CTF FACILE
Tools

Groupe 4

5 Novembre 2021

Outils utilisés

- Linux, Debian 10 pour l'OS
- Apache2 en tant que serveur web
- PostgreSQL pour la gestion de base de données
- NetFilter pour n'autoriser la réception de paquet que sur le port 80 (HTTP) et 22 (SSH)

Script de déploiement

```
#!/bin/bash

#On retrouvera la sortie standard dans install.out.log et les erreurs dans install.err.log
exec >/tmp/install.out.log 2>/tmp/install.err.log

echo "------------------ INSTALLATION DES PAQUETS NECESSAIRES ------------------"
#Mise a jour des paquets et installation des paquets requis pour le deploiement du CTF
apt update
apt install -y apache2 php postgresql postgresql-client php-pgsql git expect

echo "------------------ IMPORTATION DU GIT------------------"
#On importe le git contenant les sources pour le site web.
cd /home/debian/
git clone https://github.com/projetsecu/projetsecurite.git

#On copie les sources vers le dossier html/, c'est le dossier par defaut utilise par Apache
cp /home/debian/projetsecurite/ctf_facile/web/* /var/www/html/

#On supprime l'index.html qui est le fichier installe par defaut, ici on n'en a plus besoin
rm /var/www/html/index.html

#Comme toutes les actions sont realises par l'utilisateur root, les sources ne sont pas
    accessibles
#aux autres utilisateurs ce qui posent certains problemes au serveur pour l'acces a ces
    sources on change donc les droits
chmod 777 -R /var/www/html/


echo "------------------ CONFIGURATION DE POSTGRESQL------------------"
#On demarre le service PostgreSQL
systemctl enable --now postgresql

#On laisse un timing de 2 secondes le temps que le service demarre correctement
set timeout 2

#Creation du mot de passe pour l'utilisateur postgres, on utilise la seed du noyau
#on obtient donc un mot de passe "pseudo-aleatoire"
MYMSG=$(cat /proc/sys/kernel/random/uuid | sed 's/[-]//g' | head -c 6; echo;)

#On associe a l'utilisateur postgres le-dit mot de passe
sudo -u postgres psql  -c "ALTER USER postgres WITH password '$MYMSG'"

#On cree un nouvel utilisateur qui s'appelle admin
sudo -u postgres createuser -d admin

```

```
#On lui associe un mot de passe (c'est le mdp a trouver ^^)
sudo -u postgres psql  -c "ALTER USER admin WITH password 'kostadinkostadinovic'"

#On cree une base de donnee 'ctf_facile' dont le proprietaire est amdin
sudo -u postgres createdb ctf_facile -O admin
sudo -u postgres psql -d ctf_facile -c "CREATE TABLE users (id varchar(25) PRIMARY KEY, passwd
     varchar(50));" #Creation de la table avec id et password

#On ajoute a la database differentes donnees contenues dans un fichier .csv nomme bdd_users.
    csv
sudo -u postgres psql -U postgres -d ctf_facile -c "COPY users FROM '/home/debian/
    projetsecurite/ctf_facile/bdd_users.csv' WITH (FORMAT CSV, HEADER, DELIMITER ',', QUOTE
    ''');"

sudo -u postgres psql -c "alter database ctf_facile owner to admin;"
sudo -u postgres psql -d ctf_facile -c "alter table users owner to admin;"

#Creation d'une nouvelle table pour gerer le bannissement des adresses IP apres un certain
    nombre de requetes faites par celles-ci
sudo -u postgres psql -d ctf_facile -c "CREATE TABLE brute_force (IP varchar(15) PRIMARY KEY,
    count int, first_fail int);"
sudo -u postgres psql -d ctf_facile -c "alter table brute_force owner to admin;"

#On redemarre le service PostgreSQL
systemctl restart postgresql

echo "------------------ DEMARRAGE DU SERVEUR WEB APACHE 2------------------"
#On demarre Apache
systemctl start apache2

echo "------------------ CONFIGURATION DES REGLES DE FILTRAGE IP------------------"
#OUVERTURE D'UN PORT SSH ET D'UN PORT HTTP UNIQUEMENT

#Suppression de toutes les regles deja existantes
iptables -F
iptables -X

#On accepte les paquets en loopback
iptables -t filter -A INPUT -i lo -j ACCEPT

#On accepte les paquets arrivant et partant du port 22 et 80 (port ssh, port http) on jette
    tout le reste
iptables -A INPUT -p tcp -m tcp -m multiport ! --dports 80,443,22 -j DROP
iptables -I INPUT -p tcp --dport 22 -m state --state NEW -m recent --set
iptables -I INPUT -p tcp --dport 22 -m state --state NEW -m recent  --update --seconds 300 --
    hitcount 4 -j DROP

#ON MODIFIE LES FICHIERS SUDOERS ET SSHD_CONFIG
 #update /etc/sudoers.d/90-cloud-init-users
 #take away sudo for default ubuntu user
set timeout 2
SUDOER_TMP="$(mktemp)"
sudo cat /etc/sudoers.d/90-cloud-init-users > ${SUDOER_TMP}
echo 'debian ALL=(ALL) ALL' > "${SUDOER_TMP}"
sudo visudo -c -f ${SUDOER_TMP} && sudo cat ${SUDOER_TMP} > /etc/sudoers.d/90-cloud-init-users
SUDOER_TMP="$(mktemp)"
sudo cat /etc/sudoers.d/debian-cloud-init > ${SUDOER_TMP}
echo 'debian ALL=(ALL) ALL' > "${SUDOER_TMP}"
sudo visudo -c -f ${SUDOER_TMP} && sudo cat ${SUDOER_TMP} > /etc/sudoers.d/debian-cloud-init
rm "${SUDOER_TMP}"

set timeout 2
#On autorise la connexion ssh avec l'utilisateur root qui est desactive par defaut
sed -i -e 's/#PermitRootLogin prohibit-password/PermitRootLogin yes/g' /etc/ssh/sshd_config
/etc/init.d/ssh restart

#On cree un mot de passe a l'utilisateur root
ROOT_PASSWD=$(expect -c "
set timeout 5
spawn passwd root
expect \"New password:\"
send \"kostadinkostadinovic\r\"
expect \"Retype new password:\"
send \"kostadinkostadinovic\r\"
expect eof")

```

```
112 echo "$ROOT_PASSWD"
113
114
115 #ON AJOUTE LE FLAG
116 touch /root/flag.txt
117 echo "P9GuZi82kG69V4idd8HiR495Gz3mrJmJ" > /root/flag.txt
118
119 #On supprime le git on n'en a plus besoin
120 rm -r /home/debian/projetsecurite/
```

Commandes à connaître :

- nmap : https://tryhackme.com/room/furthernmap
- ssh : ssh user@addressIp