CTF Challenge: D(j)ocker

Conception du challenge

Pour ce challenge, j'ai créer un Dockerfile pour configurer mon conteneur. Je créer un utilisateur ctf-docker avec son mot de passe.

```
#Utiliser l'image de base Nginx
FROM nginx:alpine

RUN apk add --no-cache shadow

RUN useradd -m docker-ctf && \
    echo "docker-ctf:alejandro" | chpasswd

RUN mkdir -p /var/www/site-chall-docker
RUN echo "N4ninanNan4 naNinaNaNA" | base64 > /lib/security/pam_filter/alejandro.txt

# Copier le fichier de configuration Nginx personnalisé
COPY nginx.conf /etc/nginx/conf.d/default.conf
COPY site-chall-docker /var/www/site-chall-docker

# Exposer le port 8080
EXPOSE 8080
# Démarrer Nginx en mode premier plan
CMD ["nginx", "-g", "daemon off;"]
```

Je copie mon mon fichier nginx.conf dans le conteneur chall-docker avec deux locations. Le « / » qui pointe vers un template inutile, et un deuxième « /info » qui pointe vers les instructions du challenge.

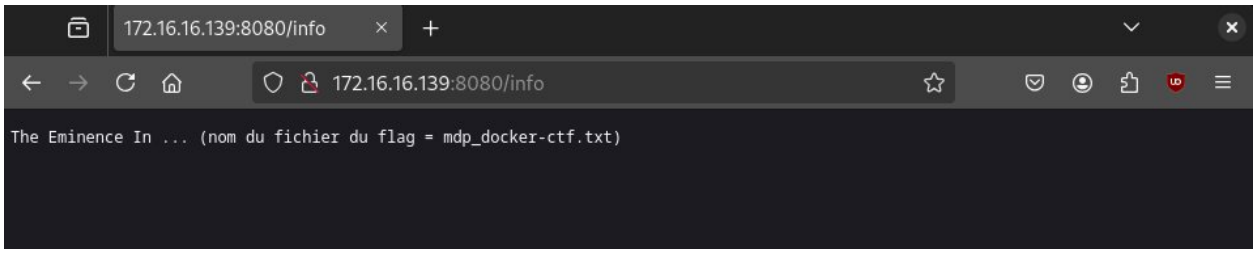
```
server {
   listen 8080;

   server_name 127.0.0.1;

   location / {
      root /var/www/site-chall-docker;
      index index.html;
      }

   location /info {
      default_type text/plain;
      return 200 'The Eminence In ... (nom du fichier du flag = mdp_docker-ctf.txt)';
   }
}
```

Je fais un « docker build –t chall-docker . « , ensuite un « docker run –d –p 8080:8080 chall-docker ».

Résolution du challenge

Dans ce challenge, l'objectif du joueur est de récupérer le FLAG au format CTF-DLS{...} contenu dans un fichier alejandro.txt (alejandro = mot de passe de l'utilisateur ctf-docker) du conteneur Docker. Le joueur vas devoir se connecter au serveur sur le port 8080 et tombera sur un template.

Le joueur devra faire un gobuster/dirbuster pour trouver la présence de la page /info, où les prochaines instruction lui sera données



La suite de « The Eminence In .. » est « Shadow », comme le fichier contenant les hash des mot de passe utilisateurs. Le joueur doit brute force le hash de l'utilisateur « ctf-docker » qui est « alejandro ». Sur cette page il est aussi dit que le fichier contenant le flag à le même nom que ce mot de passe, donc « alejandro.txt ». Le joueur devra donc faire un « find » de ce fichier et se trouve dans « /lib/security/pam_filter/ » avec son contenu encodé en base64.