

## Sécurisation d'un serveur

### Portsentry : Détection/blocage des scans de ports

#### Configuration de Portsentry

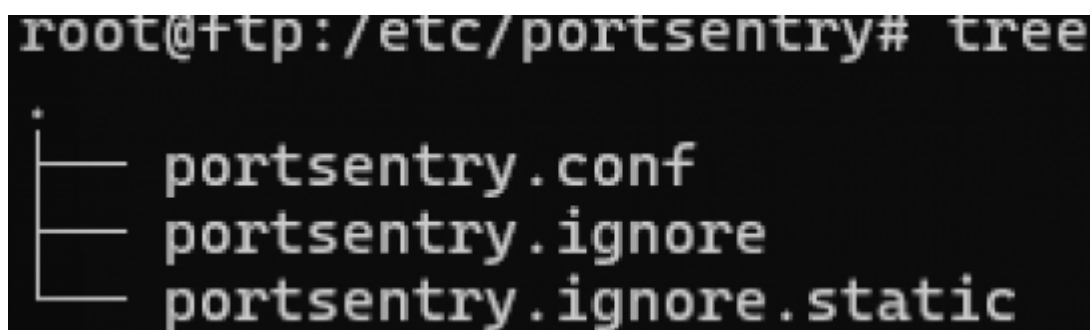
installation

Pour installer Portsentry

```
apt update  
apt install portsentry
```

#### Arborescence des fichiers avec Tree.

```
apt install tree
```



```
root@ftp:/etc/portsentry# tree  
.  
├── portsentry.conf  
├── portsentry.ignore  
└── portsentry.ignore.static
```

Par défaut, Portsentry ne bloque rien et nous allons devoir le configurer afin de détecter et bloquer le scan de ports. Il va falloir modifier le fichier où sont notifiées les adresses IPs à ne pas bloquer afin de ne pas se bloquer soi-même. Pour cela il existe 2 fichiers : portsentry.ignore et portsentry.ignore.static. Toutes les IPs que vous allez ajouter dans portsentry.ignore.static seront ajoutées dans portsentry.ignore après un redémarrage du service portsentry. Je décide de modifier le fichier [/etc/portsentry/portsentry.ignore](#) et de vérifier que l'adresse 127.0.0.1 soit bien définie

#### CONFIGURATION DES FICHIERS DE PORTSENTRY

Passons à la configuration de Portsentry:

Si vous choisissez les modes atcp et audp ("a" signifie avancé) dans /etc/defaults/portsentry, inutile de préciser les ports, Portsentry va vérifier les ports utilisés et automatiquement "lier" les ports disponibles. C'est l'option la plus efficace. Donc avec cette option, portsentry établit une liste des ports d'écoute, TCP et UDP, et bloque l'hôte se connectant sur ces ports sauf s'il est présent dans le fichier portsentry.ignore configuré auparavant. Modification du fichier [/etc/default/portsentry](#):

À présent nous allons nous attaquer au fichier de configuration principale : portsentry.conf

[/etc/portsentry/portsentry.conf](#)

## Phase de TEST

je tente d'attaquer mon serveur FTP avec mon serveur web

```
root@serveurweb2:~# nmap -v 10.31.248.20
Starting Nmap 7.93 ( https://nmap.org ) at 2024-12-09 13:17 UTC
Initiating ARP Ping Scan at 13:17
Scanning 10.31.248.20 [1 port]
Completed ARP Ping Scan at 13:17, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 13:17
Completed Parallel DNS resolution of 1 host. at 13:17, 0.01s elapsed
Initiating SYN Stealth Scan at 13:17
Scanning 10.31.248.20 [1000 ports]
Completed SYN Stealth Scan at 13:17, 21.06s elapsed (1000 total ports)
Nmap scan report for 10.31.248.20
Host is up (0.00028s latency).
All 1000 scanned ports on 10.31.248.20 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: BC:24:11:0C:DE:80 (Unknown)

Read data files from: /usr/bin/./share/nmap
```

Si on regarde à présent sur le serveur hébergeant portsentry # grep attackalert /var/log/syslog

```
2024-12-09T14:24:36.325156+01:00 ftp portsentry[6423]: attackalert: Host: 10.31.248.80/10.31.248.80 is already blocked I
gnoring
2024-12-09T14:24:47.335907+01:00 ftp portsentry[6423]: attackalert: TCP SYN/Normal scan from host: 10.31.248.80/10.31.24
8.80 to TCP port: 110
2024-12-09T14:24:47.336085+01:00 ftp portsentry[6423]: attackalert: Host: 10.31.248.80/10.31.248.80 is already blocked I
gnoring
root@ftp:~#
```

```
cat /etc/hosts.deny
```

```
root@ftp:/etc/portsentry# route -n
Table de routage IP du noyau
Destination      Passerelle      Genmask          Indic Metric Ref       Use Iface
0.0.0.0          10.31.251.254   0.0.0.0          UG    0      0        0 ens18
10.31.248.0      0.0.0.0         255.255.252.0    U     0      0        0 ens18
10.31.248.80     -               255.255.255.255 !H    0      -        0 -
root@ftp:/etc/portsentry#
```

**/etc/hosts.deny dans ce fichier** , il faut juste effacer ll'adresse pour debannir.

## Fail2ban : Bannir des IP avec fail2ban

fail2ban est une application qui analyse les logs de divers services (SSH, Apache, FTP...) en cherchant des correspondances entre des motifs définis dans ses filtres et les entrées des logs. Lorsqu'une correspondance est trouvée une ou plusieurs actions sont exécutées.

Pour l'installer rien de plus simple. Il convient ensuite de lancer le service fail2ban:

```
apt update
apt upgrade
apt install fail2ban
```

Si iptables n'est pas installé, le faire

```
apt install -y iptables
```

Arborescence du répertoire de fail2ban

```
root@ftp:/etc/fail2ban# tree -L 1 /etc/fail2ban
/etc/fail2ban
├── action.d
├── fail2ban.conf
├── fail2ban.d
├── filter.d
├── jail.conf
├── jail.d
├── jail.local
├── paths-arch.conf
├── paths-common.conf
├── paths-debian.conf
└── paths-opensuse.conf
```

puis d'en créer le démarrage automatique :

```
systemctl start fail2ban
systemctl enable fail2ban
```

Et enfin de contrôler la bonne installation :

```
systemctl status fail2ban
```

Si la réponse comporte du rouge et le mot "failed" " sur la ligne commençant par "Active :", les dernières lignes du message indiquent les raisons de l'échec et permettent sa correction avant un nouvel essai, à tenter après lecture du reste de cet article. Si la réponse comporte du vert et les mots "active (running)" sur la ligne commençant par "Active :", le service est installé et actif.

### Paramètre de configuration :

Par défaut fail2ban est installé avec 2 fichiers de configuration : /etc/fail2ban/jail.conf et /etc/fail2ban/jail.d/defaults-debian.conf . Fail2ban lit les fichiers de configurations dans cet ordre :  
\*Les fichiers .conf\* \*Les fichiers .local\*

Jail.conf est le fichier de configuration principal des jails. Il ne doit pas être modifié donc nous allons en faire une copie appelé jail.local. C'est cette copie que vous allez modifier. Créer les fichiers de configuration adéquat en se basant sur ceux présents.

```
cp /etc/fail2ban/jail.{conf,local}
```

## Editer le fichier : Activer la protection pour SSH [/etc/fail2ban/jail.local](#)

Dans le répertoire `/etc/fail2ban/jail.d`, nous avons configuré trois prisons principales : `recidive`, `sshd`, et `proftpd`. Chaque prison est associée à un service spécifique pour détecter et bloquer les tentatives d'attaque brute-force. Les fichiers suivants définissent les règles et actions pour chaque service

```
root@ftp:/etc/fail2ban/jail.d# ls
defaults-debian.conf  proftpd.conf  recidive.conf  sshd.conf
root@ftp:/etc/fail2ban/jail.d# |
```

[sisr2-usa:proftpd.conf](#) [sisr2-usa:recidive.conf](#) [sisr2-usa:sshd.conf](#)

Les fichiers `proftpd.conf`, `recidive.conf`, et `sshd.conf` jouent un rôle clé dans la protection des services contre les attaques brute-force. Ils permettent de définir des règles adaptées à chaque service et de prendre des mesures supplémentaires pour les attaquants récurrents.

**Configuration pour chaque service** À chaque prison ou service est associé un fichier de filtrage du même nom dans le dossier `/etc/fail2ban/filter.d`. Ces fichiers contiennent une ou plusieurs expressions rationnelles qui servent de motif de recherche pour les lignes correspondantes dans les logs. Les expressions rationnelles sont définies par la directive `failregex`.

### 1. ProFTPD (10.31248.20)

Le fichier `/etc/fail2ban/jail.d/proftpd.conf` contient les paramètres de la jail pour protéger le service FTP :

#### Créer un filtre pour ProFTPD :

[sisr2-usa:proftpd.conf](#)

#### Tester le filtre ProFTPD

[/etc/fail2ban/filter.d/proftpd.conf](#)

### 2. Nextcloud

Le fichier `/etc/fail2ban/jail.d/nextcloud.conf` protège l'application Nextcloud (10.31.240.80)

[/etc/fail2ban/jail.d/nextcloud.conf](#)

#### Tester le filtre Nextcloud

```
[Definition]
_groupsre = (?: (?: , ? \s* " \w+ " : (?: " [^"]+ " | \w+ ) ) * )
failregex =
^ \{ % ( _groupsre ) s , ? \s* " remoteAddr " : " <HOST> " % ( _groupsre ) s , ? \s* " message " : " Login
failed :
^ \{ % ( _groupsre ) s , ? \s* " remoteAddr " : " <HOST> " % ( _groupsre ) s , ? \s* " message " : " Trust
ed domain error .
datepattern = , ? \s* " time " \s* : \s* " %Y - %m - %d [ T ] %H : %M : %S ( %Z ) ? "
```

3. WordPress Le fichier `/etc/fail2ban/jail.d/wordpress.conf` protège les connexions à WordPress

[etc/fail2ban/jail.d/wordpress.conf](#)

### Tester le filtre pour wordpress

[/etc/fail2ban/filter.d/wordpress.conf](#)

4. DokuWiki Le fichier `/etc/fail2ban/jail.d/dokuwiki.conf` protège DokuWi\*

[/etc/fail2ban/jail.d/dokuwiki.conf](#)

Test de filtre [/etc/fail2ban/filter.d/dokuwiki.conf](#)



La prison recidive fonctionne sur le même principe que diverses plateformes telles que Twitch par exemple. Elle compte le nombre de fois qu'une ip s'est faite bannir d'un service et à certains nombres de bans, l'ip se fait bannir définitivement. Par exemple, dans la prison recidive juste au dessus, au 3e ban temporaire de n'importe quel service, l'ip se fait bannir définitivement. **Si l'on se fait ban temporairement de 3 services, chacun différents, sur le serveur, même si les bans sont temporaires la prison recidive entrera tout de même en action.** Pour ban def il faut mettre en valeur "-1" en face de bantime. Le findtime correspond jusqu'à combien de temps dans le passé l'outil va analyser les logs si jamais pour une raison ou pour une autre fail2ban devait redémarrer.

### Gestion du bannissement

Après la configuration de chaque service Une fois que la configuration de chaque service est terminée, voici les étapes finales pour valider, tester et activer Fail2ban efficacement :

```
fail2ban-client reload
```

On redémarre ensuite fail2ban :

```
systemctl restart fail2ban
```

Vérifier l'état de Fail2ban

```
systemctl status fail2ban
```

On clique ensuite la commande suivante pour s'assurer que nos prisons sont bien actives :

```
fail2ban-client status
```

On peut aussi préciser après status la prison dont on veut plus de détails pour savoir quelles ips se sont faites bannir :

```
fail2ban-client status [nom de la prison]
```

Vérifier l'état des jails Pour voir toutes les jails activées et leur statut

```
fail2ban-client status
```

Dé-bannir une IP de l'un de vos jails

```
fail2ban-client set [nom du jail] unbanip [IP concerné]
```

Bannir manuellement une IP sur l'un de vos jails

```
fail2ban-client set [nom du jail] banip [IP à bannir]
```

From:

<https://sisr2.beaupeyrat.com/> - Documentations SIO2 option SISR

Permanent link:

[https://sisr2.beaupeyrat.com/doku.php?id=sisr2-usa:portsentry\\_fail2ban](https://sisr2.beaupeyrat.com/doku.php?id=sisr2-usa:portsentry_fail2ban)

Last update: **2024/12/17 14:03**

