##KIOPTRIX: LEVEL 1.3 (#4)

Today, we'll be looking at the Kioptrix level 4 machine on vulnhub.

You can download the machine [here](https://www.vulnhub.com/entry/kioptrix-level-13-4,25/).

Let's scan the machine with nmap.

```
%%%(root 2kali)-[~/kioptrix4] %%# nmap -sS -A 192.16
```

Browsing the machine on port 80 we find a login page.

`![](pics/pic1.png)`

We can also see that the machine is running smb.

Let's use enum4linux to find out more information.

```
enum4linux 192.168.88.134 -a
```

Great! We found three usernames.

`![](pics/pic2.png)`

Let's test the login form for sql injection.

we'll use `1 'OR 1=1-- -` as the password.

We got john's password.

`![](pics/pic3.png)`

We also got Robert's password.

`![](pics/pic4.png)`

Let's ssh into the machine as john.

Looks like we are in a restricted shell.

`![](pics/pic5.png)`

Let's try to escape that shell.

I tried a bunch of commands then I tried to cd into a directory and I found that we are using lshell.

`![](pics/pic6.png)`

I searched online and found a way to escape lshell with echo [here](https://www.aldeid.com/wiki/Lshell).

`![](pics/pic7.png)`

You can also read this great [article](https://fireshellsecurity.team/restricted-linux-shell-escaping-techniques/) about escaping restricted shells.

Let's use linpeas for local enumeration and try to get root.

From the results of the script, we see that we can log into mysql as root with no password.

`![](pics/pic8.png)`

```
mysql -u root -p
```

We got in!

`![](pics/pic9.png)`

Let's give john admin priviliges.

```
select_exec('usermod -a -G admin john');
```

`![](pics/pic10.png)`

Now, we can just use `sudo su`.

We are root.

`![](pics/pic11.png)`