FP
CREATION D'UN SERVEUR OPENCVE SUR DEBIAN

Table des matières

Introduction

OpenCVE est un logiciel permettant la remonté des failles, du niveau d'importance de ces dernières concernant les différents outils mis en place.

Ce logiciel va permettre d'avoir une remonté directe des informations concernant des failles et éviter des veilles technologiques chronophages.

I/ Récupération des fichiers + installation des prérequis

Pour installer OpenCVE, il y a des logiciels à installer avant via apt install et le pip3 sur requirements.txt.

```
apt install git
git clone https://github.com/opencve/opencve

OU

wget https://github.com/opencve/opencve/archive/refs/heads/master.zip
```

```
cd opencve/

apt install python3-pip redis postgresql postgresql-server-dev-13
pip3 install -r requirements.txt

cd /usr/lib/postgresql/13/bin/
pip3 install psycopg2

cd ~/opencve
python3.9 setup.py build
python3.9 setup.py install

# Si il n'y a pas assez de RAM, mais assez de place
fallocate -l 5G /swapfile
chmod 600 /swapfile
mkswap /swapfile
swapon /swapfile
```

II/ Postgres

```
su postgres
psql
\password                                   # Rentrer le mot de passe voulu
CREATE EXTENSION pg_trgm ;
CREATE DATABASE opencve;
CREATE USER opencve WITH PASSWORD 'opencve';
GRANT ALL PRIVILEGES ON DATABASE opencve TO opencve;
```

III/ Installation et configuration d'OpenCVE

```
opencve init
[*] Configuration created in /root/opencve/opencve.cfg

nano ~/opencve/opencve.cfg
...
Server_name =                                           # Ne rien mettre pour bind 0.0.0.0
...
...
database_uri = postgresql://test:test@IP:5432/opencve           # A modifier dans le fichier de conf
...
celery_broker_url = redis://0.0.0.0:6379/0
celery_result_backend = reids://0.0.0.0:6379/1

opencve upgrade-db
opencve import-data                         # /!\ Doit avoir un minimum de place et de 5Go RAM
```

IV/ Modifier la configuration de redis

```
nano /etc/redis/redis.conf

…
bind 0.0.0.0                                                    # A modifier dans le fichier de conf
…
```

V/ Création de l'admin OpenCVE

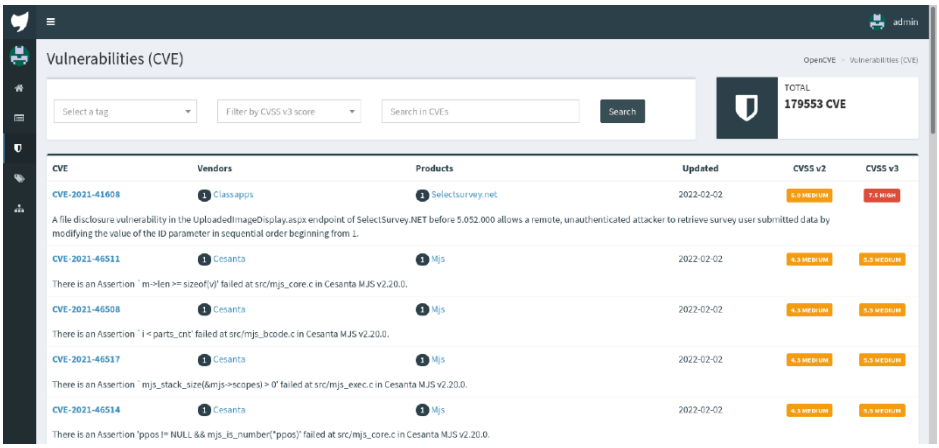
```
opencve create-user test test@test.test --admin
Password :                                                      # Rentrer le mot de passe
Repeat for confirmation :                                       # Rentrer à nouveau le mot de passe
[*] User test created
```

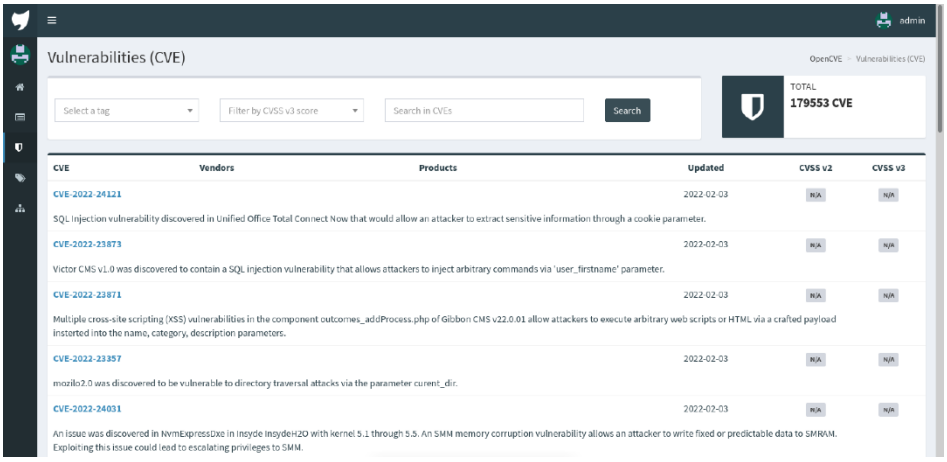
V/ Création des services de fonctionnement d'OpenCVE

```
cd /lib/systemd/system/
nano opencve-web.service              # Coller le script présent à la fin du document
nano opencve-worker.service           # Coller le script présent à la fin du document
nano opencve-beat.service             # Coller le script présent à la fin du document

systemctl daemon-reload
systemctl enable opencve-web
systemctl enable opencve-worker
systemctl enable opencve-beat
systemctl start opencve-web
systemctl start opencve-worker
systemctl start opencve-beat

/!\ Quand on redémarre un service, on redémarre les 3
```





Résultats sur la VM de test

Quand la faille est très récente – du jour même – il se peut que le score de gravité de la faille ne soit pas encore renseigné.

VI/ Installation de NTP (chrony)

```
apt install chrony
nano /etc/chrony/chrony.conf
...
server @IP du server
...

systemctl restart chronyd
chronyc sources                      # Vérifie la bonne détection du serveur ntp
chronyc makestep                     # Force la synchronisation du serveur ntp
timedatectl                          # Vérifie les infos de temps


                  --------- Si le local time est différent de l'UTC et du RTC ---------
rm /etc/localtime
ln -s /usr/share/zoneinfo/Europe/Paris /etc/localtime

timedatectl                          # Vérifie la bonne application des informations
```

VII/ Configuration serveur SMTP

```
nano opencve/opencve.cfg

[mail]
; Choices are 'smtp' or 'sendmail'
email_adapter = smtp ou sendmail

; The 'From' field of the sent emails
email_from = smtp@mail.fr

; Configuration to set up SMTP mails.
smtp_server = serveur-smtp
smtp_port = 25 ou 587 ou 465 ou 2525
smtp_use_tls = True ou False
smtp_username = smtp@mail.fr
smtp_password = password de smtp@mail.fr
```

VIII/ Configuration serveur Nginx

```
apt install nginx

nano /etc/gninx/cond.f/opencve-ssl.conf


upstream opencve_backend {
         server 127.0.0.1:8000;
}

server {
         listen 80;
         server_name opencve.fr;
         location / {
                  return 301 https://opencve.fr$request_uri;
         }
}

server {
         listen            443 ssl http2;
         listen            [::] :443 ssl http2;
         server_name       opencve.fr

         ssl_certificate "/etc/pki/nginx/certificat.crt";
         ssl_certificate_key « /etc/pki/nginx/private/key.key";
         ssl_session_cache shared:SSL:1m;
         ssl_session_timeout 10m;
         ssl_siphers HIGH:!aNULL:!MD5;
         ssl_prefer_server_ciphers on;

         location / {
                  proxy_pass http://127.0.0.1:8000

                  proxy_set_header X-Real-IP $remote_addr;
                  proxy_redirect off;
                  proxy_set_header Host $host;
                  proxy_set_header X-Forwarded-For $proxy_add_x_forwarded_for;
                  proxy_set_header X-Forwarded-Proto   $scheme;
                  proxy_set_header X-Forwarded-Host    $host;
                  proxy_set_header X-Forwarded-Port    $server_port;
                  proxy_set_header If-Modified-Since   $http_if_modified_since;
         }
}
```

IX/ Important

- Lors du déploiement du service OpenCVE, faire attention au pare-feu. Ajouter les règles nécessaires.
- Vérifier que les services démarrent bien au redémarrage du serveur (redis notamment), sinon enable le service
- Ajouter le serveur au sein d'un dns afin de permettre la résolution de nom

X/ opencve-web.service

```
[Unit]
Description=openCVE Web service

[Service]
User=root
ExecStart=/usr/bin/python3 /usr/local/bin/gunicorn -b 0.0.0.0:80 opencve.app:app

[Install]
WantedBy=multi-user.target
```

XI/ opencve-worker.service

```
[Unit]
Description=openCVE worker service

[Service]
User=root
ExecStart=/usr/bin/python3 /usr/local/bin/celery worker -A opencve.app:cel -l INFO

[Install]
WantedBy=multi-user.target
```

XII/ opencve-beat.service

```
[Unit]
Description=openCVE beat service

[Service]
User=root
ExecStart=/usr/bin/python3 /usr/local/bin/celery beat -A opencve.app:cel -l INFO

[Install]
WantedBy=multi-user.target
```