CLUB
ETHICAL HACKING

Edition 2019/2020

Séance #4
Escalation de privilèges
- Linux -

12 Février 2020

Point de contact

Rémi ALLAIN remi.allain@cyberprotect.one

Daniel DIAZ daniel.diaz@cyberprotect.one

Pré-requis

Docker est installé sur ma machine
Sinon, je l'installe en suivant cette procédure: https://docs.docker.com/install

Je sais évoluer dans un environnement Linux
Sinon je lis ce cours: https://openclassrooms.com/fr/courses/43538-reprenez-le-controle-a-laide-de-linux

Je connais les commandes Linux "de base" *(ls, cat, ssh, sudo, etc.)*
Sinon j'utilise cette cheatsheet: https://juliend.github.io/linux-cheatsheet/

Guide rapide sur l’escalation de privilège

“L’escalation de privilèges est un mécanisme permettant à un utilisateur d'obtenir des privilèges supérieurs à ceux qu'il a normalement.”

Guide rapide sur l'escalation de privilège

Étape 1: Où sommes nous ?

```
>> cat /etc/lsb-release   # OS Info
>> uname -a               # OS Info
>> ls -a
>> pwd
```

Étape 2: Qui suis-je ?

```
>> whoami
>> id
>> who
>> w
>> last
```

Guide rapide sur l'escalation de privilège

Étape 3: Quels sont mes droits ?

```
>> sudo -l
>> whoami
>> id
```

Étape 4: J'observe mon environnement

```
>> env
>> history
```

Guide rapide sur l'escalation de privilège

Étape 5: l'Indiana Jones des fichiers

```
>> ls -la ~/.ssh/
>> cat ~/.bash_history
>> grep -l -i pass /var/log/*.log
>> head /var/mail/root
```

Étape 6: Comment et vers qui la machine reçoit / envoie des connexions

```
>> ifconfig -a
>> ip addr show
>> arp -a
>> route
>> netstat -antp
>> iptables -L
```

Guide rapide sur l'escalation de privilège

Étape 7: J'analyse les programmes et les services

```
>> ps aux
>> top
>> ls -la /etc/cron*
>> dpkg -l
>> sudo -V / httpd -v / php -v# check program version (-V, -v ou --version)
```

Étape 8: Je s'appel root !

J'essaie de trouver des faiblesses, des vulnérabilités, pour passer "root".

Votre mission ....

Vous devez réussir à passer “root” sur chacun des 10 challenges.

Dans le fichier “/root/flag” se trouve un code qui permet de valider le challenge.

Les challenges sont répartis par niveaux de difficultés (10).

Généralement, on commence par le niveau 1 ... 👍

L’astuce du chef: prenez votre temps et soyez méthodique.

C'est parti !

Installation *(disponible à partir du 2020-02-12)*

```
>> git clone https://github.com/Club-Ethical-Hacking-CLUSIR-Rhone-Alpes/2020-02-12
>> cd 2020-02-12/challenge
>> docker-compose build -q
>> docker-compose up -d
>> chmod u+x start_level
```

Utilisation

```
>> ./start_level 1                          # remplacer '1' par le numéro du challenge
>> level1@localhost's password: level1      # remplacer '1' par le numéro du challenge
```

Des questions ? → remi.allain@cyberprotect.one