd server system-wide configuration file.  See
# sshd_config(5) for more information.

# This sshd was compiled with PATH=/usr/local/bin:/usr/bin

# The strategy used for options in the default sshd_config shipped with
# OpenSSH is to specify options with their default value where
# possible, but leave them commented.  Uncommented options override the
# default value.

# If you want to change the port on a SELinux system, you have to tell
# SELinux about this change.
# semanage port -a -t ssh_port_t -p tcp #PORTNUMBER
#
#Port 22
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::

# The default requires explicit activation of protocol 1
#Protocol 2

# HostKey for protocol version 1
#HostKey /etc/ssh/ssh_host_key
# HostKeys for protocol version 2
HostKey /etc/ssh/ssh_host_rsa_key
```

```
#HostKey /etc/ssh/ssh_host_dsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key

# Lifetime and size of ephemeral version 1 server key
#KeyRegenerationInterval 1h
#ServerKeyBits 1024

# Ciphers and keying
#RekeyLimit default none

# Logging
# obsoletes QuietMode and FascistLogging
#SyslogFacility AUTH
SyslogFacility AUTHPRIV
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin yes
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#RSAAuthentication yes
#PubkeyAuthentication yes

# The default is to check both .ssh/authorized_keys and .ssh/authorized_keys2
# but this is overridden so installations will only check .ssh/authorized_keys
AuthorizedKeysFile  .ssh/authorized_keys

#AuthorizedPrincipalsFile none
```

```
#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#RhostsRSAAuthentication no
# similar for protocol version 2
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# RhostsRSAAuthentication and HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication yes
#PermitEmptyPasswords no
PasswordAuthentication yes

# Change to no to disable s/key passwords
#ChallengeResponseAuthentication yes
ChallengeResponseAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no
#KerberosUseKuserok yes

# GSSAPI options
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no
```

```
#GSSAPIEnablek5users no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the ChallengeResponseAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
# PAM authentication via ChallengeResponseAuthentication may bypass
# the setting of "PermitRootLogin without-password".
# If you just want the PAM account and session checks to run without
# PAM authentication, then enable this but set PasswordAuthentication
# and ChallengeResponseAuthentication to 'no'.
# WARNING: 'UsePAM no' is not supported in Red Hat Enterprise Linux and may cause several
# problems.
UsePAM yes

#AllowAgentForwarding yes
#AllowTcpForwarding yes
#GatewayPorts no
X11Forwarding yes
#X11DisplayOffset 10
#X11UseLocalhost yes
#PermitTTY yes
#PrintMotd yes
#PrintLastLog yes
#TCPKeepAlive yes
#UseLogin no
UsePrivilegeSeparation sandbox      # Default for new installations.
#PermitUserEnvironment no
#Compression delayed
#ClientAliveInterval 0
#ClientAliveCountMax 3
#ShowPatchLevel no
#UseDNS yes
#PidFile /var/run/sshd.pid
```

```
#MaxStartups 10:30:100
#PermitTunnel no
#ChrootDirectory none
#VersionAddendum none

# no default banner path
#Banner none

# Accept locale-related environment variables
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS

# override default of no subsystems
Subsystem   sftp    /usr/libexec/openssh/sftp-server

# Example of overriding settings on a per-user basis
#Match User anoncvs
#   X11Forwarding no
#   AllowTcpForwarding no
#   PermitTTY no
#   ForceCommand cvs server
```

Pour ôter les lignes de commentaires dans ce fichier, utilisez la commande suivante :

```
[root@centos7 ~]# cd /tmp ; grep -E -v '^(#|$)'  /etc/ssh/sshd_config > sshd_config
[root@centos7 tmp]# cat sshd_config
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
SyslogFacility AUTHPRIV
AuthorizedKeysFile  .ssh/authorized_keys
PasswordAuthentication yes
```

```
ChallengeResponseAuthentication no
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
UsePAM yes
X11Forwarding yes
UsePrivilegeSeparation sandbox      # Default for new installations.
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
Subsystem   sftp    /usr/libexec/openssh/sftp-server
```

Pour sécuriser le serveur ssh, ajoutez ou modifiez les directives suivantes :

```
AllowGroups adm
Banner /etc/issue.net
HostbasedAuthentication no
IgnoreRhosts yes
LoginGraceTime 60
LogLevel INFO
PermitEmptyPasswords no
PermitRootLogin no
PrintLastLog yes
Protocol 2
StrictModes yes
X11Forwarding no
```

Votre fichier ressemblera à celui-ci :

```
AllowGroups adm
Banner /etc/issue.net
HostbasedAuthentication no
IgnoreRhosts yes
LoginGraceTime 60
```

```
LogLevel INFO
PermitEmptyPasswords no
PermitRootLogin no
PrintLastLog yes
Protocol 2
StrictModes yes
X11Forwarding no
HostKey /etc/ssh/ssh_host_rsa_key
HostKey /etc/ssh/ssh_host_ecdsa_key
HostKey /etc/ssh/ssh_host_ed25519_key
SyslogFacility AUTHPRIV
AuthorizedKeysFile  .ssh/authorized_keys
PasswordAuthentication yes
ChallengeResponseAuthentication no
GSSAPIAuthentication yes
GSSAPICleanupCredentials no
UsePAM yes
UsePrivilegeSeparation sandbox      # Default for new installations.
AcceptEnv LANG LC_CTYPE LC_NUMERIC LC_TIME LC_COLLATE LC_MONETARY LC_MESSAGES
AcceptEnv LC_PAPER LC_NAME LC_ADDRESS LC_TELEPHONE LC_MEASUREMENT
AcceptEnv LC_IDENTIFICATION LC_ALL LANGUAGE
AcceptEnv XMODIFIERS
Subsystem   sftp    /usr/libexec/openssh/sftp-server
```

A Faire - Renommez le fichier **/etc/ssh/sshd_config** en **/etc/ssh/sshd_config.old** puis copiez le fichier **/tmp/sshd_config** vers **/etc/sshd/**. Redémarrez ensuite le service sshd. N'oubliez pas de mettre l'utilisateur **trainee** dans le groupe **adm** !

Pour générer les clefs sur le serveur saisissez la commande suivante en tant que **root**:

Lors de la génération des clefs, la passphrase doit être **vide**.

```
[root@centos7 ~]# ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/root/.ssh/id_dsa): /etc/ssh/ssh_host_dsa_key
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /etc/ssh/ssh_host_dsa_key.
Your public key has been saved in /etc/ssh/ssh_host_dsa_key.pub.
The key fingerprint is:
d5:54:d3:30:1c:f5:da:f8:21:15:1f:c8:6c:3b:b1:ff root@centos7.fenestros.loc
The key's randomart image is:
+--[ DSA 1024]----+
|            +oBB.|
|           o *.o*|
|          . o +.o|
|         .   +.+ |
|        S    .=..|
|              .o.|
|                o|
|                E|
|                 |
+-----------------+
```

Important - Le chemin à indiquer pour le fichier est **/etc/ssh/ssh_host_dsa_key**. De la même façon, il est possible de générer les clefs au format **RSA**, **ECDSA** et **ED25519**.

Les clefs publiques générées possèdent l'extension **.pub**. Les clefs privées n'ont pas d'extension :

```
[root@centos7 ~]# ls /etc/ssh
```

```
moduli      sshd_config       ssh_host_dsa_key.pub  ssh_host_ecdsa_key.pub  ssh_host_ed25519_key.pub
ssh_host_rsa_key.pub
ssh_config  ssh_host_dsa_key  ssh_host_ecdsa_key    ssh_host_ed25519_key    ssh_host_rsa_key
```

Re-démarrez ensuite le service sshd :

```
[root@centos7 ~]# systemctl restart sshd.service
```

Saisissez maintenant les commandes suivantes en tant que **trainee** :

Important - Lors de la génération des clefs, la passphrase doit être **vide**.

```
[trainee@centos7 ~]$ ssh-keygen -t dsa
Generating public/private dsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_dsa):
Created directory '/home/trainee/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_dsa.
Your public key has been saved in /home/trainee/.ssh/id_dsa.pub.
The key fingerprint is:
97:92:85:d1:ae:97:f7:64:d2:54:45:89:eb:57:b1:66 trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ DSA 1024]----+
|        ..    ..=|
|         o.  . o.|
|        ...   ..o|
|         o.. ..E.|
|        S.o..oo .|
|        .oo o.+. |
|         . . =.  |
```

```
|              .  |
|                 |
+-----------------+
[trainee@centos7 ~]$ ssh-keygen -t rsa
Generating public/private rsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_rsa.
Your public key has been saved in /home/trainee/.ssh/id_rsa.pub.
The key fingerprint is:
80:4c:5a:bf:d0:2f:d1:a1:34:7c:09:a1:9c:0d:ed:2d trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ RSA 2048]----+
|    +o=o..       |
|   * Xo+o.       |
|  . B.Bo.        |
|     .E=.        |
|      o.S        |
|       .         |
|                 |
|                 |
|                 |
+-----------------+
[trainee@centos7 ~]$ ssh-keygen -t ecdsa
Generating public/private ecdsa key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_ecdsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_ecdsa.
Your public key has been saved in /home/trainee/.ssh/id_ecdsa.pub.
The key fingerprint is:
41:5d:64:cf:d6:4a:ce:8e:a9:a8:4a:62:04:57:09:fc trainee@centos7.fenestros.loc
The key's randomart image is:
```

```
+--[ECDSA  256]---+
| .....  .. o+    |
|  ...  .  .. o . |
|. ..    .     = .|
| o  E    .   = . |
|  .     S     +  |
| .           +   |
|  o .       o .  |
| . o     . .     |
|    ..... .      |
+-----------------+
[trainee@centos7 ~]$ ssh-keygen -t ed25519
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/trainee/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/trainee/.ssh/id_ed25519.
Your public key has been saved in /home/trainee/.ssh/id_ed25519.pub.
The key fingerprint is:
66:3a:83:d1:6d:79:46:48:88:7c:d9:65:59:bb:e6:d0 trainee@centos7.fenestros.loc
The key's randomart image is:
+--[ED25519  256--+
|   . . +..oo.    |
|    o +..o.  .   |
|     .  . . .    |
|     . . o . .   |
|    . . S + E    |
|     o = o +     |
|    . +     .    |
|       o         |
|                 |
+-----------------+
```

Important - Les clés générées seront placées dans le répertoire **~/.ssh/**.

Utilisation

La commande ssh prend la forme suivante:

```
ssh -l nom_de_compte numero_ip (nom_de_machine)
```

En saisissant cette commande sur votre propre machine, vous obtiendrez un résultat similaire à celle-ci :

```
[trainee@centos7 ~]$ su -
Mot de passe :
Dernière connexion : lundi  9 mai 2016 à 22:47:48 CEST sur pts/0

[root@centos7 ~]# ssh trainee@localhost
The authenticity of host 'localhost (127.0.0.1)' can't be established.
ECDSA key fingerprint is 19:cd:05:58:af:2c:10:82:52:ba:e3:31:df:bd:72:54.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
trainee@localhost's password: trainee
Last login: Mon May  9 23:25:15 2016 from localhost.localdomain
```

Important - Notez l'utilisation de **trainee@localhost** à la place de **-l trainee localhost**.

5.4 - Tunnels SSH

Le protocole SSH peut être utilisé pour sécuriser les protocoles tels telnet, pop3 etc.. En effet, on peut créer un *tunnel* SSH dans lequel passe les communications du protocole non-sécurisé.

La commande pour créer un tunnel ssh prend la forme suivante :

```
ssh -N -f compte@hôte -Lport-local:localhost:port_distant
```

Dans votre cas, vous allez créer un tunnel dans votre propre vm entre le port 15023 et le port 23 :

```
[root@centos7 ~]# ssh -N -f trainee@localhost -L15023:localhost:23
trainee@localhost's password:
```

Installez maintenant le client et le serveur telnet :

```
[root@centos7 ~]# yum install telnet telnet-server
```

Telnet n'est ni démarré ni activé. Il convient donc de le démarrer et de l'activer :

```
[root@centos7 ~]# systemctl status telnet.socket
● telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; disabled; vendor preset: disabled)
   Active: inactive (dead)
     Docs: man:telnetd(8)
   Listen: [::]:23 (Stream)
 Accepted: 0; Connected: 0

[root@centos7 ~]# systemctl start telnet.socket

[root@centos7 ~]# systemctl status telnet.socket
● telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; disabled; vendor preset: disabled)
```

```
   Active: active (listening) since Mon 2016-05-09 23:40:13 CEST; 3s ago
     Docs: man:telnetd(8)
   Listen: [::]:23 (Stream)
 Accepted: 0; Connected: 0

May 09 23:40:13 centos7.fenestros.loc systemd[1]: Listening on Telnet Server Activation Socket.
May 09 23:40:13 centos7.fenestros.loc systemd[1]: Starting Telnet Server Activation Socket.

[root@centos7 ~]# systemctl enable telnet.socket
Created symlink from /etc/systemd/system/sockets.target.wants/telnet.socket to
/usr/lib/systemd/system/telnet.socket.
[root@centos7 ~]# systemctl status telnet.socket
● telnet.socket - Telnet Server Activation Socket
   Loaded: loaded (/usr/lib/systemd/system/telnet.socket; enabled; vendor preset: disabled)
   Active: active (listening) since Mon 2016-05-09 23:40:13 CEST; 36s ago
     Docs: man:telnetd(8)
   Listen: [::]:23 (Stream)
 Accepted: 0; Connected: 0

May 09 23:40:13 centos7.fenestros.loc systemd[1]: Listening on Telnet Server Activation Socket.
May 09 23:40:13 centos7.fenestros.loc systemd[1]: Starting Telnet Server Activation Socket.
```

Connectez-vous ensuite via telnet sur le port 15023, vous constaterez que votre connexion n'aboutit pas :

```
[root@centos7 ~]# telnet localhost 15023
Trying 127.0.0.1...
Connected to localhost.
Escape character is '^]'.

Kernel 3.10.0-327.13.1.el7.x86_64 on an x86_64
centos7 login: trainee
Password:
Last login: Mon May  9 23:26:32 from localhost.localdomain
[trainee@centos7 ~]$
```

Important - Notez bien que votre communication telnet passe par le tunnel SSH.

5.5 - SCP

Introduction

La commande **scp** est le successeur et la remplaçante de la commande **rcp** de la famille des commandes **remote**. Il permet de faire des transferts sécurisés à partir d'une machine distante :

```
$ scp compte@numero_ip(nom_de_machine):/chemin_distant/fichier_distant /chemin_local/fichier_local
```

ou vers une machine distante :

```
$ scp /chemin_local/fichier_local compte@numero_ip(nom_de_machine):/chemin_distant/fichier_distant
```

Utilisation

Nous allons maintenant utiliser **scp** pour chercher un fichier sur le «serveur» :

Créez le fichier **/home/trainee/scp_test** :

```
[trainee@centos7 ~]$ pwd
/home/trainee
[trainee@centos7 ~]$ touch scp_test
```

Récupérez le fichier **scp_test** en utilisant scp :

```
[trainee@centos7 ~]$ touch /home/trainee/scp_test
[trainee@centos7 ~]$ scp trainee@127.0.0.1:/home/trainee/scp_test /tmp/scp_test
The authenticity of host '127.0.0.1 (127.0.0.1)' can't be established.
ECDSA key fingerprint is 19:cd:05:58:af:2c:10:82:52:ba:e3:31:df:bd:72:54.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '127.0.0.1' (ECDSA) to the list of known hosts.
trainee@127.0.0.1's password: trainee
scp_test                                                                                    100%    0
0.0KB/s   00:00
[trainee@centos7 ~]$ ls /tmp/scp_test
/tmp/scp_test
```

Mise en place des clefs

Il convient maintenant de se connecter sur le «serveur» en utilisant ssh et vérifiez la présence du répertoire ~/.ssh :

En saisissant cette commande, vous obtiendrez une fenêtre similaire à celle-ci :

```
[trainee@centos7 ~]$ ssh -l trainee 127.0.0.1
trainee@127.0.0.1's password:
Last login: Mon May  9 23:42:46 2016 from localhost.localdomain
[trainee@centos7 ~]$ ls -la | grep .ssh
drwx------.  2 trainee trainee 4096 May  9 23:25 .ssh
[trainee@centos7 ~]$ exit
logout
Connection to 127.0.0.1 closed.
```

Si le dossier distant .ssh n'existe pas dans le répertoire personnel de l'utilisateur connecté, il faut le créer avec des permissions de 700. Dans votre cas, puisque votre machine joue le rôle de serveur **et** du client, le dossier /home/trainee/.ssh existe **déjà**.

Ensuite, il convient de transférer le fichier local **.ssh/id_ecdsa.pub** du «client» vers le «serveur» en le renommant en **authorized_keys** :

```
[trainee@centos7 ~]$ scp .ssh/id_ecdsa.pub trainee@127.0.0.1:/home/trainee/.ssh/authorized_keys
trainee@127.0.0.1's password: trainee
id_ecdsa.pub                                                                                  100%  227
0.2KB/s   00:00
```

Connectez-vous via ssh et insérer les clefs publiques restantes dans le fichier .ssh/authorized_keys :

```
root@centos7 ~]# ssh -l trainee localhost
trainee@localhost's password: trainee
Last login: Tue May 10 01:39:33 2016 from localhost.localdomain
[trainee@centos7 ~]$ cat .ssh/id_rsa.pub >> .ssh/authorized_keys
[trainee@centos7 ~]$ cat .ssh/id_dsa.pub >> .ssh/authorized_keys
[trainee@centos7 ~]$ cat .ssh/id_ed25519.pub >> .ssh/authorized_keys
[trainee@centos7 ~]$ cat .ssh/authorized_keys
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG5BtOMFLrUbxD//RLELvkkA06CQvXuJqKSjSB2dlUXgaPyEJXuwHO0pxcdbr
g4qqb0f9sE75oMVowXxYgqhWDE= trainee@centos7.fenestros.loc
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC9KOuEH5+kyihhm99Na8UTA4Gi5AfiOVeJyS3UzH7ta73ewmv7JZqaXzar1NlHcpEMkCUs2yKxHyO/yAfjb
CSdow5vfwJiuJTes+HbpvsJqKp1+OR7tf+OMgjDcajoGi7DYuybIs9QrbWgh57QclbldHQXRO+xbeUTykxcRun7AvR5uWZe4zMooBAmVVEms+l1rn
8CUi+D811jqQGSpU39PxkojTAwgbxlevT/Twy4sfeRR47UHc3AbrHb8SgyKqbx5/S9UxkbkhJjckx0s58fnAwf9nX5rKE7RdCQisRvdLeLHozq3EO
omvc7kzejefBtUDWxBEjnSeAgIP3+OEQl trainee@centos7.fenestros.loc
ssh-dss
AAAAB3NzaC1kc3MAAACBAK9/4siucBnf/NAHBMjZWIx1coA/wYVBjfudVyKArip1fVUuYqf0Ri9vTorG8KJ2zzLRbW5z7V5ZDSn4f6P5Kv7K5xVPn
e9dYQHxImkZIljpFseUW56BwCvcgTNZVLD0tYZzF+B0/Py4waJW+pnTDfZush6DYyAhVnEuxIPI4i+PAAAAFQCeCZyDRo1o41lf19qWGJTG7W+ChQ
AAAIAKtQe9QlkW4CA9kP+q4v3N07WR5TzWsvfZARjGXgrSqTo0BeQgMLwRJHeEOhdsgJ30cNbl6QXlB4G4J6dUoTiN/sY1dFbXzjzsT/MHLedsllV
fXXRQxgvN2nsbsKEUnmqEBWzgw5s6KOkGX33+0Six0E3xvOrYxkMNLP/5VT4aQwAAAIEAmOS94peBeo78yCKzCvSFnEL72dUCFFA6CGFGqgffhK1v
P5H5pG5vQxzBn9NnIXURCACF7ZxtZaxohSoB1M0/s0DfrfNIvXRMGvsJpZ9B2psTMDl9qBffIfIARnwkWKG1gC/lWaovUpDByE1wl09ZCDCnZp/16
ULJY0zvJ566Seg= trainee@centos7.fenestros.loc
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIENas3A3hmXFj1cb+lrn2NAt6g95Pla6qUFQHd1wg2y1 trainee@centos7.fenestros.loc
ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBG5BtOMFLrUbxD//RLELvkkA06CQvXuJqKSjSB2dlUXgaPyEJXuwHO0pxcdbr
```

```
g4qqb0f9sE75oMVowXxYgqhWDE= trainee@centos7.fenestros.loc
```

Lors de la connexion suivante au serveur, l'authentification utilise le couple de clefs asymétrique et aucun mot de passe n'est requis :

```
[trainee@centos7 ~]$ ssh -l trainee localhost
Last login: Tue May 10 01:50:39 2016 from localhost.localdomain
[trainee@centos7 ~]$ exit
déconnexion
Connection to localhost closed.
```

Important - Le fichier **authorized_keys** doit avoir les permissions de 600.

LAB #6 - Mise en place d'un VPN avec OpenVPN

6.1 - Présentation

OpenVPN permet à des pairs de s'authentifier entre eux à l'aide :

- d'une **clé privée partagée** à l'avance,
- de **certificats** ou,
- à partir de la version 2.0 et à condition que le serveur possède un certificat, de **couples de noms d'utilisateur/mot de passe** sans besoin d'un certificat client

OpenVPN :

- utilise de manière intensive la bibliothèque d'authentification **OpenSSL** ainsi que le protocole **SSLv3/TLSv1**,
- n'est pas compatible avec IPsec ou d'autres logiciels VPN.

6.2 - Configuration commune au client et au serveur

Commencez par vérifiez si le paquet **openssl** est bien installé :

```
[root@centos7 ~]# rpm -q openssl
openssl-1.0.2k-8.el7.x86_64
```

Installez ensuite le paquet openvpn :

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

Naviguez au répertoire **/etc/openvpn** et créez la clef partagée :

```
[root@centos7 ~]# cd /etc/openvpn/
[root@centos7 openvpn]# openvpn --genkey --secret static.key
[root@centos7 openvpn]# cat static.key
#
# 2048 bit OpenVPN static key
#
-----BEGIN OpenVPN Static key V1-----
54f96ea50dbef7d5341efeda459b05ad
5af134bf915bbd867fdd6310f4f0b72b
331a82cdc6080622a7861e8c30cd0ffb
6b35c143e5c715077247270bdb610fc8
4c536f34742ba23f2bfe9ab148b3fa04
20d1f6e5a20d58db30cce56ce1ca5744
3028353a7e5e47b3f630738b71b04a1e
e388b5e986826ce481ff457157b3492e
61c147cd3d4373e283ad91c8ac44c0e8
3b593d342cd0a2600db7b3e7cd0efa89
d38dd861c1e4fc566e5e50004b102c7f
b444795e2691cd59dfbb51e79996339d
7e54d002aa4d5c63b3c155fbcc20f696
```

```
fe148128f2e94e509c39c72c117a684b
9fa8c7e159c451a7c52f42b2260d62c9
586d66a454319ba538559c143643e434
-----END OpenVPN Static key V1-----
```

L'architecture réseau sera donc la suivante :

```
                                  serveur <-----------------VPN-----------------> client
                                  10.0.0.1                                       10.0.0.2
                                   tun0                                            tun0
                                     |                                               |
                                     |                                               |
                                   eth0                                            eth0
                                 10.0.2.51  <-------------Réseau------------->   10.0.2.71
```

←———Votre réseau———→

6.3 - Configuration du client

Créez le fichier **/etc/openvpn/client.conf** :

```
[root@centos7 ~]# vi /etc/openvpn/client.conf
[root@centos7 ~]# cat /etc/openvpn/client.conf
remote 10.0.2.51
dev tun
port 1194
proto udp
comp-lzo
ifconfig 10.0.0.2 10.0.0.1
secret /etc/openvpn/static.key
```

Important - Trouvez la signification de chacune des directives dans ce fichier.

Arrêtez le service **firewalld** :

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

Lancez openvpn en ligne de commande et en arrière plan en spécifiant une journalisation :

```
[root@centos7 ~]# openvpn --config /etc/openvpn/client.conf > /var/log/vpn 2>&1 &
```

Vérifiez ensuite que le **socket** d'openvpn soit ouvert :

```
[root@centos7 ~]# netstat -an | grep 1194
udp        0      0 0.0.0.0:1194                0.0.0.0:*
```

Constatez ensuite la table de routage :

```
[root@centos7 ~]# netstat -ar
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Fenêtre irtt Iface
default         gateway         0.0.0.0         UG        0 0          0 eth0
10.0.0.1        0.0.0.0         255.255.255.255 UH        0 0          0 tun0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

Notez la présence de la route via **tun0**.

Constatez ensuite le montage du tunnel en regardant le contenu du fichier de journalisation **/var/log/vpn** :

```
[root@centos7 ~]# tail /var/log/vpn
```

6.4 - Configuration du serveur

Créez le fichier **/etc/openvpn/server.conf** :

```
[root@centos7 ~]# vi /etc/openvpn/server.conf
[root@centos7 ~]# cat /etc/openvpn/server.conf
dev tun
ifconfig 10.0.0.1 10.0.0.2
secret /etc/openvpn/static.key
port 1194
proto udp
user nobody
group nobody
daemon
comp-lzo
keepalive 10 60
ping-timer-rem
persist-tun
persist-key
log /var/log/vpn
verb 1
```

Important - Trouvez la signification de chacune des directives dans ce fichier.

Arrêtez le service **firewalld** :

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

Lancez openvpn en ligne de commande et en arrière plan en spécifiant une journalisation :

```
[root@centos7 ~]# openvpn --config /etc/openvpn/server.conf > /var/log/vpn 2>&1 &
[1] 7751
```

Vérifiez ensuite que le **socket** d'openvpn soit ouvert :

```
[root@centos7 ~]# netstat -an | grep 1194
udp        0      0 0.0.0.0:1194                0.0.0.0:*
```

Constatez ensuite la table de routage :

```
[root@centos7 ~]# netstat -ar
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Fenêtre irtt Iface
0.0.0.0         10.0.2.1        0.0.0.0         UG        0 0          0 eth0
10.0.0.1        0.0.0.0         255.255.255.255 UH        0 0          0 tun0
10.0.2.0        0.0.0.0         255.255.255.0   U         0 0          0 eth0
```

Constatez ensuite le montage du tunnel en regardant le contenu du fichier de journalisation **/var/log/vpn** :

```
[root@centos7 ~]# tail /var/log/vpn
```

6.5 - Tests

Du client vers le serveur

Sur le client, utilisez la commande ping pour envoyer des paquets dans le tunnel :

```
[root@centos6 ~]# ping -c3 10.0.0.1
PING 10.0.0.1 (10.0.0.1) 56(84) bytes of data.
64 bytes from 10.0.0.1: icmp_seq=1 ttl=64 time=7.62 ms
64 bytes from 10.0.0.1: icmp_seq=2 ttl=64 time=1.35 ms
```

```
64 bytes from 10.0.0.1: icmp_seq=3 ttl=64 time=0.000 ms

--- 10.0.0.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2047ms
rtt min/avg/max/mdev = 0.000/2.994/7.629/3.323 ms
```

Du serveur vers le client

Sur le serveur, utilisez la commande ping pour envoyer des paquets dans le tunnel :

```
[root@centos7 ~]# ping -c5 10.0.0.2
PING 10.0.0.2 (10.0.0.2) 56(84) bytes of data.
64 bytes from 10.0.0.2: icmp_seq=1 ttl=64 time=2.59 ms
64 bytes from 10.0.0.2: icmp_seq=2 ttl=64 time=9.08 ms
64 bytes from 10.0.0.2: icmp_seq=3 ttl=64 time=7.24 ms
64 bytes from 10.0.0.2: icmp_seq=4 ttl=64 time=7.03 ms
64 bytes from 10.0.0.2: icmp_seq=5 ttl=64 time=4.08 ms

--- 10.0.0.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4034ms
rtt min/avg/max/mdev = 2.597/6.008/9.084/2.340 ms
```

LAB #7 - Le Serveur vsftpd

7.1 - Installation

Le paquet **vsftpd** *Very Secure FTP daemon* se trouve dans les dépôts CentOS.

```
[root@centos7 ~]# yum install ftp vsftpd -y
```

Par contre le service vsftpd n'est pas démarré par défaut :

```
[root@centos7 ~]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; disabled; vendor preset: disabled)
   Active: inactive (dead)
```

Configurez le service **vsftpd** pour que celui-ci soit activé :

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

Avant de poursuivre, modifiez le mode de **SELinux** de **enforced** à **permissive** pour la session en cours :

```
[root@centos7 ~]# setenforce permissive
[root@centos7 ~]# getenforce
Permissive
```

Ensuite éditez le fichier **/etc/selinux/config** ainsi :

```
[root@centos7 ~]# vi /etc/selinux/config
[root@centos7 ~]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.
# SELINUX= can take one of these three values:
#     enforcing - SELinux security policy is enforced.
#     permissive - SELinux prints warnings instead of enforcing.
#     disabled - No SELinux policy is loaded.
SELINUX=permissive
# SELINUXTYPE= can take one of three two values:
#     targeted - Targeted processes are protected,
#     minimum - Modification of targeted policy. Only selected processes are protected.
#     mls - Multi Level Security protection.
```

```
SELINUXTYPE=targeted
```

7.2 - Configuration de base

Le fichier de configuration de vsftpd est **/etc/vsftpd/vsftpd.conf** :

```
[root@centos7 ~]# cat /etc/vsftpd/vsftpd.conf
# Example config file /etc/vsftpd/vsftpd.conf
#
# The default compiled in settings are fairly paranoid. This sample file
# loosens things up a bit, to make the ftp daemon more usable.
# Please see vsftpd.conf.5 for all compiled in defaults.
#
# READ THIS: This example file is NOT an exhaustive list of vsftpd options.
# Please read the vsftpd.conf.5 manual page to get a full idea of vsftpd's
# capabilities.
#
# Allow anonymous FTP? (Beware - allowed by default if you comment this out).
anonymous_enable=YES
#
# Uncomment this to allow local users to log in.
# When SELinux is enforcing check for SE bool ftp_home_dir
local_enable=YES
#
# Uncomment this to enable any form of FTP write command.
write_enable=YES
#
# Default umask for local users is 077. You may wish to change this to 022,
# if your users expect that (022 is used by most other ftpd's)
local_umask=022
#
# Uncomment this to allow the anonymous FTP user to upload files. This only
# has an effect if the above global write enable is activated. Also, you will
```

```
# obviously need to create a directory writable by the FTP user.
# When SELinux is enforcing check for SE bool allow_ftpd_anon_write, allow_ftpd_full_access
#anon_upload_enable=YES
#
# Uncomment this if you want the anonymous FTP user to be able to create
# new directories.
#anon_mkdir_write_enable=YES
#
# Activate directory messages - messages given to remote users when they
# go into a certain directory.
dirmessage_enable=YES
#
# Activate logging of uploads/downloads.
xferlog_enable=YES
#
# Make sure PORT transfer connections originate from port 20 (ftp-data).
connect_from_port_20=YES
#
# If you want, you can arrange for uploaded anonymous files to be owned by
# a different user. Note! Using "root" for uploaded files is not
# recommended!
#chown_uploads=YES
#chown_username=whoever
#
# You may override where the log file goes if you like. The default is shown
# below.
#xferlog_file=/var/log/xferlog
#
# If you want, you can have your log file in standard ftpd xferlog format.
# Note that the default log file location is /var/log/xferlog in this case.
xferlog_std_format=YES
#
# You may change the default value for timing out an idle session.
#idle_session_timeout=600
```

```
#
# You may change the default value for timing out a data connection.
#data_connection_timeout=120
#
# It is recommended that you define on your system a unique user which the
# ftp server can use as a totally isolated and unprivileged user.
#nopriv_user=ftpsecure
#
# Enable this and the server will recognise asynchronous ABOR requests. Not
# recommended for security (the code is non-trivial). Not enabling it,
# however, may confuse older FTP clients.
#async_abor_enable=YES
#
# By default the server will pretend to allow ASCII mode but in fact ignore
# the request. Turn on the below options to have the server actually do ASCII
# mangling on files when in ASCII mode. The vsftpd.conf(5) man page explains
# the behaviour when these options are disabled.
# Beware that on some FTP servers, ASCII support allows a denial of service
# attack (DoS) via the command "SIZE /big/file" in ASCII mode. vsftpd
# predicted this attack and has always been safe, reporting the size of the
# raw file.
# ASCII mangling is a horrible feature of the protocol.
#ascii_upload_enable=YES
#ascii_download_enable=YES
#
# You may fully customise the login banner string:
#ftpd_banner=Welcome to blah FTP service.
#
# You may specify a file of disallowed anonymous e-mail addresses. Apparently
# useful for combatting certain DoS attacks.
#deny_email_enable=YES
# (default follows)
#banned_email_file=/etc/vsftpd/banned_emails
#
```

```
# You may specify an explicit list of local users to chroot() to their home
# directory. If chroot_local_user is YES, then this list becomes a list of
# users to NOT chroot().
# (Warning! chroot'ing can be very dangerous. If using chroot, make sure that
# the user does not have write access to the top level directory within the
# chroot)
#chroot_local_user=YES
#chroot_list_enable=YES
# (default follows)
#chroot_list_file=/etc/vsftpd/chroot_list
#
# You may activate the "-R" option to the builtin ls. This is disabled by
# default to avoid remote users being able to cause excessive I/O on large
# sites. However, some broken FTP clients such as "ncftp" and "mirror" assume
# the presence of the "-R" option, so there is a strong case for enabling it.
#ls_recurse_enable=YES
#
# When "listen" directive is enabled, vsftpd runs in standalone mode and
# listens on IPv4 sockets. This directive cannot be used in conjunction
# with the listen_ipv6 directive.
listen=NO
#
# This directive enables listening on IPv6 sockets. By default, listening
# on the IPv6 "any" address (::) will accept connections from both IPv6
# and IPv4 clients. It is not necessary to listen on *both* IPv4 and IPv6
# sockets. If you want that (perhaps because you want to listen on specific
# addresses) then you must run two copies of vsftpd with two configuration
# files.
# Make sure, that one of the listen options is commented !!
listen_ipv6=YES

pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

Les directives actives de ce fichier sont :

cd /tmp ; grep -E -v '^(#|$)' /etc/vsftpd/vsftpd.conf > vsftpd.conf

```
[root@centos7 ~]# cd /tmp ; grep -E -v '^(#|$)'  /etc/vsftpd/vsftpd.conf > vsftpd.conf[root@centos7 tmp]# cat
vsftpd.conf
anonymous_enable=YES
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=NO
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
```

Ces directives sont détaillées ci-après :

Directive	**Valeur par Défaut**	**Description**
anonymous_enable	YES	Si oui, autorise les connexions anonymes
local_enable	YES	Si oui, autorise des connexions par des utilisateurs ayant un compte valide sur le système
write_enable	YES	Si oui, permet l'écriture
local_umask	022	Spécifie la valeur de l'umask lors de la création de fichiers et de répertoires
dirmessage_enable	NO	Si oui, permet d'afficher le contenu du fichier .message quand un utilisateur rentre dans le répertoire
xferlog_enable	NO	Si oui, permet d'activer la journalisation dans le fichier **/var/log/vsftpd.log**
connect_from_port_20	NO	Permet les connexions de ftp-data
listen	NO	Si oui, vfsftpd fonctionne en mode Standalone et non en tant que sous-service de xinetd

Directive	Valeur par Défaut	Description
pam_service_name	S/O	Indique le nom du service PAM utilisé par vsftpd
userlist_enable	NO	Si oui, vsftpd charge une liste d'utilisateurs spécifiés dans le fichier identifié par la directive **userlist_file**. Si un utilisateur spécifié dans la liste essaie de se connecter, la connexion sera réfusée avant la demande d'un mot de passe
tcp_wrappers	NO	Si oui, vsftpd utilise TCP WRAPPERS

7.3 - /etc/ftpusers

Votre serveur FTP est maintenant configuré pour les connexions en provenance des utilisateurs ayant un compte sur votre système.

Dans le cas où vous souhaiteriez **interdire** la connexion vers le serveur de certaines personnes mais pas de toutes les personnes ayant un compte système, créez le fichier **/etc/ftpusers**.

Voici la liste des utilisateurs système qu'il convient d'ajouter à ce fichier:

```
[root@centos7 tmp]# vi /etc/ftpusers
[root@centos7 tmp]# cat /etc/ftpusers
root
bin
daemon
adm
lp
sync
shutdown
halt
mail
uucp
operator
gopher
nobody
dbus
vcsa
```

```
rpc
nscd
tcpdump
haldaemon
apache
nslcd
postfix
avahi
ntp
rpcuser
sshd
gdm
vboxadd
named
```

Il est ensuite nécessaire d'inclure la directive **userlist_file=/etc/ftpusers** dans le fichier /etc/vsftpd/vsftpd.conf :

```
[root@centos7 tmp]# vi vsftpd.conf
[root@centos7 tmp]# cat vsftpd.conf
anonymous_enable=YES
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=NO
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
userlist_file=/etc/ftpusers
```

et de démarrer le serveur :

```
[root@centos7 tmp]# cp /etc/vsftpd/vsftpd.conf /root

[root@centos7 tmp]# rm -rf /etc/vsftpd/vsftpd.conf

[root@centos7 tmp]# cp /tmp/vsftpd.conf /etc/vsftpd/

[root@centos7 tmp]# systemctl start vsftpd

[root@centos7 tmp]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-11-24 09:52:28 CET; 8s ago
  Process: 11865 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
 Main PID: 11867 (vsftpd)
   CGroup: /system.slice/vsftpd.service
           └─11867 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Nov 24 09:52:28 centos7.fenestros.com systemd[1]: Starting Vsftpd ftp daemon...
Nov 24 09:52:28 centos7.fenestros.com systemd[1]: Started Vsftpd ftp daemon.
```

Testez maintenant le serveur :

```
[root@centos7 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 3.0.2)
Name (localhost:root): trainee
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
```

```
257 "/home/trainee"
ftp> exit
221 Goodbye.
```

Bien que trainee puisse se connecter, ce n'est pas le cas pour **root** :

```
[root@centos7 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 3.0.2)
Name (localhost:root): root
530 Permission denied.
Login failed.
ftp> pwd
530 Please login with USER and PASS.
ftp> exit
221 Goodbye.
```

Pour **chrooter** l'utilisateur dans son répertoire personnel, il convient d'ajouter les directives **chroot_local_user=YES** et **allow_writeable_chroot=YES** au fichier /etc/vsftpd/vsftpd.conf :

```
[root@centos7 ~]# vi /etc/vsftpd/vsftpd.conf
[root@centos7 ~]# cat /etc/vsftpd/vsftpd.conf
anonymous_enable=YES
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=NO
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
```

```
tcp_wrappers=YES
userlist_file=/etc/ftpusers
chroot_local_user=YES
allow_writeable_chroot=YES
```

et de redémarrer le serveur :

```
[root@centos7 ~]# systemctl restart vsftpd
[root@centos7 ~]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-11-24 11:00:09 CET; 6s ago
  Process: 604 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
 Main PID: 606 (vsftpd)
   CGroup: /system.slice/vsftpd.service
           └─606 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Nov 24 11:00:08 centos7.fenestros.com systemd[1]: Stopped Vsftpd ftp daemon.
Nov 24 11:00:08 centos7.fenestros.com systemd[1]: Starting Vsftpd ftp daemon...
Nov 24 11:00:09 centos7.fenestros.com systemd[1]: Started Vsftpd ftp daemon.
```

Lors de sa prochaine connexion, l'utilisateur voit son répertoire personnel comme la racine du système de fichiers :

```
[root@centos7 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 3.0.2)
Name (localhost:root): trainee
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
```

```
ftp> exit
221 Goodbye.
```

7.4 - Serveur vsftpd Anonyme

Configuration

Le serveur anonyme étant déjà configuré par la présence de la directive **anonymous_enable=YES**, il convient de tester celui-ci :

```
[root@centos7 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 3.0.2)
Name (localhost:root): anonymous
331 Please specify the password.
Password: <tapez n'importe quel texte ici>
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> ls
227 Entering Passive Mode (127,0,0,1,164,111).
150 Here comes the directory listing.
drwxr-xr-x    2 0        0               6 Jun 09  2021 pub
226 Directory send OK.
ftp> quit
221 Goodbye.
```

Le répertoire pour les connexions anonymes est **/var/ftp** :

```
[root@centos7 ~]# ls -l /var | grep ftp

```

```
drwxr-xr-x.  3 root root    16 Nov 24 09:39 ftp
```

Par défaut il contient un répertoire **pub** :

```
[root@centos7 ~]# ls -l /var/ftp
total 0
drwxr-xr-x. 2 root root 6 Jun  9  2021 pub
```

Pour permettre aux utilisateurs anonymes de transférer des fichiers vers le serveur, il faut d'abord créer un répertoire **upload** dans **/var/ftp/pub** et de l'affecter à ftp:ftp :

```
[root@centos7 ~]# mkdir /var/ftp/pub/upload
[root@centos7 ~]# chown ftp:ftp /var/ftp/pub/upload
```

Ensuite il faut ajouter la directive **anon_upload_enable=YES** au fichier **/etc/vsftpd/vsftpd.conf** :

```
[root@centos7 ~]# vi /etc/vsftpd/vsftpd.conf
[root@centos7 ~]# cat /etc/vsftpd/vsftpd.conf
anonymous_enable=YES
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
listen=NO
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
userlist_file=/etc/ftpusers
chroot_local_user=YES
allow_writeable_chroot=YES
```

```
anon_upload_enable=YES
```

Redémarrez le serveur vsftpd :

```
[root@centos7 ~]# systemctl restart vsftpd
[root@centos7 ~]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-11-24 11:14:45 CET; 7s ago
  Process: 5385 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
 Main PID: 5387 (vsftpd)
   CGroup: /system.slice/vsftpd.service
           └─5387 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Nov 24 11:14:45 centos7.fenestros.com systemd[1]: Stopped Vsftpd ftp daemon.
Nov 24 11:14:45 centos7.fenestros.com systemd[1]: Starting Vsftpd ftp daemon...
Nov 24 11:14:45 centos7.fenestros.com systemd[1]: Started Vsftpd ftp daemon.
```

Testez ensuite votre configuration :

```
[root@centos7 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 3.0.2)
Name (localhost:root): ftp
331 Please specify the password.
Password: <tapez n'importe quel texte ici>
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd pub/upload
250 Directory successfully changed.
ftp> pwd
257 "/pub/upload"
ftp> put rndc.key
```

```
local: rndc.key remote: rndc.key
227 Entering Passive Mode (127,0,0,1,31,174).
150 Ok to send data.
226 Transfer complete.
77 bytes sent in 0.00904 secs (8.51 Kbytes/sec)
ftp> ls
227 Entering Passive Mode (127,0,0,1,99,12).
150 Here comes the directory listing.
-rw-------    1 14       50             77 Nov 24 10:16 rndc.key
226 Directory send OK.
ftp> quit
221 Goodbye.
```

7.5 - Serveur vsftpd et Utilisateurs Virtuels

Présentation

Le serveur vsftpd utilise le système PAM pour gérer les authentifications. Le module concerné est **pam_userdb**. Ce module consulte une base de données au format Berkeley pour obtenir les coordonnées de connexion des utilisateurs.

Configuration

Pour configurer des utilisateurs virtuels, il convient de créer un fichier de configuration à part, **/root/vftpusers** , dans lequel on inscrit le nom et le mot de passe des utilisateurs virtuels :

```
[root@centos7 ~]# vi /root/vftpusers
[root@centos7 ~]# cat /root/vftpusers
mila
123456789
```

Ce fichier doit ensuite être converti au format Berkeley :

```
[root@centos7 ~]# db_load -T -t hash -f /root/vftpusers /etc/vsftpd/vftpusers.db
```

Modifiez ensuite les permissions sur le fichier **/etc/vsftpd/vftpusers.db** et supprimez le fichier **/root/vftpusers** :

```
[root@centos7 ~]# chmod 600 /etc/vsftpd/vftpusers.db
[root@centos7 ~]# rm -f /root/vftpusers
```

Créez ensuite un fichier PAM **/etc/pam.d/vftpusers** :

```
[root@centos7 ~]# vi /etc/pam.d/vftpusers
[root@centos7 ~]# cat /etc/pam.d/vftpusers
#%PAM-1.0
auth    required        pam_userdb.so   db=/etc/vsftpd/vftpusers
account required        pam_userdb.so   db=/etc/vsftpd/vftpusers
session required        pam_loginuid.so
```

Important - Notez que **pam_userdb.so** ajoute automatiquement l'extension **.db** aux noms des fichiers de base de données.

Modifiez maintenant le fichier /etc/vsftpd/vsftpd.conf :

```
[root@centos7 ~]# vi /etc/vsftpd/vsftpd.conf
[root@centos7 ~]# cat /etc/vsftpd/vsftpd.conf
anonymous_enable=YES
local_enable=YES
write_enable=YES
local_umask=022
dirmessage_enable=YES
xferlog_enable=YES
connect_from_port_20=YES
xferlog_std_format=YES
```

```
listen=NO
listen_ipv6=YES
pam_service_name=vsftpd
userlist_enable=YES
tcp_wrappers=YES
userlist_file=/etc/ftpusers
chroot_local_user=YES
allow_writeable_chroot=YES
anon_upload_enable=YES
pam_service_name=vftpusers
guest_enable=YES
guest_username=ftp
virtual_use_local_privs=YES
```

>

Redémarrez le service vsftpd :

```
[root@centos7 ~]# systemctl restart vsftpd
[root@centos7 ~]# systemctl status vsftpd
● vsftpd.service - Vsftpd ftp daemon
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Thu 2022-11-24 11:37:04 CET; 7s ago
  Process: 12206 ExecStart=/usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf (code=exited, status=0/SUCCESS)
 Main PID: 12209 (vsftpd)
   CGroup: /system.slice/vsftpd.service
           └─12209 /usr/sbin/vsftpd /etc/vsftpd/vsftpd.conf

Nov 24 11:37:04 centos7.fenestros.com systemd[1]: Stopped Vsftpd ftp daemon.
Nov 24 11:37:04 centos7.fenestros.com systemd[1]: Starting Vsftpd ftp daemon...
Nov 24 11:37:04 centos7.fenestros.com systemd[1]: Started Vsftpd ftp daemon.
```

Testez ensuite la configuration :

```
[root@centos7 ~]# ftp localhost
Connected to localhost (127.0.0.1).
220 (vsFTPd 3.0.2)
Name (localhost:root): mila
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> pwd
257 "/"
ftp> quit
221 Goodbye.
```

Important - Notez que les utilisateurs virtuels atterrissent dans le répertoire personnel du compte indiqué par la directive **guest_username** du fichier **/etc/vsftpd/vsftpd.conf**.

LAB #8 - OpenVAS

8.1 - Présentation

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

8.2 - 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
```

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
```

8.3 - Installation

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

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

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

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

8.4 - 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.
```

Installez donc **redis** :

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

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

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

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

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

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

Activez et démarrez le service **redis** :

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

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

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

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

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

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

```
[root@centos7 ~]# wget https://www.dropbox.com/s/j3ulbuzqtrd7r9d/greenbone-nvt-sync
```

Rendez le script exécutable :

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

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

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

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

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

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

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

Vérifiez ensuite la réussite de la commande précédente :

```
[root@centos7 ~]# ls -l /var/lib/openvas/plugins/ | more
total 36288
drwxr-xr-x   2 trainee trainee   32768 Mar  3 11:33 2008
drwxr-xr-x   2 trainee trainee   77824 Mar  3 11:33 2009
drwxr-xr-x   2 trainee trainee   77824 Mar  4 10:59 2010
drwxr-xr-x   2 trainee trainee  253952 Mar  3 11:33 2011
drwxr-xr-x   2 trainee trainee  307200 Mar  3 11:33 2012
drwxr-xr-x   3 trainee trainee  266240 Mar  3 11:33 2013
drwxr-xr-x   3 trainee trainee  249856 Mar  3 11:33 2014
drwxr-xr-x   3 trainee trainee  401408 Mar  3 11:33 2015
drwxr-xr-x   3 trainee trainee  389120 Mar  4 10:59 2016
drwxr-xr-x  64 trainee trainee  282624 Mar  3 11:33 2017
drwxr-xr-x 289 trainee trainee   12288 Feb 16 12:02 2018
drwxr-xr-x 214 trainee trainee   12288 Nov 25 11:24 2019
drwxr-xr-x 180 trainee trainee    4096 Jan 25 11:10 2020
drwxr-xr-x  72 trainee trainee    4096 Mar  4 10:59 2021
-rw-r--r--   1 trainee trainee    3470 Jul 20  2020 404.inc
-rw-r--r--   1 trainee trainee    3012 Dec  9 10:01 aas_detect.nasl
-rw-r--r--   1 trainee trainee    3166 Aug 27  2020 adaptbb_detect.nasl
-rw-r--r--   1 trainee trainee    4016 Aug 27  2020 AfterLogic_WebMail_Pro_detect.nasl
-rw-r--r--   1 trainee trainee    3176 Nov 12 11:33 amanda_detect.nasl
```

```
-rw-r--r--   1 trainee trainee    3173 Nov 12 11:33 amanda_version.nasl
-rw-r--r--   1 trainee trainee    3549 Mar  1 11:32 apache_server_info.nasl
-rw-r--r--   1 trainee trainee    7491 Mar  4 10:59 apache_SSL_complain.nasl
-rw-r--r--   1 trainee trainee    4679 Nov 12 11:33 apcnisd_detect.nasl
-rw-r--r--   1 trainee trainee    3303 Aug 27  2020 AproxEngine_detect.nasl
-rw-r--r--   1 trainee trainee    2706 Feb 14  2020 arcserve_backup_detect.nasl
-rw-r--r--   1 trainee trainee    2700 Mar  3 11:33 arkoon.nasl
-rw-r--r--   1 trainee trainee    7477 Nov 12 11:33 asip-status.nasl
-rw-r--r--   1 trainee trainee    4522 Aug 27  2020 atmail_detect.nasl
drwxr-xr-x   4 trainee trainee   20480 Mar  2 12:14 attic
-rw-r--r--   1 trainee trainee    2703 Nov 12 11:33 auth_enabled.nasl
-rw-r--r--   1 trainee trainee    2573 May  7  2020 aventail_asap.nasl
-rw-r--r--   1 trainee trainee    4620 Dec 21 15:00 awstats_detect.nasl
-rw-r--r--   1 trainee trainee    3711 Aug 27  2020 axigen_web_detect.nasl
-rw-r--r--   1 trainee trainee 1639798 Feb 14  2020 bad_dsa_ssh_host_keys.txt
--More--
```

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

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

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

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

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

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

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

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

```
[root@centos7 ~]# openvas-mkcert-client -i
This script will now ask you the relevant information to create the SSL client certificates for OpenVAS.

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

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

*********
Client certificates life time in days [3650]:
Country (two letter code) [UK]:
State or province name [SURREY]:
Location (e.g. town) [ADDLESTONE]:
```

```
Organization [I2TCH LIMITED]:
Organization unit [TRAINING]:
e-Mail []: infos@i2tch.eu
Generating RSA private key, 4096 bit long modulus
....++
.......++
e is 65537 (0x10001)
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [DE]:State or Province Name (full name) [Some-State]:Locality Name (eg, city)
[]:Organization Name (eg, company) [Internet Widgits Pty Ltd]:Organizational Unit Name (eg, section) []:Common
Name (eg, your name or your server's hostname) []:Email Address []:Using configuration from /tmp/openvas-mkcert-
client.13962/stdC.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'UK'
stateOrProvinceName   :ASN.1 12:'SURREY'
localityName          :ASN.1 12:'ADDLESTONE'
organizationName      :ASN.1 12:'I2TCH LIMITED'
organizationalUnitName:ASN.1 12:'TRAINING'
commonName            :ASN.1 12:'om'
emailAddress          :IA5STRING:'infos@i2tch.eu'
Certificate is to be certified until Jun 17 02:03:34 2028 GMT (3650 days)

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

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

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

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

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

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

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

```
   CGroup: /system.slice/openvas-scanner.service
           ├─16957 openvassd: Reloaded 200 of 45658 NVTs (0% / ETA: 26:31)
           └─16958 openvassd (Loading Handler)

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

Construisez maintenant la base de données :

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

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

```
[root@centos7 ~]# openvas-check-setup
...
Step 2: Checking OpenVAS Manager ...
        OK: OpenVAS Manager is present in version 6.0.9.
        OK: OpenVAS Manager client certificate is present as /etc/pki/openvas/CA/clientcert.pem.
        OK: OpenVAS Manager database found in /var/lib/openvas/mgr/tasks.db.
        OK: Access rights for the OpenVAS Manager database are correct.
        OK: sqlite3 found, extended checks of the OpenVAS Manager installation enabled.
        OK: OpenVAS Manager database is at revision 146.
        OK: OpenVAS Manager expects database at revision 146.
        OK: Database schema is up to date.
        OK: OpenVAS Manager database contains information about 45654 NVTs.
        ERROR: No users found. You need to create at least one user to log in.
        It is recommended to have at least one user with role Admin.
        FIX: create a user by running 'openvasmd --create-user=<name> --role=Admin && openvasmd --user=<name> --
new-password=<password>'
...
```

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

Créez donc un utilisateur :

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

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

```
[root@centos7 ~]# openvas-check-setup
...
Step 2: Checking OpenVAS Manager ...
        OK: OpenVAS Manager is present in version 6.0.9.
        OK: OpenVAS Manager client certificate is present as /etc/pki/openvas/CA/clientcert.pem.
        OK: OpenVAS Manager database found in /var/lib/openvas/mgr/tasks.db.
        OK: Access rights for the OpenVAS Manager database are correct.
        OK: sqlite3 found, extended checks of the OpenVAS Manager installation enabled.
        OK: OpenVAS Manager database is at revision 146.
        OK: OpenVAS Manager expects database at revision 146.
        OK: Database schema is up to date.
        OK: OpenVAS Manager database contains information about 45654 NVTs.
        OK: At least one user exists.
        ERROR: No OpenVAS SCAP database found. (Tried: /var/lib/openvas/scap-data/scap.db)
        FIX: Run a SCAP synchronization script like openvas-scapdata-sync or greenbone-scapdata-sync.

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

Important - Notez l'erreur **ERROR: No OpenVAS SCAP database**

found. (Tried: /var/lib/openvas/scap-data/scap.db).

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

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

```
[root@centos7 ~]# wget https://www.dropbox.com/s/c8pkgna4ez1h2cc/greenbone-feed-sync
```

Rendez le script exécutable :

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

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

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

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

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

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

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

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

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

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

Récupérer donc la base CERT :

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

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

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

```
        ERROR: Greenbone Security Assistant is NOT running!
        FIX: Start Greenbone Security Assistant (gsad).

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

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

Activer et démarrer OpenVAS Manager :

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

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

Activer et démarrer le Greenbone Security Assistant :

```
[root@centos7 ~]# systemctl enable openvas-gsa
```

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

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

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

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

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

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

Important - Notez les WARNINGS.

Installez les paquets suggérés :

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

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

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

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

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

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

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

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

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

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

```
Length: 10197 (10.0K) [text/plain]
Saving to: ‘comment.sty’

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

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

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

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

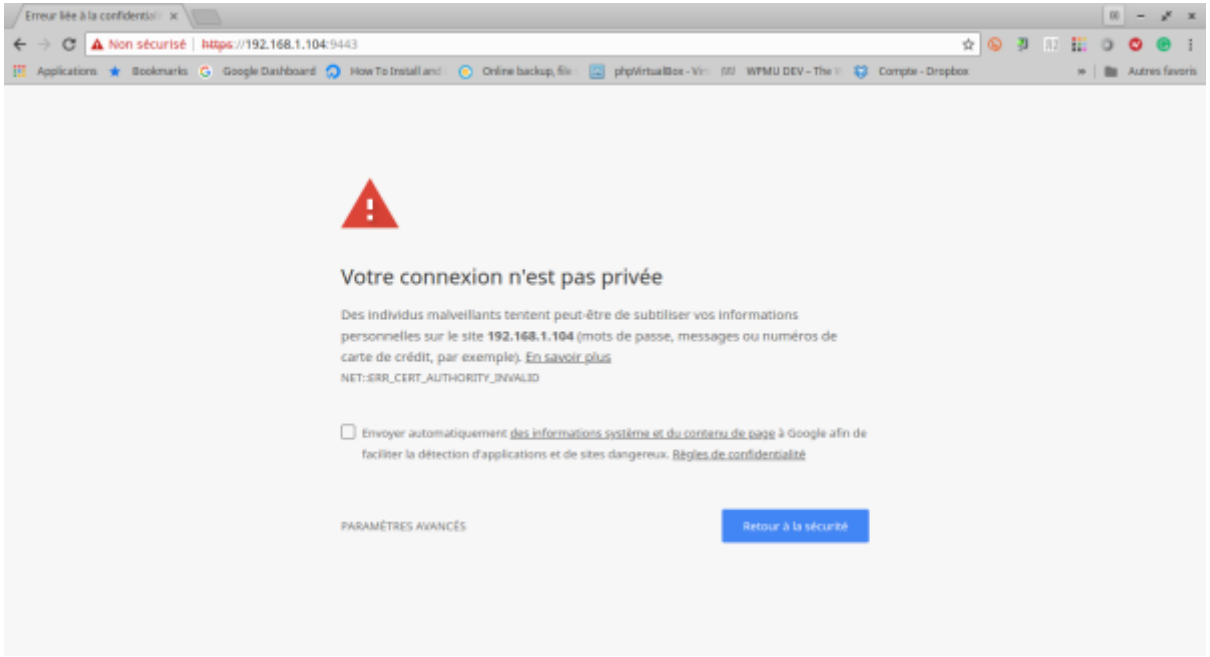
```
[root@centos7 ~]# openvas-check-setup
...
Step 10: Checking presence of optional tools ...
        OK: pdflatex found.
        OK: PDF generation successful. The PDF report format is likely to work.
        OK: ssh-keygen found, LSC credential generation for GNU/Linux targets is likely to work.
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

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

8.5 -Utilisation

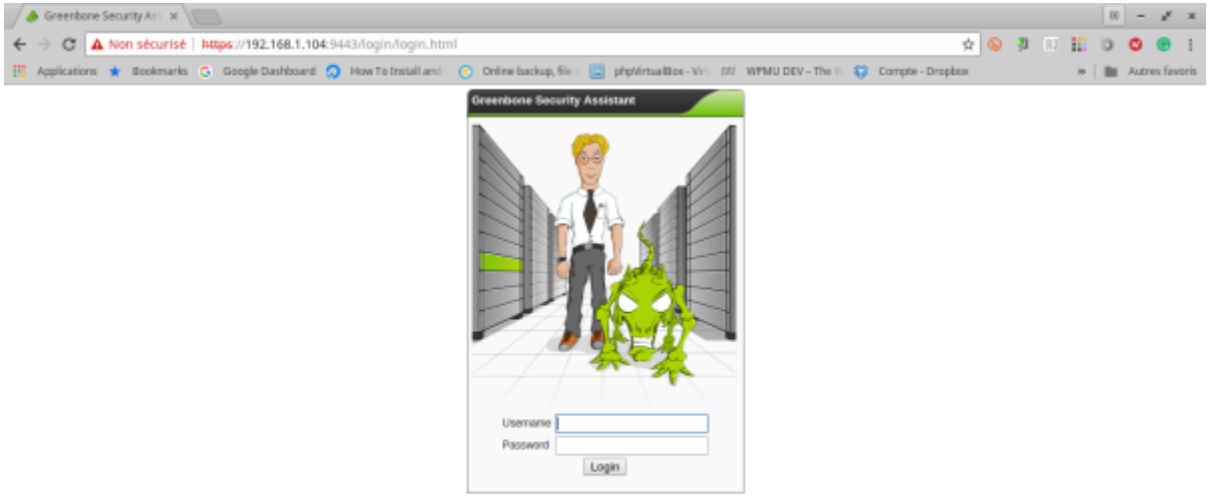
Passez votre VM en mode graphique :

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

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



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



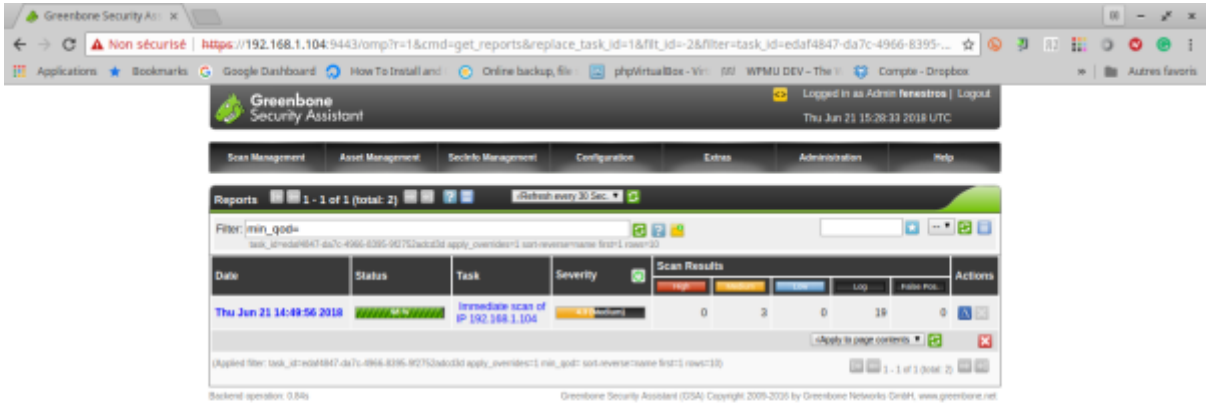
Entrez le nom de votre utilisateur ainsi que son mot de passe et cliquez sur le bouton **Login**. Vous obtiendrez une fenêtre similaire à celle-ci :

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

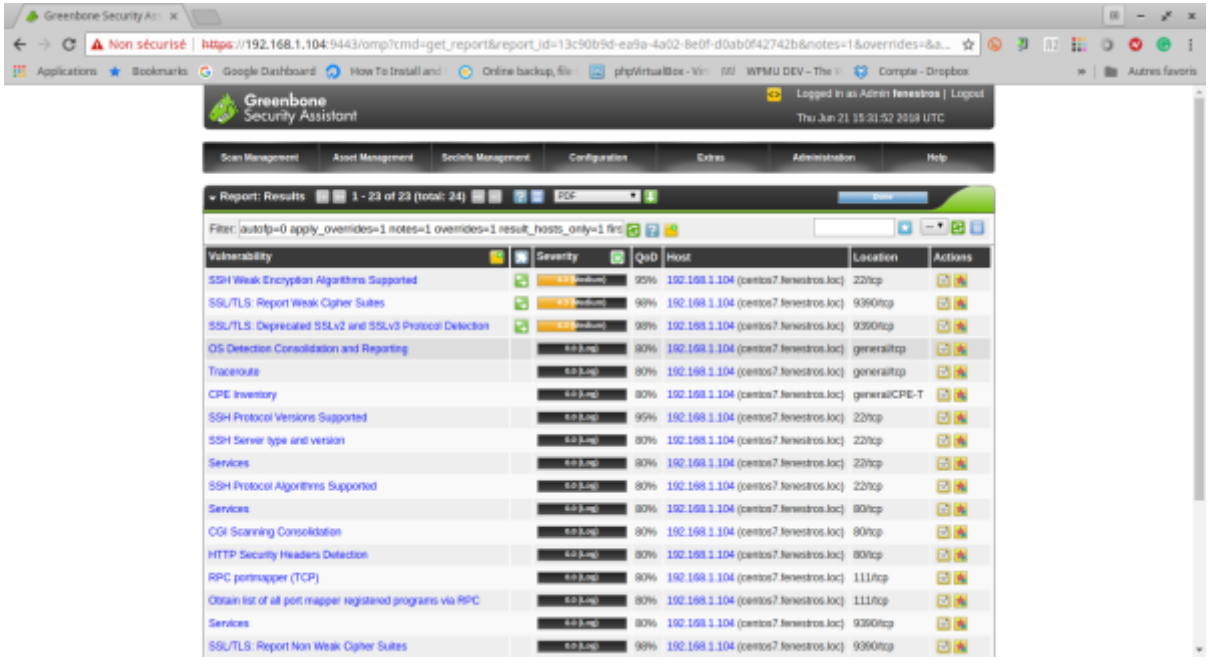
Important - Vous pouvez indiquer un réseau entier de la forme 10.0.2.0/24

Analyse des Résultats

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



ainsi que les détails de celui-ci :



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