NewWorld SA

Recette - Services RebondSSH

Projet réalisé par SCAFFIDI FONTI Mathis et PERDIGON Théo

Date de modification 10 mars 2022

Sommaire

1. Service de rebond SSH

Un serveur SSH de rebond est accessible dans la DMZ publique, depuis l'extérieur, on y accède à l'adresse **p7.btsinfogap.org.**
Un script est ensuite disponible sur le serveur afin de rebondir sur les différents serveurs de la DMZ privé du réseau.

Le client est sur un réseau extérieur

```
theo@Theo13:~$ ssh mntnnc@p7.btsinfogap.org -p2222
mntnnc@p7.btsinfogap.org's password:
Linux REBOND 5.10.0-12-amd64 #1 SMP Debian 5.10.103-1 (2022-03-07) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Mar 10 16:53:39 2022 from 172.28.13.1
mntnnc@REBOND:~$
```

Le script de connexion se lance automatiquement

```
SCRIPT DE CONNEXION AUX SERVEURS

Voici la liste des serveurs :

     1  DNS
     2  DNS2
     3  DHCP
     4  DHCP2
     5  DCWebDev
     6  CentraleDB
     7  NAS
     8  RADIUS
     9  GLPI
    10  PROXY

Sur quel serveur voulez-vous vous connecter (Ctrl+C pour quitter) :
```

2. Fail2ban

Étant donné que le serveur est accessible depuis l'extérieur, il est doté d'une protection anti attaque en force brute grâce à la solution Fail2ban. L'attaquant se fera automatiquement bannir pendant 24h s' il dépasse 5 tentatives de connexion échouées.

Le Client est sur le réseau extérieur

```
theo@Theo13:~$ ssh mntnnc@p7.btsinfogap.org -p2222
mntnnc@p7.btsinfogap.org's password:
Permission denied, please try again.
mntnnc@p7.btsinfogap.org's password:
Permission denied, please try again.
mntnnc@p7.btsinfogap.org's password:
mntnnc@p7.btsinfogap.org: Permission denied (publickey,password).
theo@Theo13:~$
```

```
theo@Theo13:~$ ssh mntnnc@p7.btsinfogap.org -p2222
ssh: connect to host p7.btsinfogap.org port 2222: Connection refused
```

On constate donc, du côté serveur, que l'hôte à été banni après 3 tentatives

```
2022-03-10 17:05:08,619 fail2ban.filter         [2446]: INFO    [sshd] Found 172.28.13.1 - 2022-03-10 17:05:08
2022-03-10 17:05:12,097 fail2ban.filter         [2446]: INFO    [sshd] Found 172.28.13.1 - 2022-03-10 17:05:12
2022-03-10 17:05:15,040 fail2ban.filter         [2446]: INFO    [sshd] Found 172.28.13.1 - 2022-03-10 17:05:15
2022-03-10 17:05:15,157 fail2ban.actions        [2446]: NOTICE  [sshd] Ban 172.28.13.1
```