Version : **2021.01**

Dernière mise-à-jour : 2023/02/15 15:56

LCF306 - Gestion de l'Authentification

Contenu du Module

- Utiliser la Commande Fail2Ban-server
- Ajouter un Prison

Le Problématique

Un pirate peut utiliser un logiciel de **crackage** pour tenter de découvrir un mot de passe. Le plus connu est **John The Ripper**.

Le principe de ces logiciels est simples - le logiciel utilise des dictionnaires de mots de passe qui sont utilisés le uns après les autres à une vitesse qui peut atteindre des milliers par seconde.

LAB #1 - John the Ripper

Installation

Créez le script suivant dans un terminal de RHEL/CentOS 7 en tant que root :

```
[trainee@centos7 ~]$ su -
Password: fenestros
Last login: Mon Apr 23 17:23:14 CEST 2018 on tty1
[root@centos7 ~]# vi john.sh
[root@centos7 ~]# cat john.sh
#!/bin/bash
# Centos 7 John the Ripper Installation
yum -y install wget gpgme
yum -y group install "Development Tools"
cd
wget http://www.openwall.com/john/j/john-1.8.0.tar.xz
wget http://www.openwall.com/john/j/john-1.8.0.tar.xz.sign
wget http://www.openwall.com/signatures/openwall-signatures.asc
gpg --import openwall-signatures.asc
```

```
gpg --verify john-1.8.0.tar.xz.sign
tar xvfJ john-1.8.0.tar.xz
cd john-1.8.0/src
make clean linux-x86-64
cd ../run/
./john --test
#password dictionnary download
wget -O - http://mirrors.kernel.org/openwall/wordlists/all.gz | gunzip -c > openwall.dico
```

Rendez-le exécutable :

```
[root@centos7 ~]# chmod u+x john.sh
```

Exécutez le script :

```
[root@centos7 ~]# ./john.sh
```

Utilisation

Placez-vous dans le répertoire **/root/john-1.8.0/run** :

```
[root@centos7 ~]# cd john-1.8.0/run/
```

Utilisez l'utilitare **unshadow** pour créer le fichier des mots de passe :

```
[root@centos7 run]# ./unshadow /etc/passwd /etc/shadow > mypasswd
```

Consultez le fichier **mypasswd** :

```
[root@centos7 run]# cat mypasswd
root:$6$TX12b5lW9UXD8Ld6$l/PjTA.XrBAbsayGCaSFaM5ibLo2xBBeYNCyEdVv9uMUctxq9Q0YBxLwCvS2bCdgr.BeSmXvi6BwD55KKscaJ.:0
:0:root:/root:/bin/bash
```

```
bin:*:1:1:bin:/bin:/sbin/nologin
daemon:*:2:2:daemon:/sbin:/sbin/nologin
adm:*:3:4:adm:/var/adm:/sbin/nologin
lp:*:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:*:5:0:sync:/sbin:/bin/sync
shutdown:*:6:0:shutdown:/sbin:/sbin/shutdown
halt:*:7:0:halt:/sbin:/sbin/halt
mail:*:8:12:mail:/var/spool/mail:/sbin/nologin
operator:*:11:0:operator:/root:/sbin/nologin
games:*:12:100:games:/usr/games:/sbin/nologin
ftp:*:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:*:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:!!:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
systemd-bus-proxy:!!:999:997:systemd Bus Proxy:/:/sbin/nologin
systemd-network:!!:998:996:systemd Network Management:/:/sbin/nologin
dbus:!!:81:81:System message bus:/:/sbin/nologin
polkitd:!!:997:995:User for polkitd:/:/sbin/nologin
abrt:!!:173:173::/etc/abrt:/sbin/nologin
usbmuxd:!!:113:113:usbmuxd user:/:/sbin/nologin
colord:!!:996:993:User for colord:/var/lib/colord:/sbin/nologin
libstoragemgmt:!!:995:992:daemon account for libstoragemgmt:/var/run/lsm:/sbin/nologin
setroubleshoot:!!:994:991::/var/lib/setroubleshoot:/sbin/nologin
rpc:!!:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
rtkit:!!:172:172:RealtimeKit:/proc:/sbin/nologin
chrony:!!:993:990::/var/lib/chrony:/sbin/nologin
unbound:!!:992:989:Unbound DNS resolver:/etc/unbound:/sbin/nologin
tss:!!:59:59:Account used by the trousers package to sandbox the tcsd daemon:/dev/null:/sbin/nologin
geoclue:!!:991:988:User for geoclue:/var/lib/geoclue:/sbin/nologin
ntp:!!:38:38::/etc/ntp:/sbin/nologin
sssd:!!:990:987:User for sssd:/:/sbin/nologin
rpcuser:!!:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:!!:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pulse:!!:171:171:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:!!:42:42::/var/lib/gdm:/sbin/nologin
```

```
gnome-initial-setup:!!:989:984::/run/gnome-initial-setup/:/sbin/nologin
avahi:!!:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
postfix:!!:89:89::/var/spool/postfix:/sbin/nologin
sshd:!!:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
tcpdump:!!:72:72::/:/sbin/nologin
trainee:$6$4PW9kfdOIOmWmSSO$8vikc1pyXgVc.C8xKP5EvIbBwe1fWd3DSvgWGQ5FAr7jwyMCbLQOOWbvomS9z1Q6V8IqZjBSREWafNzOYjKqC
0:1000:1000:trainee:/home/trainee:/bin/bash
vboxadd:!!:988:1::/var/run/vboxadd:/bin/false
```

Lancez **john** pour craquer le fichier **mypasswd** :

```
[root@centos7 run]# ./john mypasswd
Loaded 2 password hashes with 2 different salts (crypt, generic crypt(3) [?/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
trainee          (trainee)
1g 0:00:00:26 4% 2/3 0.03831g/s 230.1p/s 230.2c/s 230.2C/s Hanson..Kristine
1g 0:00:00:27 4% 2/3 0.03658g/s 230.3p/s 230.4c/s 230.4C/s Ruthless..Tanner
1g 0:00:00:28 4% 2/3 0.03549g/s 230.3p/s 230.3c/s 230.3C/s Bonjour..Blessing
1g 0:00:00:36 5% 2/3 0.02775g/s 230.6p/s 230.7c/s 230.7C/s dances..olivias
1g 0:00:01:14 10% 2/3 0.01348g/s 231.2p/s 231.2c/s 231.2C/s rabbitrabbit..dennisdennis
1g 0:00:01:16 11% 2/3 0.01311g/s 231.1p/s 231.2c/s 231.2C/s grahamgraham..sharkshark
1g 0:00:01:18 11% 2/3 0.01277g/s 231.2p/s 231.2c/s 231.2C/s reggiereggie..vickivicki
1g 0:00:01:19 11% 2/3 0.01263g/s 231.1p/s 231.1c/s 231.1C/s javierjavier..melvinmelvin
1g 0:00:01:20 12% 2/3 0.01244g/s 231.2p/s 231.2c/s 231.2C/s goldengolden..dixondixon
1g 0:00:01:21 12% 2/3 0.01231g/s 231.2p/s 231.2c/s 231.2C/s obiwanobiwan..bytemebyteme
1g 0:00:01:22 12% 2/3 0.01218g/s 231.1p/s 231.1c/s 231.1C/s suzysuzy..raeb
1g 0:00:01:23 12% 2/3 0.01200g/s 231.1p/s 231.2c/s 231.2C/s xilef..ognimalf
1g 0:00:01:24 12% 2/3 0.01188g/s 231.1p/s 231.2c/s 231.2C/s auhsoj..trebreh
1g 0:00:01:25 12% 2/3 0.01171g/s 231.2p/s 231.2c/s 231.2C/s namgib..lareneg
1g 0:00:02:34 21% 2/3 0.006482g/s 231.2p/s 231.2c/s 231.2C/s tinker3..ashraf3
[q] <------------------------------------------------------------------------------appuyez sur la touche
q
Use the "--show" option to display all of the cracked passwords reliably
```

```
Session aborted
```

Consultez la liste des mots de passe craqués :

```
[root@centos7 run]# ./john --show mypasswd
trainee:trainee:1000:1000:trainee:/home/trainee:/bin/bash

1 password hash cracked, 1 left
```

Surveillance Sécuritaire

La commande last

Cette commande indique les dates et heures des connexions des utilisateurs à partir du contenu du fichier **/var/log/wtmp** :

```
[root@centos7 ~]# last
trainee  pts/2        10.0.2.2         Tue Jun 19 18:47   still logged in
trainee  pts/0        10.0.2.2         Tue Jun 19 17:29 - 19:49  (02:20)
trainee  pts/0        2.2.0.10.rev.sfr Tue Jun 19 16:37 - 17:28  (00:51)
trainee  pts/1        2.2.0.10.rev.sfr Tue Jun 19 12:24 - 17:28  (05:04)
trainee  pts/0        10.0.2.2         Tue Jun 19 11:26 - 16:36  (05:10)
reboot   system boot  3.10.0-693.21.1. Tue Jun 19 11:25 - 01:03  (13:37)
trainee  tty1                          Mon Apr 23 17:23 - 17:25  (00:02)
reboot   system boot  3.10.0-693.21.1. Mon Apr 23 17:21 - 01:03 (57+07:41)
trainee  pts/0        10.0.2.2         Mon Apr 23 12:04 - 17:21  (05:16)
reboot   system boot  3.10.0-327.13.1. Mon Apr 23 12:03 - 17:21  (05:17)
reboot   system boot  3.10.0-327.13.1. Sat Apr 30 16:22 - 17:21 (723+00:59)
trainee  pts/0        2.2.0.10.rev.sfr Sat Apr 30 16:20 - 16:21  (00:00)
trainee  tty1                          Sat Apr 30 16:17 - 16:21  (00:03)
reboot   system boot  3.10.0-327.13.1. Sat Apr 30 16:17 - 16:21  (00:04)
trainee  pts/0        2.2.0.10.rev.sfr Sat Apr 30 16:11 - 16:17  (00:05)
```

```
trainee  tty1                         Sat Apr 30 16:08 - 16:17  (00:08)
reboot   system boot  3.10.0-327.13.1. Sat Apr 30 16:04 - 16:17  (00:13)
trainee  tty1                         Sat Apr 30 15:46 - 16:03  (00:16)
reboot   system boot  3.10.0-327.13.1. Sat Apr 30 15:32 - 16:03  (00:31)
trainee  pts/1        gateway         Sat Apr 30 15:35 - 15:40  (00:05)
trainee  pts/0        :0              Sat Apr 30 15:29 - 15:40  (00:10)
trainee  :0           :0              Sat Apr 30 15:29 - 15:40  (00:11)
(unknown :0           :0              Sat Apr 30 15:22 - 15:29  (00:06)
reboot   system boot  3.10.0-327.13.1. Sat Apr 30 15:21 - 15:40  (00:19)
trainee  pts/0        gateway         Sat Apr 30 15:12 - 15:27  (00:14)
trainee  tty1                         Sat Apr 30 14:19 - 15:27  (01:07)
reboot   system boot  3.10.0-327.el7.x Sat Apr 30 14:19 - 15:27  (01:07)
trainee  tty1                         Sat Apr 30 14:18 - 14:19  (00:00)
reboot   system boot  3.10.0-327.el7.x Sat Apr 30 14:18 - 14:19  (00:01)
trainee  pts/0        10.0.2.2        Sat Apr 30 14:16 - 14:17  (00:01)
trainee  tty1                         Sat Apr 30 14:15 - 14:17  (00:02)
reboot   system boot  3.10.0-327.el7.x Sat Apr 30 14:13 - 14:19  (00:06)
trainee  pts/0        :0              Sat Apr 30 14:11 - 14:11  (00:00)
trainee  :0           :0              Sat Apr 30 14:10 - 14:11  (00:01)
(unknown :0           :0              Sat Apr 30 14:10 - 14:10  (00:00)
reboot   system boot  3.10.0-327.el7.x Sat Apr 30 14:09 - 14:11  (00:02)
trainee  pts/0        :0              Sat Apr 30 12:38 - crash  (01:31)
trainee  :0           :0              Sat Apr 30 12:36 - crash  (01:33)
(unknown :0           :0              Sat Apr 30 12:34 - 12:36  (00:01)
reboot   system boot  3.10.0-327.el7.x Sat Apr 30 12:34 - 14:11  (01:37)
trainee  tty1                         Sat Apr 30 12:19 - 12:28  (00:09)
reboot   system boot  3.10.0-327.el7.x Sat Apr 30 12:18 - 12:28  (00:10)
trainee  pts/0        :0              Sat Apr 30 12:15 - 12:18  (00:03)
trainee  :0           :0              Sat Apr 30 12:14 - 12:18  (00:03)
(unknown :0           :0              Sat Apr 30 12:11 - 12:14  (00:02)
reboot   system boot  3.10.0-327.el7.x Sat Apr 30 12:10 - 12:28  (00:18)
trainee  pts/1        :0              Sat Apr 30 12:06 - 12:09  (00:03)
trainee  pts/1        :0              Sat Apr 30 12:01 - 12:02  (00:01)
trainee  pts/0        :0              Sat Apr 30 11:57 - 12:09  (00:12)
```

```
trainee  pts/0        :0               Sat Apr 30 11:55 - 11:56  (00:01)
trainee  :0           :0               Sat Apr 30 11:54 - 12:09  (00:15)
(unknown :0           :0               Sat Apr 30 11:53 - 11:54  (00:00)
reboot   system boot  3.10.0-327.el7.x Sat Apr 30 11:43 - 12:28  (00:45)

wtmp begins Sat Apr 30 11:43:38 2016
```

La commande lastlog

Cette commande indique les dates et heures de la connexion au système la plus récente des utilisateurs :

```
[root@centos7 ~]# lastlog
Username         Port     From             Latest
root             pts/2                     Tue Jun 19 18:47:20 +0200 2018
bin                                        **Never logged in**
daemon                                     **Never logged in**
adm                                        **Never logged in**
lp                                         **Never logged in**
sync                                       **Never logged in**
shutdown                                   **Never logged in**
halt                                       **Never logged in**
mail                                       **Never logged in**
operator                                   **Never logged in**
games                                      **Never logged in**
ftp                                        **Never logged in**
nobody                                     **Never logged in**
avahi-autoipd                              **Never logged in**
systemd-bus-proxy                           **Never logged in**
systemd-network                            **Never logged in**
dbus                                       **Never logged in**
polkitd                                    **Never logged in**
abrt                                       **Never logged in**
usbmuxd                                    **Never logged in**
```

```
colord                                      **Never logged in**
libstoragemgmt                              **Never logged in**
setroubleshoot                              **Never logged in**
rpc                                         **Never logged in**
rtkit                                       **Never logged in**
chrony                                      **Never logged in**
unbound                                     **Never logged in**
tss                                         **Never logged in**
geoclue                                     **Never logged in**
ntp                                         **Never logged in**
sssd                                        **Never logged in**
rpcuser                                     **Never logged in**
nfsnobody                                   **Never logged in**
pulse                                       **Never logged in**
gdm              :0                         Sat Apr 30 15:22:30 +0200 2016
gnome-initial-setup                            **Never logged in**
avahi                                       **Never logged in**
postfix                                     **Never logged in**
sshd                                        **Never logged in**
tcpdump                                     **Never logged in**
trainee          pts/2    10.0.2.2          Tue Jun 19 18:47:12 +0200 2018
vboxadd                                     **Never logged in**
snort                                       **Never logged in**
apache                                      **Never logged in**
```

La Commande lastb

Cette commande indique les dates et heures des connexions infructueueses des utilisateurs à partir du contenu du fichier **/var/log/btmp** :

```
[root@centos7 ~]# lastb
root     pts/0                        Tue Jun 19 16:37 - 16:37  (00:00)


```

```
btmp begins Tue Jun 19 16:37:18 2018
```

/var/log/secure

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

```
[root@centos7 ~]# tail -n 15 /var/log/secure
Jun 19 22:03:57 centos7 polkitd[532]: Unregistered Authentication Agent for unix-process:21784:3831602 (system
bus name :1.320, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_GB.UTF-8) (disconnected
from bus)
Jun 19 22:04:06 centos7 polkitd[532]: Registered Authentication Agent for unix-process:21883:3832537 (system bus
name :1.321 [/usr/bin/pkttyagent --notify-fd 5 --fallback], object path
/org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_GB.UTF-8)
Jun 19 22:04:07 centos7 polkitd[532]: Unregistered Authentication Agent for unix-process:21883:3832537 (system
bus name :1.321, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_GB.UTF-8) (disconnected
from bus)
Jun 19 23:45:43 centos7 su: pam_unix(su-l:session): session opened for user prison by trainee(uid=0)
Jun 19 23:46:13 centos7 su: pam_unix(su-l:session): session closed for user prison
Jun 19 23:48:25 centos7 su: pam_unix(su-l:session): session opened for user prison by trainee(uid=0)
Jun 19 23:48:25 centos7 su: pam_unix(su-l:session): session closed for user prison
Jun 19 23:52:22 centos7 su: pam_unix(su-l:session): session opened for user prison by trainee(uid=0)
Jun 19 23:52:27 centos7 su: pam_unix(su-l:session): session closed for user prison
Jun 19 23:54:35 centos7 su: pam_unix(su-l:session): session opened for user prison by trainee(uid=0)
Jun 19 23:55:33 centos7 su: pam_unix(su-l:session): session closed for user prison
Jun 20 00:01:21 centos7 su: pam_unix(su-l:session): session opened for user prison by trainee(uid=0)
Jun 20 00:01:50 centos7 su: pam_unix(su-l:session): session closed for user prison
Jun 20 00:01:53 centos7 su: pam_unix(su-l:session): session opened for user prison by trainee(uid=0)
Jun 20 00:02:19 centos7 su: pam_unix(su-l:session): session closed for user prison
```

Les Contre-Mesures

Les contre-mesures incluent le renforcement de la sécurité des comptes et l'utilisation des mots de passe complexes.

LAB #2 - Renforcer la sécurité des comptes

Passez en revue le fichier **/etc/passwd** :

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPv4LL Stack:/var/lib/avahi-autoipd:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/cache/rpcbind:/sbin/nologin
rtkit:x:499:499:RealtimeKit:/proc:/sbin/nologin
abrt:x:498:498::/etc/abrt:/sbin/nologin
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
```

```
tcpdump:x:72:72::/:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
nslcd:x:65:55:LDAP Client User:/:/sbin/nologin
saslauth:x:497:495:"Saslauthd user":/var/empty/saslauth:/sbin/nologin
postfix:x:89:89::/var/spool/postfix:/sbin/nologin
avahi:x:70:70:Avahi mDNS/DNS-SD Stack:/var/run/avahi-daemon:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
pulse:x:496:494:PulseAudio System Daemon:/var/run/pulse:/sbin/nologin
gdm:x:42:42::/var/lib/gdm:/sbin/nologin
trainee:x:500:500:trainee:/home/trainee:/bin/bash
vboxadd:x:495:1::/var/run/vboxadd:/bin/false
prison:x:501:502:chroot_user:/home/prison:/bin/chroot
```

Important : Notez que la valeur de l'UID de root est toujours de 0. Notez cependant que sous RHEL 5 et 6 les UID des utilisateurs normaux commencent à **500** et les UID des comptes système sont inclus entre 1 et 99 par convention. Sous RHEL 7, les UID des utilisateurs normaux commencent à **1000** et les UID des comptes système sont inclus entre 201 et 999. Sous Debian 6, 7 et 8 les UID des utilisateurs normaux commencent à **1000** et les UID des comptes système sont inclus entre 100 et 999 par convention. Sous openSUSE, les UID des utilisateurs normaux commencent à **1000** et les UID des comptes système sont inclus entre 100 et 499. Sous Ubuntu 14.04 les UID des utilisateurs normaux commencent à **1000** et les UID des comptes système sont inclus entre 100 et 999.

Chaque ligne est constituée de 7 champs :

- Le nom d'utilisateur
- Le mot de passe. Une valeur de **x** dans ce champs indique que le système utilise le fichier **/etc/shadow** pour stocker les mots de passe.
- L'UID. Une valeur unique qui est utilisée pour déterminée les droits aux fichiers et aux répertoires.
- Le GID. Une valeur indiquant le groupe **principal** de l'utilisateur
- Le nom complet. Ce champs optionnel est aussi appelé **GECOS**
- Le répertoire personnel de l'utilisateur
- Le shell de l'utilisateur.

Notez d'abord les utilisateurs inutiles. Par exemple, dans le cas ci-dessus, l'utilisateur suivant est inutile si vous ne souhaitez par imprimer a partir du serveur:

```
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

Supprimez donc les utilisateurs et groupes inutiles en utilisant des commandes telles:

```
# userdel -r lp [Entree]
```

```
# groupdel lp [Entree]
```

Pour les utilisateurs restants, utilisez le système de shadowing :

```
[root@centos7 ~]# cat /etc/shadow
root:$6$TX12b5lW9UXD8Ld6$l/PjTA.XrBAbsayGCaSFaM5ibLo2xBBeYNCyEdVv9uMUctxq9Q0YBxLwCvS2bCdgr.BeSmXvi6BwD55KKscaJ.::
0:99999:7:::
bin:*:16659:0:99999:7:::
daemon:*:16659:0:99999:7:::
adm:*:16659:0:99999:7:::
lp:*:16659:0:99999:7:::
sync:*:16659:0:99999:7:::
shutdown:*:16659:0:99999:7:::
halt:*:16659:0:99999:7:::
mail:*:16659:0:99999:7:::
operator:*:16659:0:99999:7:::
games:*:16659:0:99999:7:::
```

```
ftp:*:16659:0:99999:7:::
nobody:*:16659:0:99999:7:::
avahi-autoipd:!!:16779::::::
systemd-bus-proxy:!!:16779::::::
systemd-network:!!:16779::::::
dbus:!!:16779::::::
polkitd:!!:16779::::::
abrt:!!:16779::::::
usbmuxd:!!:16779::::::
colord:!!:16779::::::
libstoragemgmt:!!:16779::::::
setroubleshoot:!!:16779::::::
rpc:!!:16779:0:99999:7:::
rtkit:!!:16779::::::
chrony:!!:16779::::::
unbound:!!:16779::::::
tss:!!:16779::::::
geoclue:!!:16779::::::
ntp:!!:16779::::::
sssd:!!:16779::::::
rpcuser:!!:16779::::::
nfsnobody:!!:16779::::::
pulse:!!:16779::::::
gdm:!!:16779::::::
gnome-initial-setup:!!:16779::::::
avahi:!!:16779::::::
postfix:!!:16779::::::
sshd:!!:16779::::::
tcpdump:!!:16779::::::
trainee:$6$4PW9kfdOIOmWmSSO$8vikc1pyXgVc.C8xKP5EvIbBwe1fWd3DSvgWGQ5FAr7jwyMCbLQOOWbvomS9z1Q6V8IqZjBSREWafNzOYjKqC
0::0:99999:7:::
vboxadd:!!:16921::::::
```

Chaque ligne est constituée de 8 champs :

- Le nom de l'utilisateur. Ce champs est utilisé pour faire le lien avec le fichier **/etc/passwd**,
- Le mot de passe **crypté** de l'utilisateur. Le cryptage est à sens **unique**. Ce champ peut aussi contenir une des trois valeurs suivantes :
  - **!!** - Le mot de passe n'a pas encore été défini et l'utilisateur ne peut pas se connecter,
  - * - L'utilisateur ne peut pas se connecter,
  - **vide** - aucun mot de passe sera demandé pour l'utilisateur concerné,
- Le nombre de jours entre le **01/01/1970** et le dernier changement du mot de passe,
- Le nombre de jours que le mot de passe est encore valide. Une valeur de **0** dans ce champs indique sue le mot de passe n'expire jamais,
- Le nombre de jours après lequel le mot de passe doit être changé,
- Le nombre de jours avant la date de modification forcée que l'utilisateur recevra un avertissement,
- Le nombre de jours après l'expiration du mot de passe que le compte sera désactivé,
- Le **numéro** du jour après le **01/01/1970** que le compte a été désactivé.

LAB #3 - PAM sous RHEL/CentOS 7

PAM (*Pluggable Authentification Modules* ou Modules d'Authentification Enfichables) est une architecture modulaire permettant à l'administrateur système de définir une politique d'authentification pour les logiciels prenant en charge PAM.

Les fichiers de configuration se trouvent dans le répertoire **/etc/pam.d** :

```
[root@centos7 ~]# ls /etc/pam.d
atd                     login              smtp
chfn                    other              smtp.postfix
chsh                    passwd             sshd
config-util             password-auth      su
crond                   password-auth-ac   sudo
cups                    pluto              sudo-i
fingerprint-auth        polkit-1           su-l
fingerprint-auth-ac     postlogin          system-auth
gdm-autologin           postlogin-ac       system-auth-ac
gdm-fingerprint         ppp                system-config-language
gdm-launch-environment  remote             systemd-user
gdm-password            runuser            vlock
```

```
gdm-pin                 runuser-l          vmtoolsd
gdm-smartcard           setup              xserver
ksu                     smartcard-auth
liveinst                smartcard-auth-ac
```

Ces fichiers ont une structure spécifique et sont nommés d'après le service ou l'application qu'ils contrôlent. Leur contenu fait appel à des modules qui se trouvent dans le répertoire **/lib64/security** :

```
[root@centos7 ~]# ls /lib64/security
pam_access.so          pam_krb5afs.so           pam_selinux.so
pam_cap.so             pam_krb5.so              pam_sepermit.so
pam_chroot.so          pam_lastlog.so           pam_shells.so
pam_console.so         pam_limits.so            pam_sss.so
pam_cracklib.so        pam_listfile.so          pam_stress.so
pam_debug.so           pam_localuser.so         pam_succeed_if.so
pam_deny.so            pam_loginuid.so          pam_systemd.so
pam_echo.so            pam_mail.so              pam_tally2.so
pam_env.so             pam_mkhomedir.so         pam_time.so
pam_exec.so            pam_motd.so              pam_timestamp.so
pam_faildelay.so       pam_namespace.so         pam_tty_audit.so
pam_faillock.so        pam_nologin.so           pam_umask.so
pam_filter             pam_oddjob_mkhomedir.so  pam_unix_acct.so
pam_filter.so          pam_permit.so            pam_unix_auth.so
pam_fprintd.so         pam_postgresok.so        pam_unix_passwd.so
pam_ftp.so             pam_pwhistory.so         pam_unix_session.so
pam_gnome_keyring.so   pam_pwquality.so         pam_unix.so
pam_group.so           pam_rhosts.so            pam_userdb.so
pam_issue.so           pam_rootok.so            pam_warn.so
pam_keyinit.so         pam_securetty.so         pam_wheel.so
pam_krb5               pam_selinux_permit.so    pam_xauth.so
```

Les modules les plus importants sont :

Module	**Description**
pam_access.so	Ce module est utilisé pour interdire l'accès aux services sécurisés par des hôtes non-autorisés.
pam_echo.so	Ce module présente le contenu du fichier passé en argument à tout utilisateur lors de sa connexion.
pam_limits.so	Ce module implémente les limites des ressources détaillées dans le fichier **/etc/security/limits.conf** et dans les fichiers ***.conf** trouvés dans le répertoire **/etc/security/limits.d/**.
pam_listfile.so	Ce module est utilisé pour consulter un fichier spécifique pour vérifier les authiorisations. Par exemple, le service ftp utilise ce module pour consulter le fichier **/etc/ftpusers** qui contient une liste d'utilisateurs qui ne sont **pas** autorisés à se connecter au serveur ftp.
pam_nologin.so	Ce module interdit les connexions d'utilisteurs, autre que root, dans le cas où le fichier **/etc/nologin** est présent.
pam_pwquality.so	Ce module est utilisé pour vérifier la qualité du mot de passe d'un utilisateur
pam_securetty.so	Ce module interdit des connexions de root à partir des périphériques tty qui ne sont pas listés dans le fichier **/etc/securetty**.
pam_unix.so	Ce module est utilisé pour vérifier les informations suivantes ; expire, last_change, max_change, min_change, warn_change.

Chaque fichier dans /etc/pam.d contient les règles PAM utilisées pendant l'authentification. Ouvrez le fichier **login** :

```
[root@centos7 ~]# cat /etc/pam.d/login
#%PAM-1.0
auth [user_unknown=ignore success=ok ignore=ignore default=bad] pam_securetty.so
auth       substack     system-auth
auth       include      postlogin
account    required     pam_nologin.so
account    include      system-auth
password   include      system-auth
# pam_selinux.so close should be the first session rule
session    required     pam_selinux.so close
session    required     pam_loginuid.so
session    optional     pam_console.so
# pam_selinux.so open should only be followed by sessions to be executed in the user context
session    required     pam_selinux.so open
session    required     pam_namespace.so
session    optional     pam_keyinit.so force revoke
session    include      system-auth
session    include      postlogin
```

```
-session   optional     pam_ck_connector.so
```

La première ligne de ce fichier est un commentaire qui spécifie que le fichier est conforme à la spécification PAM 1.0.

Ce fichier, tout comme les autres, est ensuite structuré de la façon suivante :

- Une module par ligne,
- Quatre champs séparés par un espace dans chaque règle dont les trois premières sont obligatoires.

Le **premier champs** est le ***type de module***. Il en existe quatre :

Type	**Description**
auth	Utilisé pour authentifier un utilisateur ou les pré-requis système (par exemple /etc/nologin)
account	Utilisé pour vérifier si l'utilisateur peut s'authentifier (par exemple la validité du compte)
password	Utilisé pour vérifier si l'utilisateur dispose des droits pour mettre le mécanisme d'authentification à jour
session	Utilisé pour gérer la session après l'authentification (par exemple monter un répertoire)

Le **deuxième champs** est le ***Control-flag***. Il en existe quatre :

Control-flag	**Description**
required	La réussite de ce module est indispensable. L'échec d'un module *required* n'est communiqué à l'application qu'après la vérification de tous les modules ayant un *control-flag* de **required**
requisite	La réussite de ce module est indispensable. L'échec d'un module *requisite* est immédiatement communiqué à l'application
sufficient	La réussite de ce module est suffisant pour authoriser l'authentification. Si aucun test *required* précédent est en échec, la vérification s'arrête. Si un test *required* précédent était en échec, le test *sufficient* est ignoré. L'échec d'un test *sufficient* n'a pas de conséquence si tous les tests *required* réussissent.
optional	La réussite ou l'échec de ce module est sans importance, **sauf** s'il s'agit du seul module à exécuter
include	Ce control-flag permet d'inclure toutes les lignes du même *type de module* se trouvant dans le fichier spécifié en argument

Le **troisième champs** stipule le ***module*** associé à la règle. Sans chemin absolu, le fichier est supposé être dans le répertoire **/lib/security**. Pour inclure un module en dehors de ce répertoire il convient donc de stipuler son chemin absolu.

Le **quatrième champs** contient éventuellement les **arguments**.

Ouvrez maintenant le fichier **password-auth-ac** :

```
[root@centos7 ~]# cat /etc/pam.d/password-auth-ac
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth        required      pam_deny.so

account     required      pam_unix.so
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 1000 quiet
account     required      pam_permit.so

password    requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password    sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
-session     optional      pam_systemd.so
session     [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session     required      pam_unix.so
```

Dans ce fichier, si la règle **sufficient** réussit, les modules suivants ne sont pas invoqués.

Bloquer un Compte après N Echecs de Connexion

Le module PAM **pam_tally.so** permet de bloquer un compte après N échecs de connexion. Afin d'activer ce comportement, il convient d'ajouter dans le fichier **/etc/pam.d/system-auth** la ligne suivante :

```
auth required pam_tally.so onerr=fail deny=3 unlock_time=300
```

Dans ce cas, après trois tentatives infructueuses de connexion, le compte sera bloquer pendant 5 minutes.

Configuration

Certains modules de PAM peuvent être configurés grâce aux fichiers présents dans le répertoire **/etc/security** :

```
[root@centos7 ~]# ls /etc/security
access.conf       console.perms    limits.d        opasswd         time.conf
chroot.conf       console.perms.d  namespace.conf  pam_env.conf
console.apps      group.conf       namespace.d     pwquality.conf
console.handlers  limits.conf      namespace.init  sepermit.conf
```

Parmi les fichiers cités on note ceux qui peuvent être utilisés pour configurer les modules suivants :

Fichier/*Répertoire*	**Description**
access.conf	Utilisé par le module pam_access.so
console.apps	Utilisés par le module pam_console.so
console.perms	Utilisé par le module pam_console.so
console.perms.d	Utilisé par le module pam_console.so
group.conf	Utilisés par le module pam_group.so
limits.conf	Utilisé par le module pam_limits.so
pam_env.conf	Utilisé par le module pam_env.so
time.conf	Utilisé par le module pam_time.so

A faire : Passez en revue chacun de ces fichiers.

Dernièrement, PAM propose une solution pour toutes les applications ne disposant pas de leurs propres fichiers de configuration PAM. Cette solution

prend la forme du fichier **/etc/pam.d/other** :

```
[root@centos7 ~]# cat /etc/pam.d/other
#%PAM-1.0
auth     required       pam_deny.so
account  required       pam_deny.so
password required       pam_deny.so
session  required       pam_deny.so
```

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.

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
```

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 :

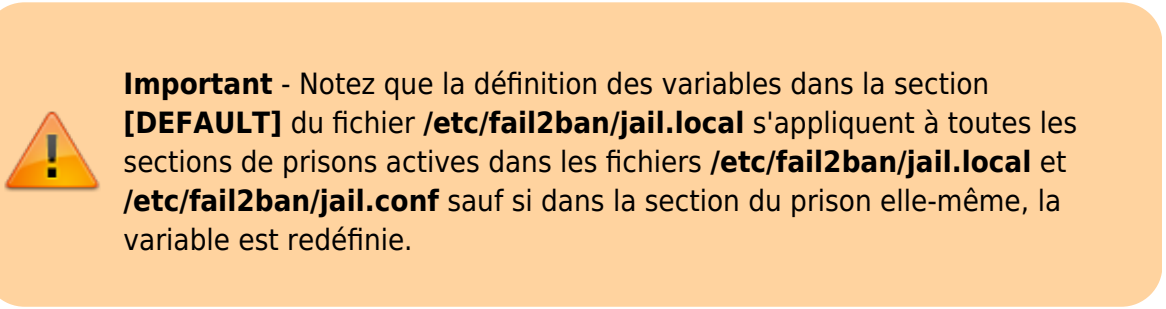
```
[root@centos7 ~]# vi /etc/fail2ban/jail.local
[root@centos7 ~]# cat /etc/fail2ban/jail.local
[DEFAULT]
ignoreip = 127.0.0.1 172.YY+20.0.3
findtime = 3600
```

```
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.



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

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
```

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
```

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 10.0.2.15
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
```
