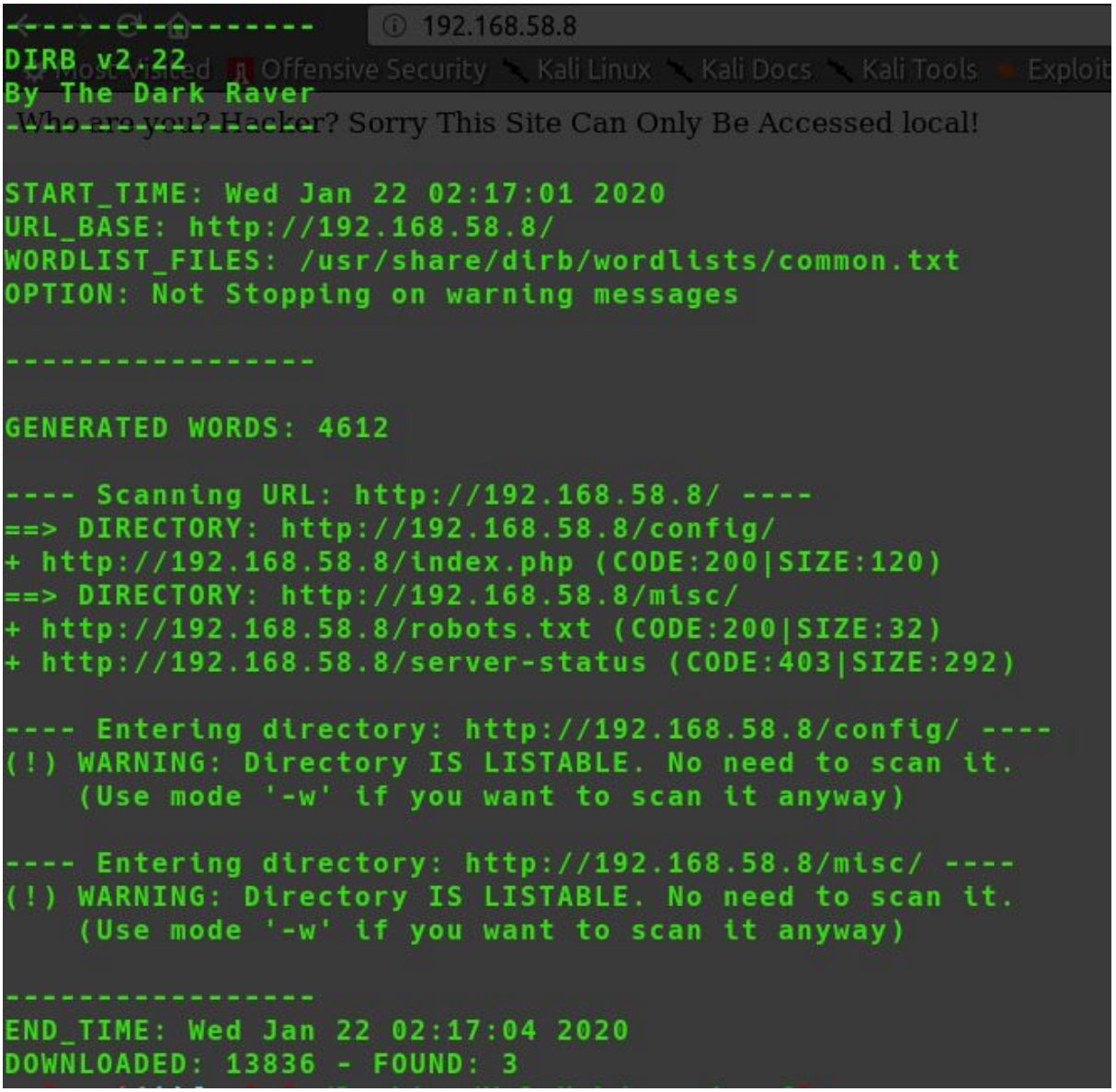
Writeup for Me and My Girlfriend 1 in (Vulnhub) by TyPh0oN

1.I use netdiscover for finding ip address

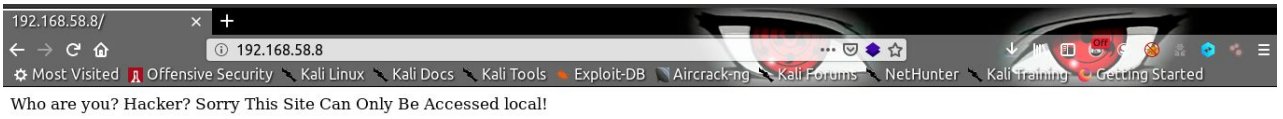
2.I scan this ip with nmap for more info

```
Starting Nmap 7.80 ( https://nmap.org ) at 2020-01-22 02:16 +0630
Nmap scan report for 192.168.58.8
Host is up (0.00017s latency).
Not shown: 997 closed ports
PORT   STATE    SERVICE VERSION
22/tcp open     ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 57:e1:56:58:46:04:33:56:3d:c3:4b:a7:93:ee:23:16 (DSA)
|   2048 3b:26:4d:e4:a0:3b:f8:75:d9:6e:15:55:82:8c:71:97 (RSA)
|   256 8f:48:97:9b:55:11:5b:f1:6c:1d:b3:4a:bc:36:bd:b0 (ECDSA)
|_  256 d0:c3:02:a1:c4:c2:a8:ac:3b:84:ae:8f:e5:79:66:76 (ED25519)
53/tcp filtered domain
80/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:F1:B5:AA (Oracle VirtualBox virtual NIC)
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 3.2 - 4.9
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT     ADDRESS
1   0.17 ms 192.168.58.8

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 12.00 seconds
```

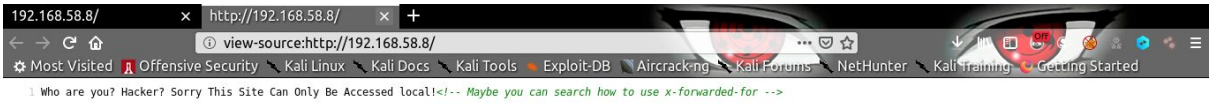
3.i use dirb for find subdirectory in this web


192.168.58.8
Most Visited
Offensive Security
Kali Linux
Kali Docs
Kali Tools
Exploit
DIRB v2.22
By The Dark Raver
Who are you? Hacker? Sorry This Site Can Only Be Accessed local!
START_TIME: Wed Jan 22 02:17:01 2020
URL_BASE: http://192.168.58.8/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages
GENERATED WORDS: 4612
---- Scanning URL: http://192.168.58.8/ ----
==> DIRECTORY: http://192.168.58.8/config/
+ http://192.168.58.8/index.php (CODE:200|SIZE:120)
==> DIRECTORY: http://192.168.58.8/misc/
+ http://192.168.58.8/robots.txt (CODE:200|SIZE:32)
+ http://192.168.58.8/server-status (CODE:403|SIZE:292)
---- Entering directory: http://192.168.58.8/config/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
---- Entering directory: http://192.168.58.8/misc/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
(Use mode '-w' if you want to scan it anyway)
END_TIME: Wed Jan 22 02:17:04 2020
DOWNLOADED: 13836 - FOUND: 3

I see this web page

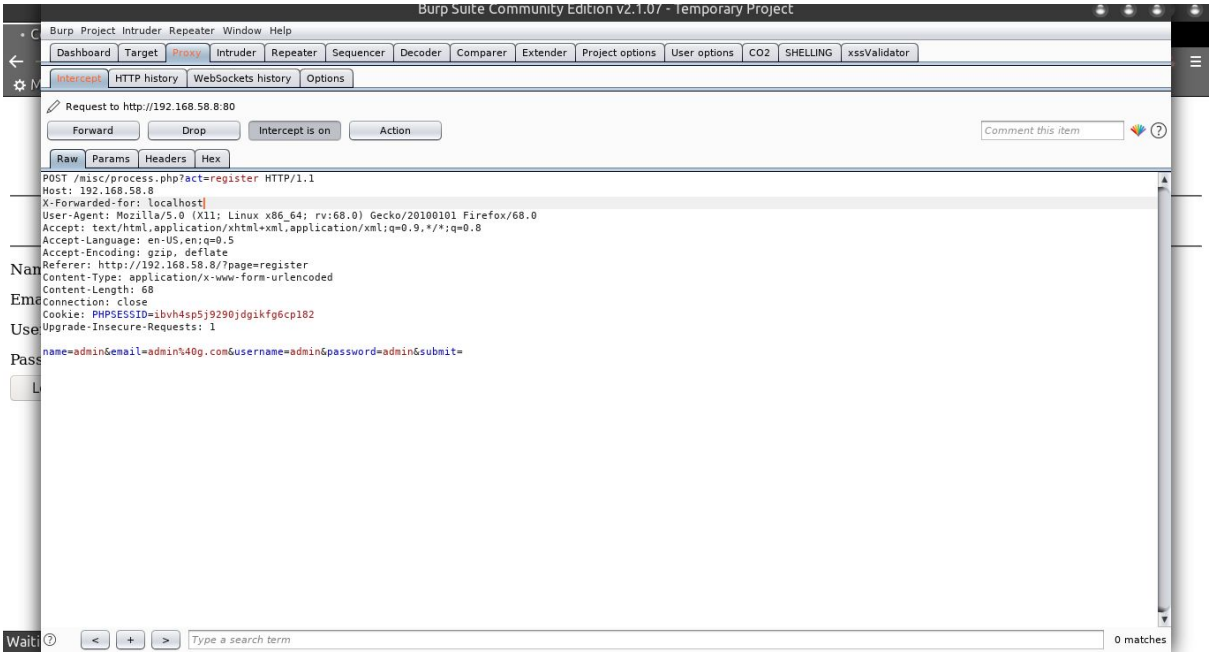


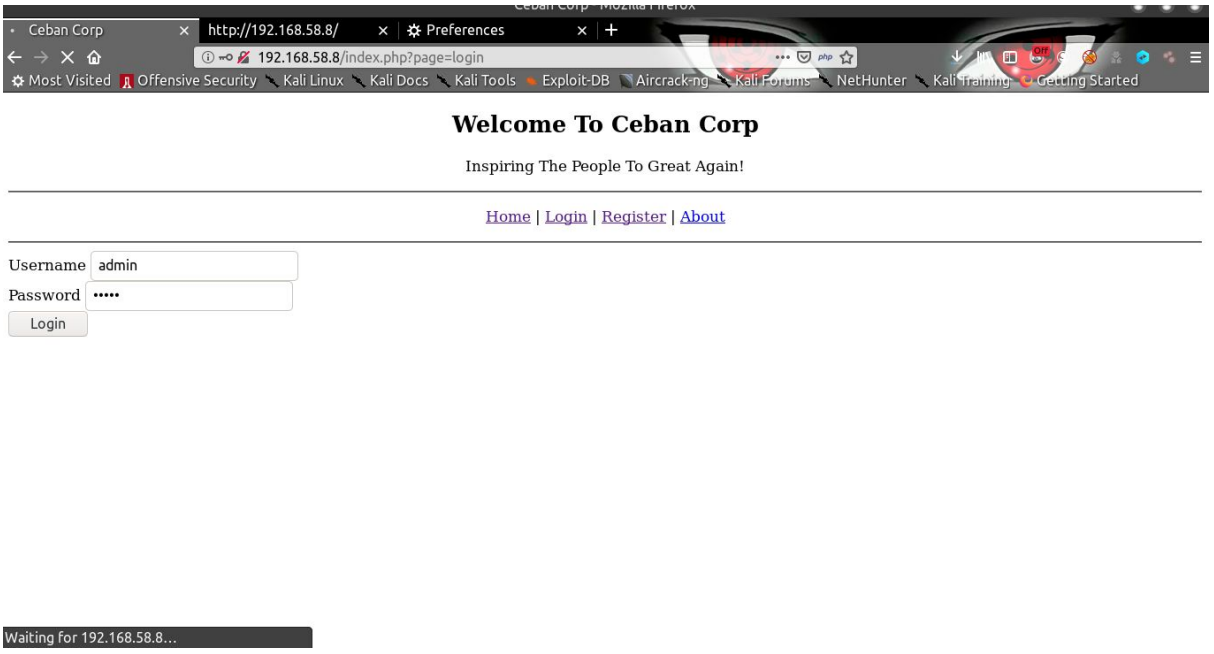
In this time,I check the source code



I use burp suite for intercepting and i add X-Forwarded-for: localhost
In this time ,The Web Page is change like this

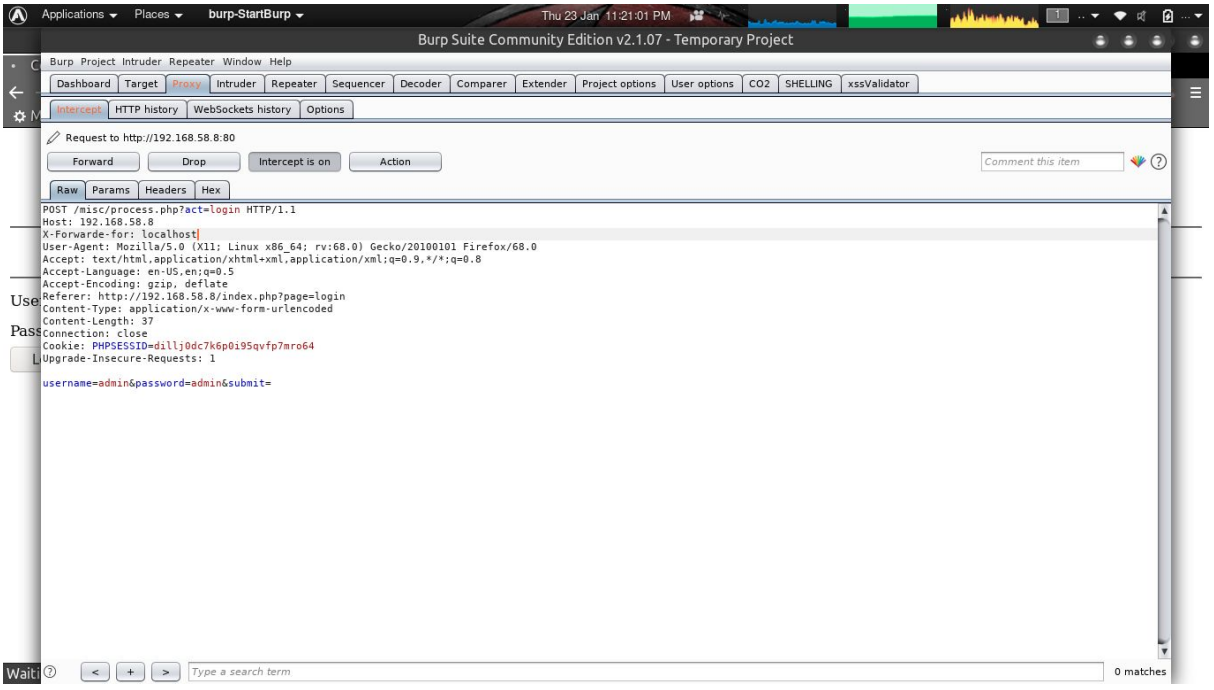
I click register for registration account
But we need to add X-Forwarded-for: localhost





I register with admin:admin

We need to add X-Forwarde-for: localhost

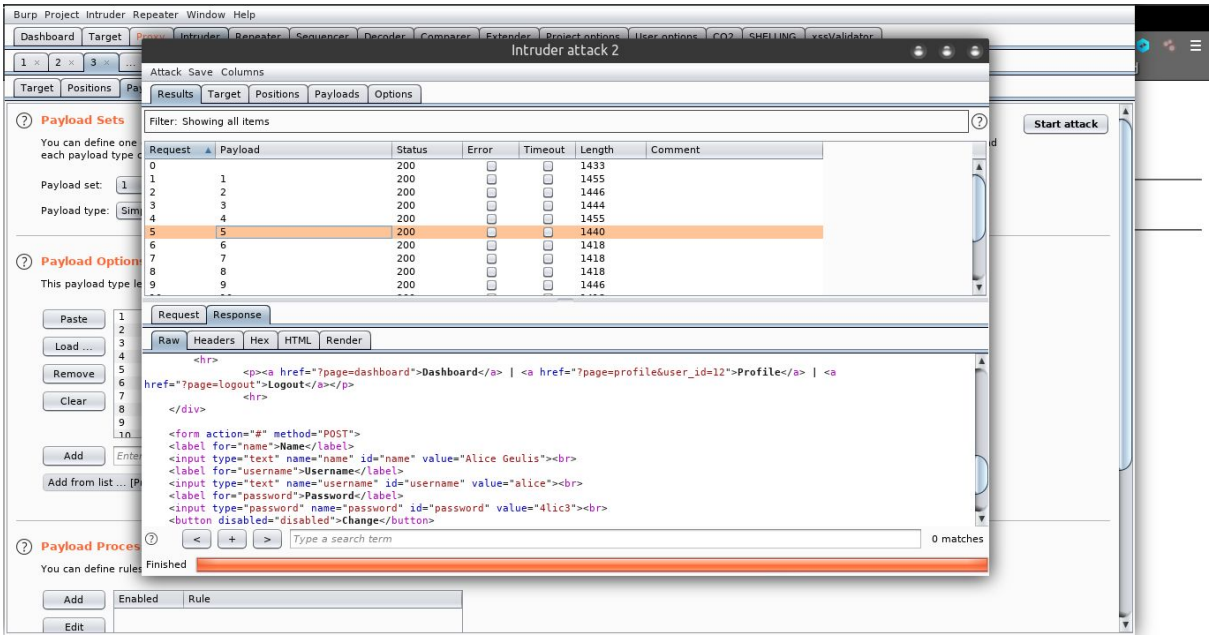


I use this username and password to login

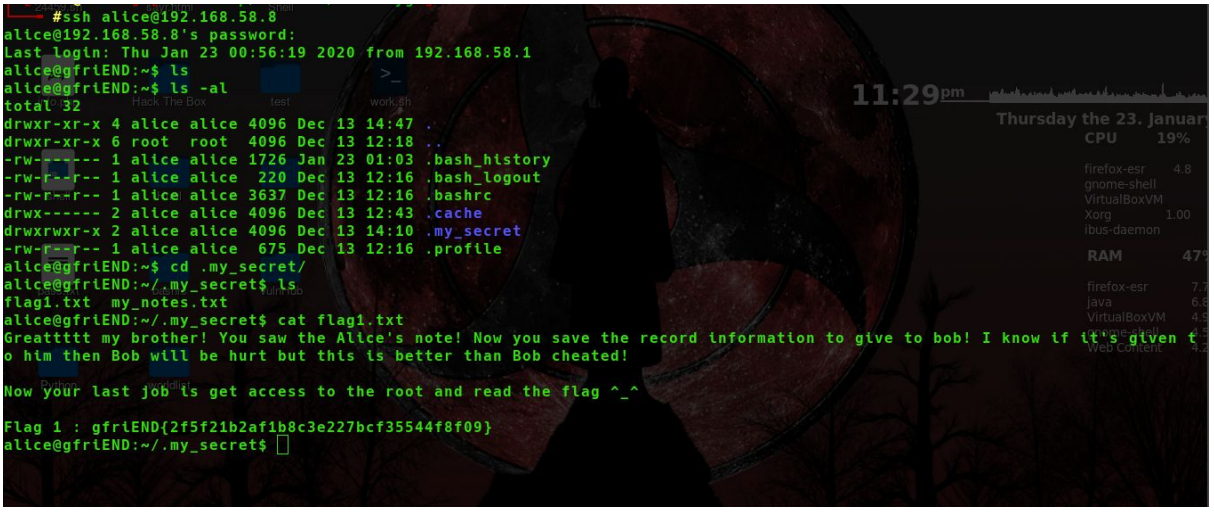
In these time,the url address bar show like this
http://192.168.58.8/index.php?page=profile&user_id=12

I use burp suite to brute force this id

After brute forcing
I see username alice and password 4lic3 in id 5

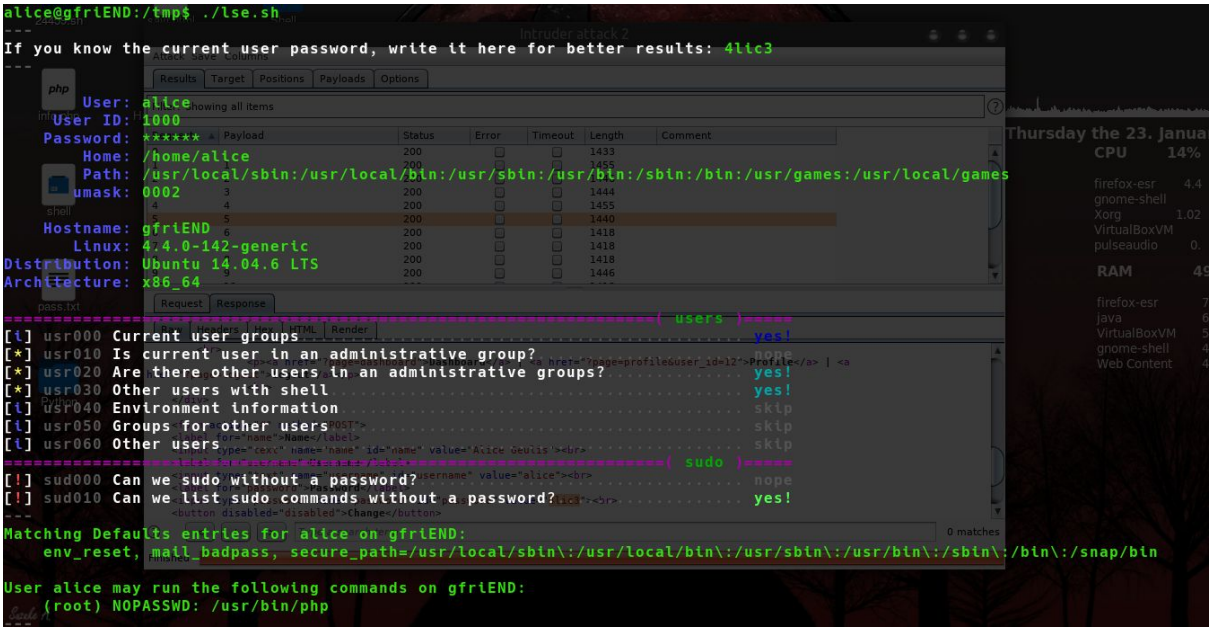


I try to login with this username and password
lucky i got ssh login with this username and password
#SSH alice@192.168.58.8
Password is 4lic3
After ssh login
I found one secret folder and i found flag1 in this folder



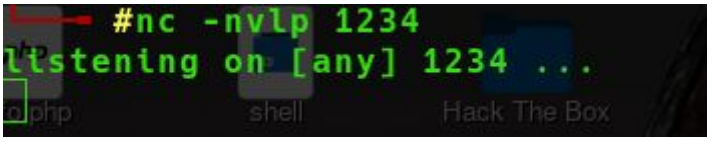
I downloaded **linux-smart-enumeration**

script and run this script



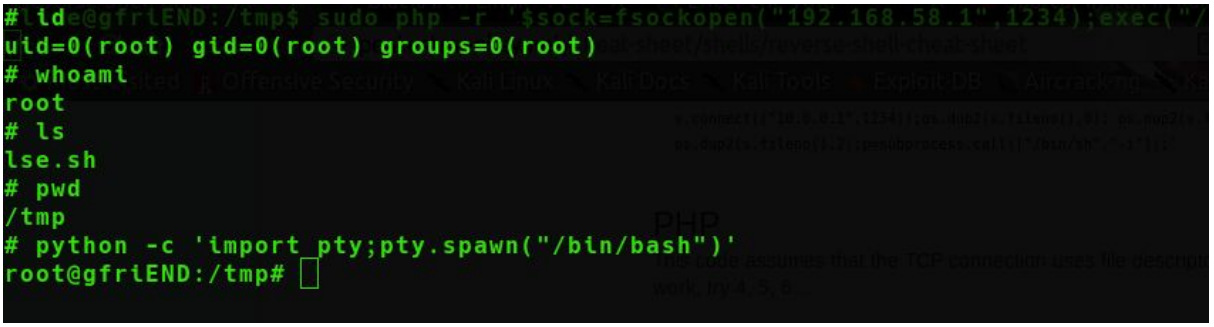
I found php can run without password

In this time i use netcat to listen



I use php reverse shell to get root access in this lab

Now i get root access



Final flag (flag2 is locate in the root dir)

Thank for giving your valuable time to read my writeup (TyPh0oN)