Simulation attaque/Bannissement adresseIP

Dinura Karunanayake

1 / Installation de Fail2ban sous Ubuntu

1) Fail2ban est un log dont l'objectif premier est de détecter des tentatives d'intrusion ou de connexions infructueuses sur un service et de bannir les adresses IP à l'origine de ces tentatives d'intrusion.
   Il est donc primordial de l'avoir avec nous pour éviter tout type d'attaques.
   Tout d'abord, nous devons bénéficier des droits administrateurs :

```
dkarunanayake@Ubo0:~$ su
Mot de passe :
```

2) Après avoir eu accès aux droits administrateurs, lançons l'installation de Fail2ban avec la commande suivante et de le confirmer :

```
apt install fail2ban

root@Ubo0:/home/dkarunanayake# apt install fail2ban
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  python3-pyinotify whois
Suggested packages:
  mailx monit sqlite3 python-pyinotify-doc
The following NEW packages will be installed:
  fail2ban python3-pyinotify whois
0 upgraded, 3 newly installed, 0 to remove and 467 not upgraded.
Need to get 444 kB of archives.
After this operation, 2 400 kB of additional disk space will be used.
Do you want to continue? [Y/n] Y
```

3) Voilà, Fail2ban est implémenté dans votre terminal. Maintenant, nous allons le mettre en place en commençant par lancer le service :

```
root@Ubo0:/home/dkarunanayake# systemctl start fail2ban
```

   Puis de créer le démarrage automatique :

```
root@Ubo0:/home/dkarunanayake# systemctl enable fail2ban
```

Et enfin de contrôler sa bonne installation :

```
root@Ubo0:/home/dkarunanayake# systemctl status fail2ban
* fail2ban.service - Fail2Ban Service
     Loaded: loaded (/lib/systemd/system/fail2ban.service; enabled; vendor pre>
     Active: active (running) since Mon 2023-12-04 09:17:32 CET; 45s ago
       Docs: man:fail2ban(1)
   Main PID: 7865 (f2b/server)
      Tasks: 5 (limit: 2269)
     Memory: 13.4M
     CGroup: /system.slice/fail2ban.service
             `-7865 /usr/bin/python3 /usr/bin/fail2ban-server -xf start

déc. 04 09:17:32 Ubo0 systemd[1]: Starting Fail2Ban Service...
déc. 04 09:17:32 Ubo0 systemd[1]: Started Fail2Ban Service.
déc. 04 09:17:32 Ubo0 fail2ban-server[7865]: Server ready
```

PS : si vous voyez le « active (running) » en vert, cela veut dire que votre fail2ban à bien été mis en place et prêt à bloquer des adresses.

On peut ainsi observer si les prisons ont bien été lancées correctement avec la commande suivante :

```
root@Ubo0:/home/dkarunanayake# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
```

2 / Installation de Open SSH sous Ubuntu

1) On aura besoin d'open ssh installé dans les 2 machines différentes afin de pouvoir simuler l'attaque et le bannissement. Pour cela, il vous suffit de faire la commande suivante :

```
apt install openssh-server
```

Vous pourrez aussi vérifier si le serveur ssh a bien été mis en place avec cette commande :

```
root@Ubo0:/home/dkarunanayake# systemctl status sshd
* ssh.service - OpenBSD Secure Shell server
     Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: >
     Active: active (running) since Mon 2023-12-04 09:12:42 CET; 6 days ago
       Docs: man:sshd(8)
             man:sshd_config(5)
   Main PID: 6262 (sshd)
      Tasks: 1 (limit: 2269)
     Memory: 1.0M
     CGroup: /system.slice/ssh.service
             `-6262 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups

déc. 04 09:12:42 Ubo0 systemd[1]: Starting OpenBSD Secure Shell server...
déc. 04 09:12:42 Ubo0 sshd[6262]: Server listening on 0.0.0.0 port 22.
déc. 04 09:12:42 Ubo0 sshd[6262]: Server listening on :: port 22.
déc. 04 09:12:42 Ubo0 systemd[1]: Started OpenBSD Secure Shell server.
```

3 / Installation de Patator sous Ubuntu

1) Depuis une autre VM Ubuntu, nous allons attaquer la machine contenant le fail2ban et l'open ssh.
   Pour cela, nous allons installer Patator, qui est un service d'attaque par force brut.
   Pour l'installer, il faut faire la commande suivante :

```
root@Ubu1:/home/patator# apt install patator
```

4 / Commencement de l'attaque

1) Après installation, il faut se placer dans notre bureau et créer un fichier qui contiendra tous les mots de passe que vous voulez faire tester au fail2ban pour vérifier si c'est le bon mot de passe ou non :
   La commande « cd » permettant de faire le déplacement et la commande « touch » permettant de créer le fichier.

```
root@Ubu1:/home/patator# cd Desktop
root@Ubu1:/home/patator/Desktop# touch mdp.txt
```

   Si vous ne possédez les droits d'écritures, vous pouvez modifier les droits du fichier grâce à la commande « chmod » :

```
root@Ubu1:/home/patator/Desktop# chmod 777 mdp.txt
```

2) Après avoir rempli votre fichier avec le nombre de mots de passe que vous souhaitez tester, nous allons passer au vif du sujet : l'attaque.
   Depuis la VM où nous avons installer patator, effectuer cette commande suivante pour attaquer la VM où on retrouve fail2ban :

```
root@Ubu1:/home/patator# patator ssh_login host=192.168.56.102 user=dkarunanayake password=FILE0 0=/home/patator/Desktop/mdp.txt
```

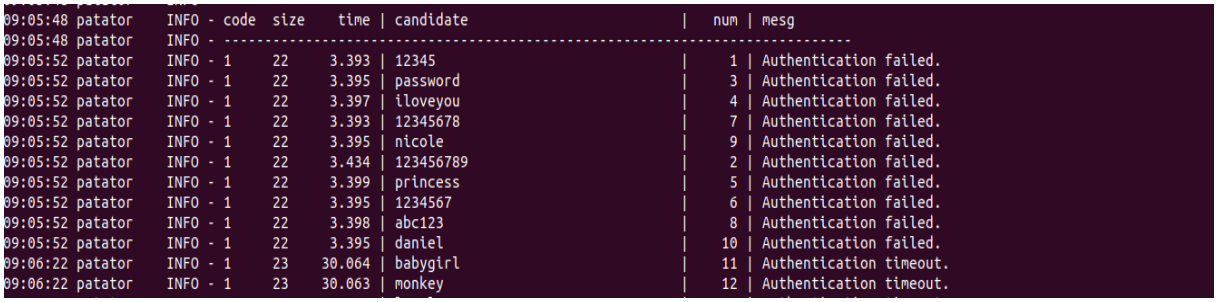
   Où le host doit être celui de la machine contenant fail2ban.

   Pour connaître l'adresse IP d'une machine, vous pouvez utiliser la commande suivante :

```
root@Ubo0:/home/dkarunanayake# hostname -I
192.168.56.102
```

Le user doit être le nom de la machine contenant fail2ban et le password doit contenir le chemin dans lequel se trouve le fichier mdp.txt que vous avez créer.

Après avoir exécuter cette commande, le terminal devrait vous afficher ceci :



Lorsqu'on retrouve le message « Authentification failed », cela signifie que l'adresse IP de l'attaquant à été banni dans la prison du fail2ban.

Cela peut être vérifié depuis la VM où l'on retrouve fail2ban grâce à la commande suivante :