Protéger son serveur des attaques par brute force avec Fail2ban

par Goldkey (Accueil)

Date de publication : 04 juin 2008

Dernière mise à jour :

Ce tutoriel a pour but d'expliquer comment protéger son serveur des attaques par brute force avec Fail2ban sur un serveur Debian.

I - Prérequis....3
II - Rappel....3
III - Installation de Fail2ban....3
IV - Configuration et premiers test....3
IV-A - SSH....4
IV-B - FTP....4
IV-C - HTTP....4
IV-D - Les premiers tests....5
V - Pour aller plus loin....5
V-A - Création d'une nouvelle règle : protection d'un espace membre (PHP)....5
V-B - Mise en place de la géolocalisation des adresses IP's....6
V-C - Intéraction de Fail2ban avec des programmes externes....7
VI - Conclusion....7

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2008 Developpez LLC. Tout droits réservés Developpez LLC. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents et images sans l'autorisation expresse de Developpez LLC. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

I - Prérequis

Le contenu de cet article a été rédigé en se basant sur une distribution Debian Etch. L'interface réseau utilisée est eth0 (192.168.0.9). Suivant votre configuration n'oublié pas de l'adapter au besoin.

II - Rappel

Les attaques par "brute force" permettent de trouver un mot de passe en testant une à une toutes les combinaisons possibles. Celles-ci peuvent être déclinées en "attaque par dictionnaire" afin de tester une série de mot de passe définit afin d'augmenter les chances de réussite.

Pour limiter ce genre d'attaques nous allons utiliser le logiciel **Fail2ban** sur notre serveur. Il permet de scruter des fichiers de log et de bannir les adresses IP qui ont obtenu un nombre élevé d'échecs lors de leur tentative authentification.

III - Installation de Fail2ban

Pour installer le package Fail2ban sur une distribution Debian il suffit de taper la commande :

```
apt-get install fail2ban
```

Les principaux fichiers de configuration installés par le paquet Debian se situent dans le répertoire :

```
/etc/fail2ban
```

- fail2ban.conf -> fichier de configuration de Fail2ban
- jail.conf -> fichier de configuration du banissement pour les services
- filter.d/ -> dossier contenant les fichiers regex pour le banissement
- action.d -> dossier contenant les règles d'action de Fail2ban

Pour vérifier que le démon Fail2ban est actif il suffit de taper la commande suivante :

```
/etc/init.d/fail2ban status
```

qui devrait nous indiquer

```
Status of fail2ban: fail2ban is running
```

Le fichier de log de Fail2ban se situe dans le répertoire :

```
/var/www/fail2ban/fail2ban.log
```

IV - Configuration et premiers test

Après installation de Fail2ban, un seul service est activé : SSH. Dans ce chapitre nous verrons comment sécuriser les services SSH, FTP, HTTP dont les configurations sont fournit en standard dans le package Debian.

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2008 Developpez LLC. Tout droits réservés Developpez LLC. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents et images sans l'autorisation expresse de Developpez LLC. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

IV-A - SSH

La configuration utilisée est identique à celle proposée par défaut. Celle-ci se trouve dans le fichier jail.conf :

```
[ssh]

enabled = true
port    = ssh
filter  = sshd
logpath  = /var/log/auth.log
maxretry = 4
```

La fichier sshd.conf contenant la règle regex pour matcher les erreurs d'authentification SSH se situe dans le répertoire filter.d La règle regex utilisée est :

```
failregex = (?:(?:Authentication failure|Failed [-/\w+]+) for(?: [iI](?:llegal|nvalid) user)?|[Ii]
(?:llegal|nvalid)
            user|ROOT LOGIN REFUSED) . *(?: from|FROM) <HOST>(?: port \d *)?(?: ssh\d *)?\s *$
```

IV-B - FTP

Par défaut Fail2ban supporte trois serveurs FTP : Vsftpd, Proftpd, Wuftpd. Ici nous avons choisit d'illustrer cet exemple avec Vsftpd.

Nous allons activer la protection FTP en modifiant la variable de la section FTP :

```
[vsftpd]

enabled  = true
port     = ftp
filter   = vsftpd
logpath  = /var/log/auth.log
maxretry = 6
```

Ci-dessous

```
failregex = vsftpd: \(pam_unix\) authentication failure; . * rhost=<HOST>(?:\s+user=\S *)?\s *$
```

IV-C - HTTP

Fail2ban propose, par défaut, une règle intéressante pour Apache. Elle permet de bannir les IP's tentant d'accéder à des URL's inexistantes sur votre serveur. Pour activer cette fonctionnalité, il faut modifier la section [apache-noscript] comme suit :

```
[apache-noscript]

enabled = true
port    = http
filter  = apache-noscript
logpath = /var/log/apache */ *error.log
```

La règle utilisée pour matcher les erreurs d'accès sur Apache est :

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2008 Developpez LLC. Tout droits réservés Developpez LLC. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents et images sans l'autorisation expresse de Developpez LLC. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

```
failregex = [[]client (?P<HOST>\S *)[]] File does not exist:. *\.php
```

Ici on ne se préocuppe que des tentatives d'accès sur des fichiers ayant l'extension .php (à adapter au besoin).

IV-D - Les premiers tests

Suite à la mise en place des règles que nous avons vu, voici ce que vous pourriez voir dans le fichier de log de Fail2ban, lors d'échecs d'authentification :

```
[apache-noscript]
2008-06-01 20:50:45,868 fail2ban.actions: WARNING [ssh] Ban 90.XXX.77.241
2008-06-01 20:55:36,910 fail2ban.actions: WARNING [apache-noscript] Ban 90.XXX.77.242
2008-06-02 20:03:07,870 fail2ban.actions: WARNING [vsftpd] Ban 90.XXX.77.243
```

V - Pour aller plus loin

V-A - Création d'une nouvelle règle : protection d'un espace membre (PHP)

Dans cet exemple nous allons voir comment protéger un espace membre nécessitant un login et un mot de passe. Ci-dessous les deux exemples de scripts PHP nécessaires à la mise en place d'un espace membre (volontairement simplifiés) :

- -index.php : la page permettant de saisir le login et mot de passe

```
<html>
<body>
<form name="connexion" action="login.php" method="post">
<p>Login :<br><input type="text" name="logintext"></p>
<p>Password :<br><input type="password" name="passwordtext"></p>
<input name="envoi" type="submit" value="connect">
</form>
</body>
</html>
```

- -login.php : la page permettant le traitement des données et l'écriture d'un fichier de log dans le répertoire /var/www/test/log/webaccess.log Celui-ci va permettre a Fail2ban d'identifier les tentatives de connexions échouées.

```
<?php
$login="admin"; //le login
$password="admin"; //le mot de passe

if($_POST['logintext']==$login && $_POST['passwordtext']==$password) {
print('>html><body><p>Bienvenue dans l'espace membre</p></body></html>');
}else{
print('<html><body><p>Erreur</p></body></html>');
$fp = fopen ("log/webaccess.log", "a");
$log = date("M j G:i:s")." webaccess authentification failure; rhost=".$_SERVER['REMOTE_ADDR']."
 user=".$_POST['logintext']."\n";
fputs ($fp, $log);
fclose ($fp);
}
?>
```


Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2008 Developpez LLC. Tout droits réservés Developpez LLC. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents et images sans l'autorisation expresse de Developpez LLC. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

Nous allons créer une nouvelle règle dans Fail2ban : webaccess. Pour cela, nous allons créer un fichier webaccess.conf dans le répertoire /ect/fail2ban/filter.d/ contenant :

```
[Definition]

# Option: failregex
# Notes.: regex to match the password failures messages in the logfile. The
# host must be matched by a group named "host". The tag "<HOST>" can
# be used for standard IP/hostname matching.
# Values: TEXT
#
failregex = webaccess authentification failure; rhost=<HOST>
# Option: ignoreregex
# Notes.: regex to ignore. If this regex matches, the line is ignored.
# Values: TEXT
#
ignoreregex =
```

Puis nous allons créer une nouvelle section dans dans Fail2ban permettant de faire appelle à notre nouvelle régle. Editer le fichier /etc/fail2ban/jail.conf et ajouter la section ci-dessous :

```
[webaccess]

enabled = true
port = http
filter = webaccess
logpath = /var/www/test/log/webaccess.log
maxretry = 4
```

Rédemmarrer Fail2ban avec la commande /etc/init.d/fai2ban restart Et voila votre script est protégé contre les attaques.

V-B - Mise en place de la géolocalisation des adresses IP's

Le but de la géolocalisation dans notre cas et de pouvoir indiquer dans le fichier log de Fail2ban, de quel pays provient l'adresse IP bannie. Pour mettre en place cette géolocalisation nous allons utiliser la version gratuite de **GeoIP** (de Maxmind). Pour installer le paquet utiliser la commande :

```
apt-get install geoip-bin
```

Puis nous allons éditer le script « actions » de fail2ban situé dans :

```
/usr/share/fail2ban/server/actions.py
```

A la ligne 31 il faut modifié la script de la façon suivante :

```
import time, logging, commands
```

Puis a la ligne 139 il faut modifé la ligne de telle facon :

```
logSys.warn("[%s] Ban %s %s" % (self.jail.getName(), aInfo["ip"], commands.getstatusoutput('geoiplookup
 ' + aInfo["ip"])[1][23:]))
```


Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2008 Developpez LLC. Tout droits réservés Developpez LLC. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents et images sans l'autorisation expresse de Developpez LLC. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.

Et voila ce que vous obtiendrez dans votre fichier de log :

```
2008-04-04 18:06:40,530 fail2ban.actions: WARNING [vsftpd] Ban 202.XXX.115.229 IN, India
```

V-C - Intéraction de Fail2ban avec des programmes externes

Grace aux actions fournies dans Fail2ban il est possible d'intéragir avec d'autres programmes. Ces actions sont déclenchées par des évènements tel que le démarrage ou l'arret de l'application ou le bannissement-débanissement d'une adresse. Toutes les actions disponibles par défaut dans Fail2ban se trouvent dans le répertoire action.d. Dans le fichier jail.conf, 3 règles sont configurées par défaut dont une activée:

```
action_ = %(banaction)s[name=%(__name__)s, port="%(port)s", protocol="%(protocol)s]
```

Activée par défaut, elle permet le banissement en utilisant l'action iptables-multiport.

```
action_mw = %(banaction)s[name=%(__name__)s, port="%(port)s", protocol="%(protocol)s]
              %(mta)s-whois[name=%(__name__)s, dest="%(destemail)s", protocol="%(protocol)s]
```

Permet le banissement en utlisant l'action iptables-multiport et l'envoi d'un mail d'information avec l'action sendmail-whois.

```
action_mwl = %(banaction)s[name=%(__name__)s, port="%(port)s", protocol="%(protocol)s]
               %(mta)s-whois-lines[name=%(__name__)s, dest="%(destemail)s", logpath=%(logpath)s]
```

Cette règle permet le banissement en utilisant l'action iptables-multiport et l'envoi d'un mail d'information avec l'action sendmail-whois-lines ainsi que l'écriture dans un fichier de log.

Notre but ici sera de modifier l'action iptables-multiport afin d'y intégrer l'appel de la commande WHOIS et d'écrire le résultat dans un fichier de log. Pour ce faire nous allons éditer le fichier iptables-multiport qui se trouve dans le dossier action.d. L'évènement qui nous intéresse particulièrement pour exécuter notre commande WHOIS est le banissement. Le paragraphe est donc celui-ci:

```
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP
```

Nous allons ajouter une ligne afin d'écrire dans le fichier de log le résultat de la commande WHOIS:

```
actionban = iptables -I fail2ban-<name> 1 -s <ip> -j DROP
            whois --verbose -B <ip> >> /var/log/fail2ban.whois.log
```

VI - Conclusion

Fail2ban

Les sources présentées sur cette pages sont libres de droits, et vous pouvez les utiliser à votre convenance. Par contre la page de présentation de ces sources constitue une oeuvre intellectuelle protégée par les droits d'auteurs. Copyright © 2008 Developpez LLC. Tout droits réservés Developpez LLC. Aucune reproduction, même partielle, ne peut être faite de ce site et de l'ensemble de son contenu : textes, documents et images sans l'autorisation expresse de Developpez LLC. Sinon vous encourez selon la loi jusqu'à 3 ans de prison et jusqu'à 300 000 E de dommages et intérêts.