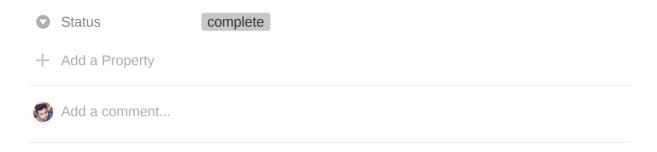
# **Kioptrix Level 4**



## Figuring out the machine IP address

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

### Nmap Scanning on the IP address



Resuts of the nmap scan in normal format

#### Possible network attack vectors and explanations

<u>Aa</u> Name	Status	<b>≡</b> Reason
139, 445 SMB	not-exploited	No known exploits, tried normally browsing the available shares and found nothing.
80	exploited	Used SQLi to get into the application to get passwords for login as well as for SSH
+ New		

#### 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 v
```

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 <a href="https://www.exploit-db.com/exploits/39632">https://www.exploit-db.com/exploits/39632</a> this exploit which helped me to escape to a bash shell. Ref:

https://fireshellsecurity.team/restricted-linux-shellescaping-techniques/

Using the command <code>grep -i 'mysql' -r ./ .</code> 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.

**←**