

FAIL2BAN & PATATOR

Bienvenue dans ce document qui vous montrera comment installer Fail2Ban et attaquer avec Patator.

Information :

Nom projet : Fail2ban & Patator

Personne(s) : Individuel

Date : Deuxième année de BTS (Novembre 2023)

Consigne 1 :

- Installer fail2ban
- Activer la protection de ssh
- Montrer en envoyant une capture d'écran que la règle sshd s'affiche bien quand vous exécutez la commande `sudo fail2ban-client status`

Consigne 2 :

- Installer patator
- Testez-le en essayant de vous connecter en ssh au serveur protégé par fail2ban
- Vous pouvez utiliser Rock You comme liste de mots de passe.
- Essayez d'attaquer le serveur de votre voisin (règle nat nécessaire)
- Montrer en envoyant une capture d'écran de patator qu'il a bien été bloqué par la machine protégée par fail2ban
- Ajoutez une capture de failban-client status ssh sur laquelle on voit l'IP de l'attaquant.

Qu'est-ce que c'est Fail2ban et Patator ?

Fail2Ban :

Fail2Ban est un logiciel open source conçu pour améliorer la sécurité d'un serveur en protégeant contre les attaques par force brute et d'autres types d'attaques automatisées sur les services réseau.

Le but principal de Fail2Ban est de surveiller les journaux du système à la recherche de motifs spécifiques liés à des tentatives d'authentification échouées, puis de prendre des mesures pour bloquer l'accès de l'adresse IP source de l'attaque.

Patator :

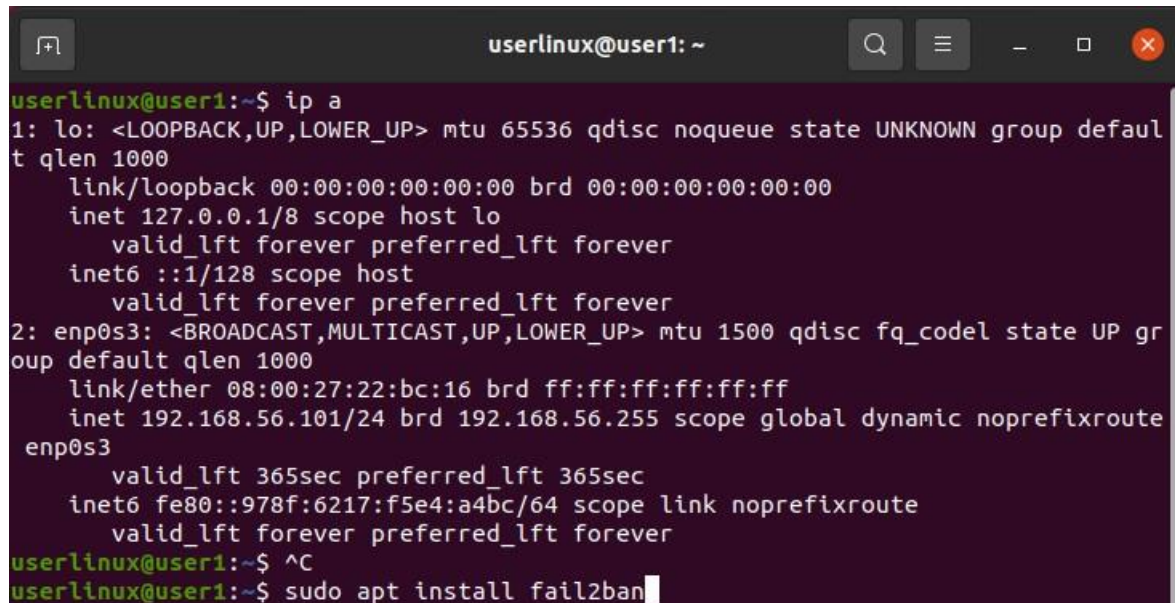
Patator est un outil de test de pénétration open source conçu pour effectuer des attaques par force brute contre divers protocoles et services. Son objectif est de tester la sécurité des systèmes en évaluant la résistance des mots de passe et la robustesse des mécanismes d'authentification. Patator est capable de cibler une large gamme de services, y compris des protocoles réseau tels que SSH, FTP, HTTP, SMB, et bien d'autres.

FAIL2BAN & PATATOR

Pensez à installer 2 machines (virtuels) différentes, les mettre à jour et installer dans les deux openssh.
Une machine sera pour utiliser Fail2ban (défenseur) et l'autre sera pour Pataor (attaquant).

Installer Fail2ban

Etape 1 : Installer les paquets Fail2Ban avec cette commande : **#sudo apt install fail2ban**



```
userlinux@user1: ~  
userlinux@user1:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
        valid_lft forever preferred_lft forever  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000  
    link/ether 08:00:27:22:bc:16 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.56.101/24 brd 192.168.56.255 scope global dynamic noprefixroute enp0s3  
        valid_lft 365sec preferred_lft 365sec  
    inet6 fe80::978f:6217:f5e4:a4bc/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
userlinux@user1:~$ ^C  
userlinux@user1:~$ sudo apt install fail2ban
```

FAIL2BAN & PATATOR

Etape 2 :

Une fois installer, vous devez l'activer avec ces commandes :

Systemctl start fail2ban

Systemctl enable fail2ban

Pour vérifier s'il est bien activé, saisissez la commande suivante :

Systemctl status fail2ban

```
userlinux@user1: ~  
userlinux@user1:~$ systemctl start fail2ban  
userlinux@user1:~$ systemctl enable fail2ban  
Synchronizing state of fail2ban.service with SysV service script with /lib/systemd/systemd-sysv-install.  
Executing: /lib/systemd/svsvd-sysv-install enable fail2ban  
userlinux@user1:~$ systemctl status fail2ban  
● fail2ban.service - Fail2Ban Service  
   Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor preset: enabled)  
   Active: active (running) since Wed 2023-12-20 22:06:38 CET; 1min 54s ago  
     Docs: man:fail2ban(1)  
  Main PID: 59745 (f2b/server)  
    Tasks: 5 (limit: 4919)  
   Memory: 12.6M  
    CGroup: /system.slice/fail2ban.service  
            └─59745 /usr/bin/python3 /usr/bin/fail2ban-server -xf start  
lines 1-9/9 (END)
```

Etape 3 : Une fois vérifier, vous pouvez voir les prisons actives avec cette commande :

sudo fail2ban-client status

```
userlinux@user1:~$ sudo fail2ban-client status  
[sudo] Mot de passe de userlinux :  
Status  
|- Number of jail:      1  
|- Jail list:          sshd  
userlinux@user1:~$
```

Passons a Patator :

Etape 1 : Installer patator et créer un fichier password.txt dans lequel vous métrerez des mots de passe : **sudo apt install patator**

FAIL2BAN & PATATOR

Etape2 : Saisissez la commande suivante pour que l'attaquant puisse tester tous les mots de passe chez le défenseur. Pour cela il faut indiquer le nom et l'IP du défenseur :

patator ssh_login host=192.168.56.101 user=Tourab password=FILE0 0=/home/azerty/password.txt

```
14:54:05 patator INFO - Hits/Done/Skip/Fail/Size: 0/12/0/12/12, Avg: 3 r/s, Time: 0h 0m 3s
root@azerty:/home/azerty# hostname -I
192.168.56.102
root@azerty:/home/azerty# patator ssh_login host=192.168.56.101 user=tourab password=FILE0 0=/home/azerty/password.txt
14:56:14 patator INFO - Starting Patator v0.7 (https://github.com/lanjelot/patator) at 2023-12-08 14:56 CET
14:56:14 patator INFO -
14:56:14 patator INFO - code size time | candidate | num | mesg
14:56:14 patator INFO - -----
14:56:17 patator INFO - 1 22 2.755 | bonjour | 1 | Authentication failed.
14:56:17 patator INFO - 1 22 2.769 | caca | 2 | Authentication failed.
14:56:17 patator INFO - 1 22 2.755 | jouer | 3 | Authentication failed.
14:56:17 patator INFO - 1 22 2.759 | manger | 4 | Authentication failed.
14:56:17 patator INFO - 1 22 2.756 | salut12 | 5 | Authentication failed.
14:56:17 patator INFO - 1 22 2.765 | bonsoir45 | 6 | Authentication failed.
14:56:17 patator INFO - 1 22 2.755 | cacabouda12 | 7 | Authentication failed.
14:56:17 patator INFO - 1 22 2.752 | pipi | 8 | Authentication failed.
14:56:17 patator INFO - 1 22 2.755 | garage | 9 | Authentication failed.
14:56:17 patator INFO - 1 22 2.758 | salutation | 10 | Authentication failed.
14:56:47 patator INFO - 1 23 30.064 | aurevoir | 11 | Authentication timeout.
14:56:47 patator INFO - 1 23 30.100 | 123456 | 12 | Authentication timeout.
14:56:47 patator INFO - Hits/Done/Skip/Fail/Size: 12/12/0/0/12, Avg: 0 r/s, Time: 0h 0m 33s
root@azerty:/home/azerty#
```

Etape 3 : Vérifier si sur la machine du défenseur fail2ban a pu bannir l'IP avec la commande suivante :

sudo fail2ban-client status sshd

```
10.0.2.15
tourab@tourab:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 0
| |- Total failed: 0
| '- File list: /var/log/auth.log
- Actions
| |- Currently banned: 0
| |- Total banned: 0
| '- Banned IP list:
tourab@tourab:~$ hostname -I
192.168.56.101
tourab@tourab:~$ sudo fail2ban-client status sshd
Status for the jail: sshd
|- Filter
| |- Currently failed: 1
| |- Total failed: 10
| '- File list: /var/log/auth.log
- Actions
| |- Currently banned: 1
| |- Total banned: 1
| '- Banned IP list: 192.168.56.102
tourab@tourab:~$
```

IP de l'attaquant

FIN