Infra Chapril - Demande #5114

Muscler un peu fail2ban

10/01/2021 12:01 - François Poulain

Statut:	Fermé	**Début:**	10/01/2021
Priorité:	Normale	**Echéance:**	
Assigné à:	François Poulain	**% réalisé:**	0%
Catégorie:		**Temps estimé:**	0.00 heure
Version cible:	Sprint 2021 janvier		

Description

Parmis les gens coupés par le fwall, il y en a qui abusent un peu. On peut leur couper les vivres. Par ex :

```
=(^-^)=root@maine:~# journalctl --since today | grep -i 'kernel: DROP' | grep -o 'SRC=[^ ]*' | sor
t | uniq -c | sort -h | tail -50
     40 SRC=45.129.33.15
     40 SRC=45.129.33.165
     40 SRC=45.129.33.169
     42 SRC=135.148.25.98
     42 SRC=45.129.33.82
     43 SRC=45.129.33.162
     44 SRC=130.61.116.104
     44 SRC=45.129.33.185
     44 SRC=45.129.33.5
     44 SRC=45.129.33.6
     46 SRC=192.168.1.57
     46 SRC=45.129.33.129
     46 SRC=45.129.33.8
     47 SRC=45.129.33.186
     48 SRC=45.129.33.9
     48 SRC=77.121.10.115
     49 SRC=185.107.96.3
     49 SRC=45.129.33.12
     49 SRC=45.129.33.84
     50 SRC=45.129.33.10
     54 SRC=51.89.191.147
     56 SRC=45.129.33.14
     57 SRC=103.145.13.58
     60 SRC=34.192.55.182
     61 SRC=45.129.33.59
     61 SRC=94.102.51.28
     63 SRC=45.155.205.103
     65 SRC=139.99.252.82
     65 SRC=146.88.240.4
     69 SRC=135.148.25.101
     74 SRC=94.102.49.191
     93 SRC=2a01:cb09:b062:6588:d1c8:eaaa:614a:1505
    158 SRC=108.179.242.155
    161 SRC=45.129.33.151
    183 SRC=51.222.143.1
    202 SRC=45.129.33.152
    212 SRC=45.129.33.40
    217 SRC=162.235.47.190
    261 SRC=106.240.239.26
    438 SRC=89.248.169.94
    439 SRC=80.82.70.25
    514 SRC=180.246.149.83
    574 SRC=195.54.161.151
    581 SRC=89.248.162.161
    727 SRC=171.224.180.78
   1398 SRC=76.192.120.115
   2447 SRC=192.168.1.4
```

```
   2447 SRC=192.168.1.5
   3301 SRC=79.124.62.82
  20288 SRC=240e:00f7:4f01:000c:0000:0000:0000:0003
```

Historique

#1 - 10/01/2021 12:15 - Laurent POUJOULAT

Pour information, il y a une jail qui se nomme "recidive" qui permet de virer ceux qui abusent (récidivent). En mettant 3 mois sur recidive on est généralement tranquille.

#2 - 10/01/2021 12:20 - Christian P. Momon

Ça a l'air bien ça \o/

#3 - 10/01/2021 12:32 - François Poulain

Les 192.168.1.4 et 192.168.1.5 c'est bootp qu'on n'utilise pas. On pourrait le désactiver (et quoi qu'il en soit whitelister ces deux ip dans fail2ban).

#4 - 30/01/2021 19:22 - François Poulain

J'ai ajouté sur bastion recidive et nginx-botsearch.

#5 - 30/01/2021 19:56 - François Poulain

- Statut changé de Nouveau à En cours de traitement

J'ai fait une tentative sur maine de bloquer celles et ceux qui abusent de se faire dropper des paquets. Je dupliquerai sur coon si c'est concluant.

#6 - 30/01/2021 22:33 - François Poulain

- Statut changé de En cours de traitement à Résolu

Ça a l'air concluant ; j'ai dupliqué sur coon.

#7 - 01/02/2021 01:24 - Christian P. Momon

- Assigné à mis à François Poulain

#8 - 03/02/2021 23:23 - Quentin Gibeaux

- Statut changé de Résolu à Fermé

#9 - 04/02/2021 04:35 - Christian P. Momon

- Version cible changé de Backlog à Sprint 2021 janvier