I. Objet

Sécurisé les serveurs contre les attaque « brute force » et « DOS ». Je vais utiliser la solution Fail2Ban.

II. Domaine d'application

Cette procédure s'applique aux utilisateurs de la société GSB.

III. Documents associés

AUCUN DOCUMENT ASSOCIE

IV. Définitions

Comment marche Fail2Ban ?

Fail2Ban est un logiciel libre permettant d'analyser des fichiers de logs et de déclencher des actions si certaines choses suspectes sont détectées. La grande force de Fail2Ban est sa grande modularité que cela soit au niveau des mécanismes de détections basées sur les expressions régulières ou sur les actions à mener qui peuvent aller de l'expédition d'un mail à la mise en place de règles de Firewall.

Fail2Ban se base sur un système de prisons (jails) que l'on peut définir, activer ou désactiver dans un simple fichier de configuration *(/etc/fail2ban/jail.conf).*
Une prison (jail) est composée, entre autres, des éléments suivants:

- **Nom du fichier** de log à analyser.
- **Filtre** à appliquer sur ce fichier de log (la liste des filtres disponibles se trouve dans le répertoire */etc/fail2ban/filter.d*). Il est bien sûr possible de créer ses propres filtres.
- **Paramètres** permettant de définir si une action doit être déclenchée quand le filtre correspond ("match"): Nombre de "matchs" (maxretry), intervalle de temps correspondant (findtime)...
- **Action** à mener si nécessaire. La liste des actions se trouve dans le répertoire */etc/fail2ban/action.d.* Il est également possible de créer ses propres actions.

Source : developpez.com

I. Installation de Fai2Ban

Je travail sur Debian 6, il suffit de saisir la commande suivante pour lancer l'installation :

```
aptitude install fail2ban
```

II. Protection contre les attaques "brute force" SSH

Si une machine cliente échoue 3 fois de suite lors de la saisie du login/password sur le serveur SSH alors on bloque l'accès au port TCP/SSH pendant 15 minutes.

La définition de cette prison (jail) est à faire dans le fichier */etc/fail2ban/jail.conf:*

```
[ssh]
enabled = true
port = ssh
filter = sshd
action = iptables[name=SSH, port=ssh, protocol=tcp]
logpath = /var/log/auth.log
maxretry = 3
bantime = 900
```

Un fois le filtre activé on relance Fail2Ban avec la commande :

```
service fail2ban restart
```

On peut voir son efficacité en regardant le fichier de log (par défaut sous*/var/log/fail2ban.log*):

```
:/etc/fail2ban$ tail -f /var/log/fail2ban.log
2012-02-23 15:03:48,069 fail2ban.actions: WARNING [ssh] Unban 21
2012-02-23 15:04:19,111 fail2ban.actions: WARNING [ssh] Ban 217.
2012-02-23 15:19:20,086 fail2ban.actions: WARNING [ssh] Unban 21
2012-02-23 15:19:54,129 fail2ban.actions: WARNING [ssh] Ban 217.
2012-02-23 15:34:55,102 fail2ban.actions: WARNING [ssh] Unban 21
2012-02-23 15:36:34,211 fail2ban.actions: WARNING [ssh] Ban 217.
2012-02-23 15:51:35,182 fail2ban.actions: WARNING [ssh] Unban 21
2012-02-23 15:52:41,258 fail2ban.actions: WARNING [ssh] Ban 217.
2012-02-23 16:07:42,234 fail2ban.actions: WARNING [ssh] Unban 21
2012-02-23 16:08:16,277 fail2ban.actions: WARNING [ssh] Ban 217.
```

ATTENTION :

Configuration inutile
lors de l'authentification par clef privée/public
(RSA)

III. Protection contre les attaques "brute force" FTP

Par default les informations de connexion au serveur FTP son indiquer dans */var/log/auth.log.* Pour simplifier la vision de c'est log, je vais les enregistrer dans le dossier */var/log/pure-ftpd/auth.log*

Éditer le fichier */etc/rsyslog.conf* et y mettre ceci:

```
ftp.*    /var/log/pure-ftpd/auth.log
```

Redémarre le service rsyslog:

```
service rsyslog restart
```

Si une machine cliente échoue 3 fois de suite lors de la saisie du login/password sur le serveur FTP alors on bloque l'accès au port TCP/FTP pendant 15 minutes.

Dans le fichier de configuration */etc/fail2ban/jail.conf* les informations de configuration concernant le service pure-ftpd n'est pas complété. Il faut donc les renseigner à la main.

```
[pure-ftpd]

enabled = true
port = ftp,ftp-data,ftps,ftps-data
filter = pure-ftpd
action = iptables[name=pure-ftpd, port=ftp,ftp-data,ftps,ftps-data, protocol=tcp]
logpath = /var/log/pure-ftpd/auth.log
maxretry = 3
bantime = 900
```

IV. Protection contre les attaques DOS (HTTP/GET)

Ces attaques se caractérisent par un nombre inhabituel de requêtes http ou https venant d'un même client (du moins d'une même adresse IP source). Le bute de ces attaque sont :

- L'inondation d'un réseau afin d'empêcher son fonctionnement ;
- La perturbation des connexions entre deux machines, empêchant l'accès à un service particulier ;
- L'obstruction d'accès à un service à une personne en particulier.

Pour empêcher cela nous allons crée une jail (prison). Editer le fichier suivant :

```
/etc/fail2ban/jail.conf
```

Puis ajouter les lignes dans la catégorie « http »

```
# Protect against DOS attack
# 360 requests in 2 min > Ban for 10 minutes

[http-get-dos]

enabled = true
port = http,https
filter = http-get-dos
logpath = /var/log/apache2/access.log
maxretry = 360
findtime = 120
action = iptables[name=HTTP, port=http, protocol=tcp]
bantime = 600
```

Comme vous pouvez le voir dans l'action inscrite, uniquement le port 80 (http) et bloquer en cas de déclanchement de cette prison (jail). Je vais empêcher toute connexion à notre serveur pendant une durée de 24h par exemple.
Pour interdire toutes les communications, je vais modifier la règle Iptable

```
action = iptables-allports[name=http-get-dos]
```

Et pou finir, modifier le temps (en second) du ban de l'adresse IP client
(86400 sec = 24H)

```
bantime = 86400
```

Le filtre « http-get-dos » n'est pas créer par default donc nous allons établir ce fichier de configuration.
Pour commencer, crée simple un fichier avec le nom suivant « http-get-dos.conf »

```
touch /etc/fail2ban/filter.d/http-get-dos.conf
```

Ensuite, éditer le fichier avec la commande « nano » ou « vi ».
Pour terminer, j'effectue un copier/coller des informations dans mon fichier http-get-dos.conf

```
# Fail2Ban configuration file

#

# Author: http://www.go2linux.org

#

[Definition]

# Option: failregex
# Note: This regex will match any GET entry in your logs, so basically all valid and not valid entries are a match.
# You should set up in the jail.conf file, the maxretry and findtime carefully in order to avoid false positives.
failregex = ^<HOST>.*"GET
# Option: ignoreregex
# Notes.: regex to ignore. If this regex matches, the line is ignored.
# Values: TEXT
#

ignoreregex =
```

N'oubliez pas de redémarrer le service après les modifications :

```
service fail2ban restart
```

Pour visionner les actions en temps réel du service fail2ban rien de plus simple avec la commande tail :

```
tail –f /var/log/fail2ban.log
```

V. Protection contre les attaques DFind

Vous avez très certainement dans les logs des attaques de type w00tw00t.at.ISC.SANS. Elles sont le fruit de kiddies utilisant un logiciel de scanning nommé DFind.
Si votre serveur est à jour et correctement configuré, vous ne devriez pas en avoir peur. Mais on va quand même s'occuper de ces attaques.

On créé maintenant le fichier qui contenant le regex de détection de la signature de Dfind :

```
touch /etc/fail2ban/filter.d/apache-w00tw00t.conf
```

On le rempli avec ce qui suit :

```
[Definition]

failregex = ^<HOST> -.*"GET \/w00tw00t\.at\.ISC\.SANS\.DFind\:\).*".*

ignoreregex =
```

Pour finir on édit le fichier jail.conf :

```
vi /etc/fail2ban/jail.conf
```

Et on y ajoute les lignes suivantes, elles on pour effet de bannir complètement pendant 24h l'IP des attaquant.

```
[apache-w00tw00t]

enabled  = true
filter   = apache-w00tw00t
action   = iptables-allports[name=apache-w00tw00t]
logpath  = /var/log/apache2/access.log
maxretry = 1
bantime  = 86400
```

On redémarre Fail2ban

```
service fail2ban restart
```

www.anthony-cochet.fr