cybersécurité

fail 2 ban

installer et configurer fail2ban

Introduction

Fail2Ban surveille les logs. Au bout d'un certain nombre de tentatives, il bannit l'adresse IP du hacker grâce à son IP.

Installation

Allez sur le serveur où vous souhaitez l'installer :

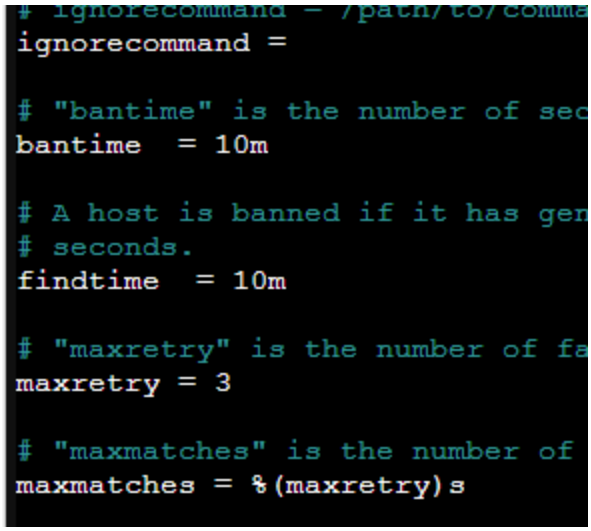
```
apt-get install fail2ban
apt-get install iptables
```

Configuration

Accédez au fichier de configuration nommé jail.conf :

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

Ensuite, descendez jusqu'ici et configurez selon vos préférences.



Après cela, redémarrez le service Fail2Ban :

```
systemctl restart fail2ban
systemctl status fail2ban
```

```
root@Proxy:/etc# systemctl status fail2ban.service
* fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendo
     Active: active (running) since Wed 2023-12-06 13:37:56 UTC; 40min ag
       Docs: man:fail2ban(1)
    Process: 61348 ExecStartPre=/bin/mkdir -p /run/fail2ban (code=exited,
   Main PID: 61349 (fail2ban-server)
      Tasks: 5 (limit: 17486)
     Memory: 11.3M
        CPU: 1.383s
     CGroup: /system.slice/fail2ban.service
             `-61349 /usr/bin/python3 /usr/bin/fail2ban-server -xf start
```

Test

Prenez un poste de "hacker" et tentez de vous connecter en SSH sur le serveur où Fail2Ban est installé :

```
ssh test@ipdusrv
```

Entrez des mots de passe incorrects. Normalement, après 3 tentatives, le message suivant devrait apparaître.

```
test@10.10.20.100's password:
test@10.10.20.100: Permission denied (publickey,password).
root@pirate:~#
```

Sur le serveur, si vous tapez la commande iptables -L, vous devriez voir l'adresse IP bannie pour le moment.

```
root@Proxy:/etc# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source
f2b-sshd   tcp  --  anywhere

Chain FORWARD (policy ACCEPT)
target     prot opt source

Chain OUTPUT (policy ACCEPT)
target     prot opt source

Chain f2b-sshd (1 references)
target     prot opt source
REJECT     all  --  10.10.20.45
chable
RETURN     all  --  anywhere
root@Proxy:/etc#
```