RESUMO

“Pickle Rick” é uma máquina de nível fácil vulnerável a ferramentas de força-bruta e com permissões de usuários mal configuradas, permitindo a inicialização de uma shell reversa e fácil obtenção de privilégios root.

RECURSOS UTILIZADOS

- Nmap

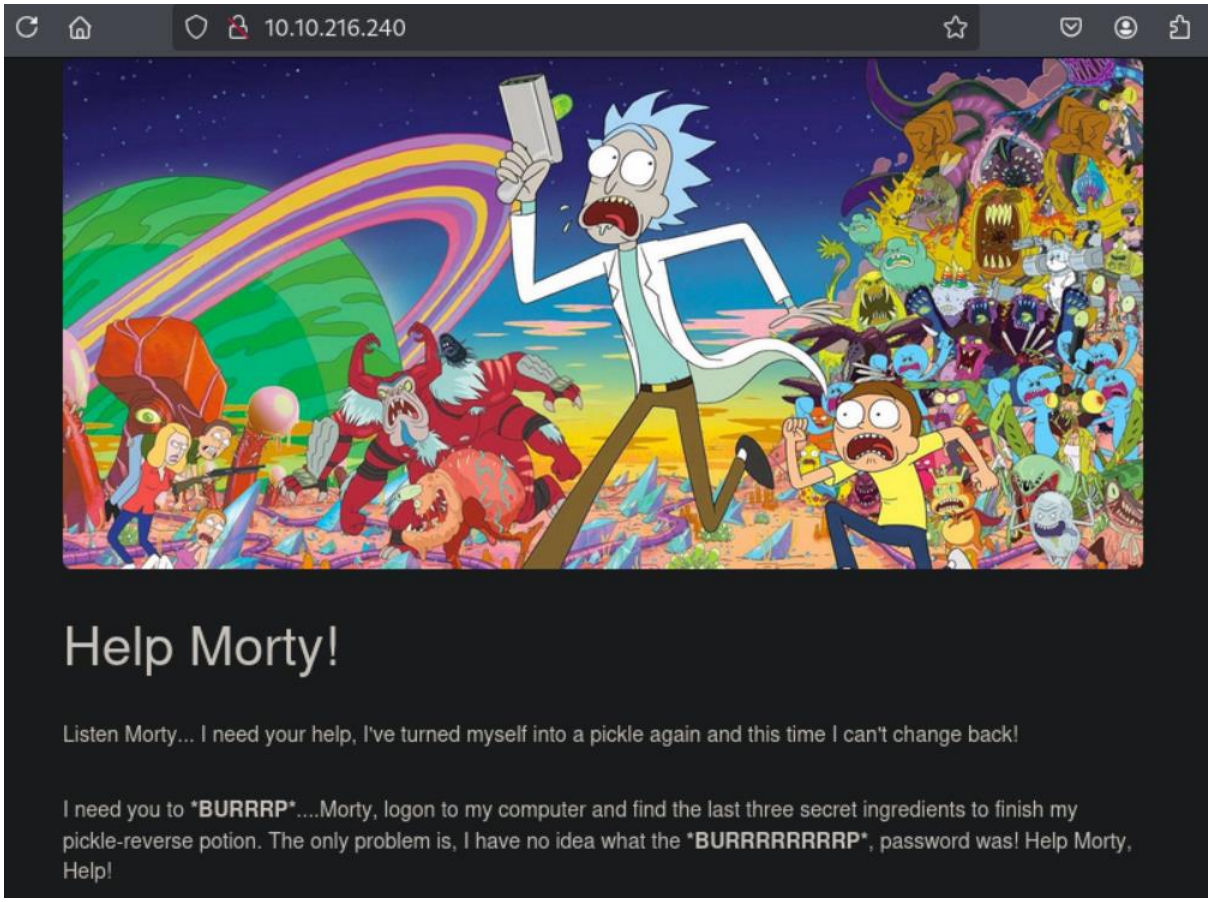
- Gobuster

- Netcat

RECONHECIMENTO

Escaneando o IP da máquina alvo com Nmap, percebem-se dois serviços rodando na máquina alvo, dentre eles um servidor HTTP, podendo ser acessado por um navegador e proporcionando a página inicial abaixo.

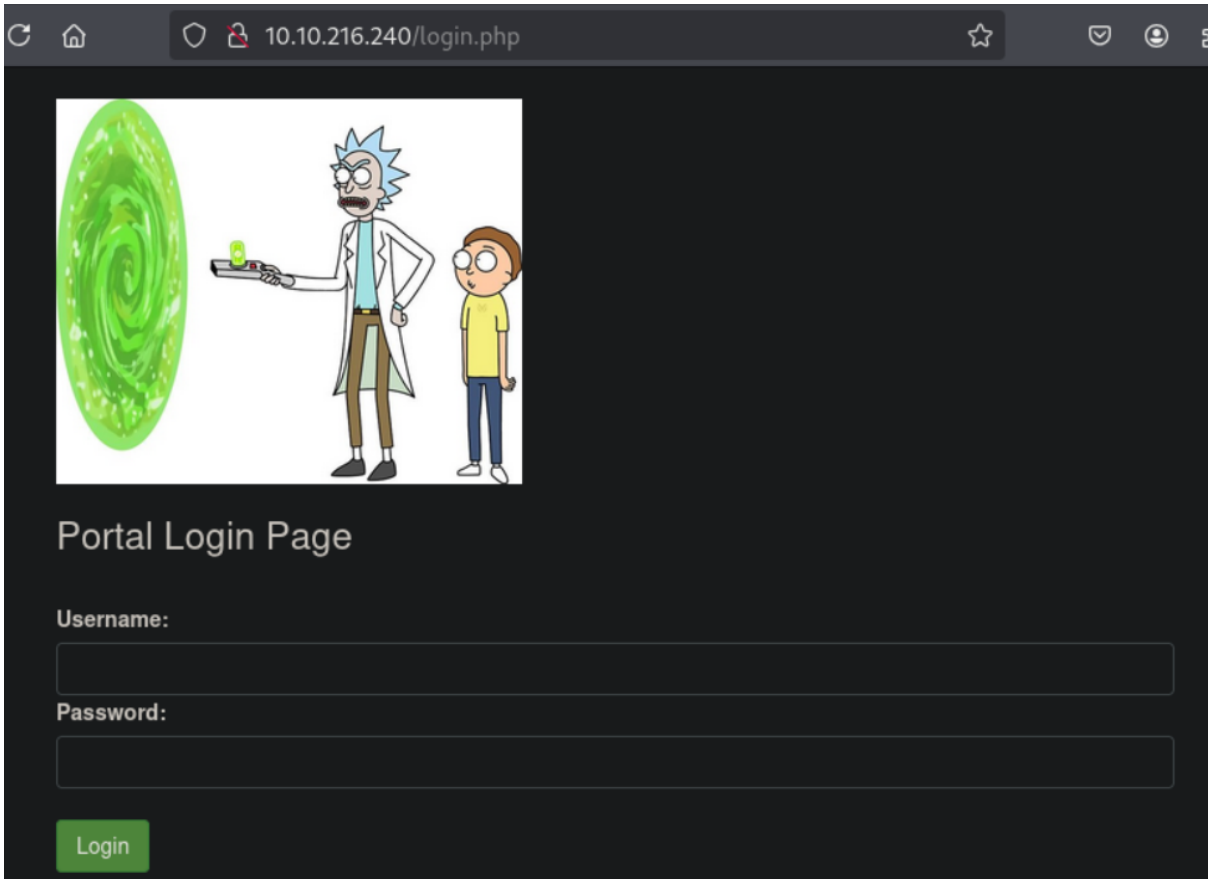
```
└─$ nmap -sV 10.10.216.240 -p1-600
Starting Nmap 7.95 ( https://nmap.org ) at 2025-05-06 10:01 -03
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 50.00% done; ETC: 10:02 (0:00:07 remaining)
Stats: 0:00:14 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 100.00% done; ETC: 10:01 (0:00:00 remaining)
Nmap scan report for 10.10.216.240
Host is up (0.25s latency).
Not shown: 598 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.11 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
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 17.01 seconds
```



FORÇA-BRUTA

Utilizando a ferramenta GoBuster em modo diretório, é possível encontrar diversos diretórios com potencial para exploração. Iniciaremos por login.php.

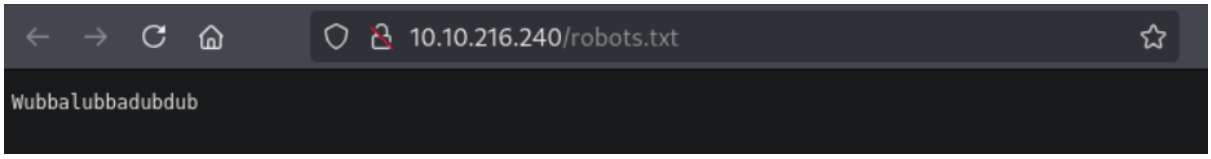
```
└─$ gobuster dir -u http://10.10.216.240 -w /usr/share/wordlists/dirbuster/directory-list-2.3
-medium.txt -t 12 -x .php,.html,.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.216.240
[+] Method:                  GET
[+] Threads:                 12
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php,html,txt
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.php                 (Status: 403) [Size: 278]
/.html                (Status: 403) [Size: 278]
/index.html           (Status: 200) [Size: 1062]
/login.php            (Status: 200) [Size: 882]
/robots.txt           (Status: 200) [Size: 17]
/assets               (Status: 301) [Size: 315] [--> http://10.10.216.240/assets/]
/portal.php           (Status: 302) [Size: 0] [--> /login.php]
```

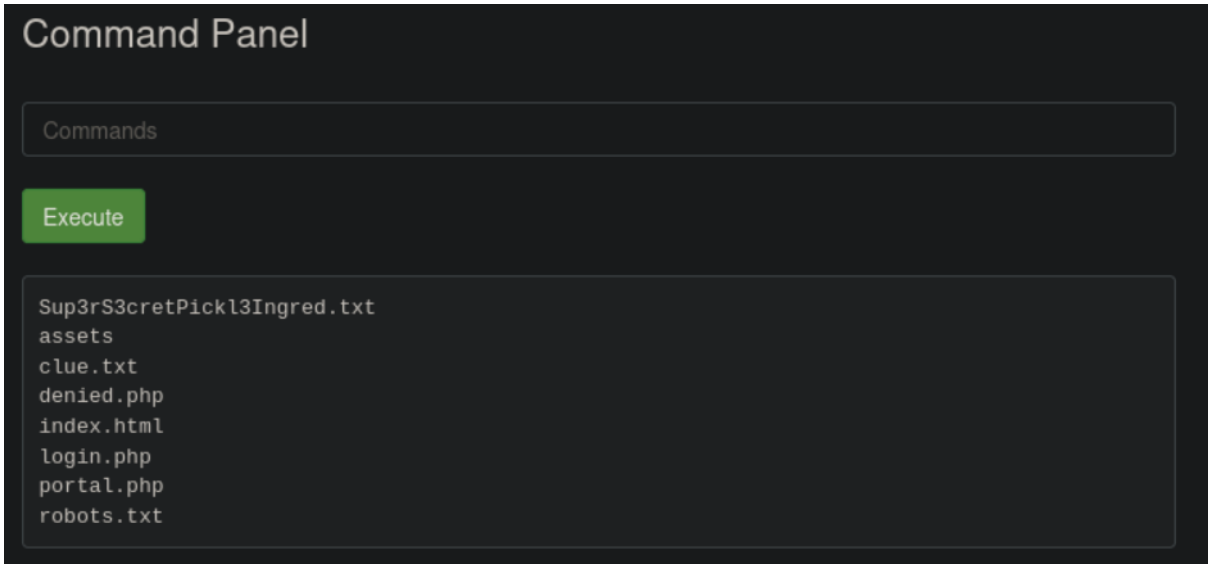


COLETA DE DADOS

Agora, com acesso a uma página de login, é necessário um nome de usuário e uma senha. Vasculhando o código fonte dos diretórios encontrados até o momento com Ctrl+U, encontra-se um possível nome de usuário no código da página inicial e, acessando /robots.txt, também uma possível senha. Retornando à página de login e utilizando os dados coletados, obtém-se uma linha de comando, seu funcionamento pode ser testado com o comando “ls”.

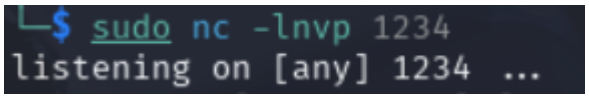
```
26   </div>
27
28   <!--
29
30     Note to self, remember username!
31
32     Username: R1ckRul3s
33
34   -->
35
36 </body>
37 </html>
38
```





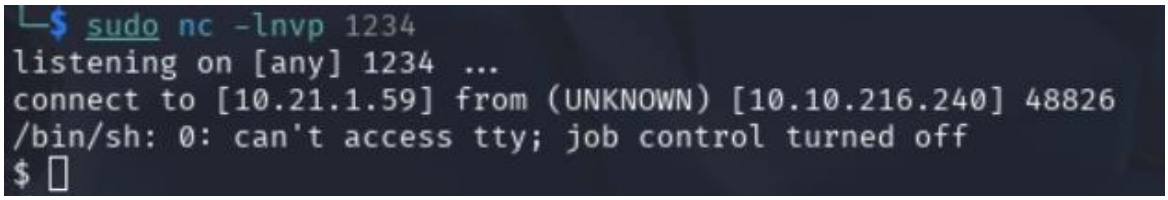
SHELL REVERSA

Agora com uma linha de comando disponível, para facilitar a navegação e obtenção das flags, cabe a utilização de uma ferramenta de shell reversa. Neste caso foi utilizado NetCat (comando “nc”) na máquina atacante.



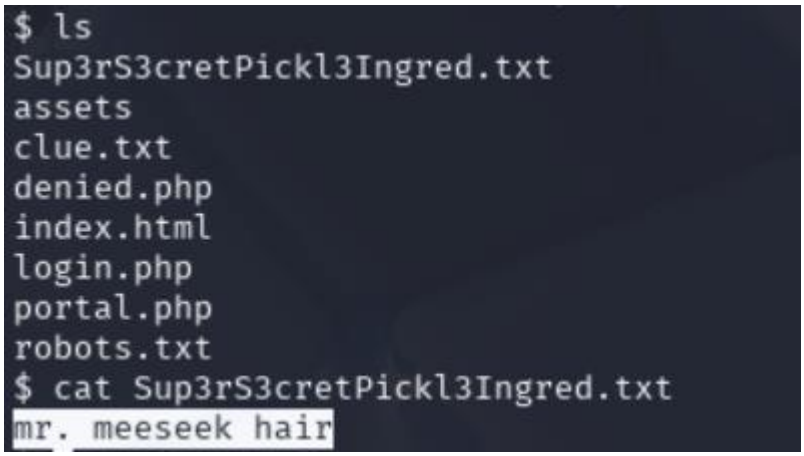
Como foram encontrados diversos arquivos com extensão .php até o momento, foi utilizado o comando de php para shell reversa encontrado no site pentestmonkey.

Retornando ao terminal da máquina atacante, pode-se verificar o sucesso na obtenção da shell.

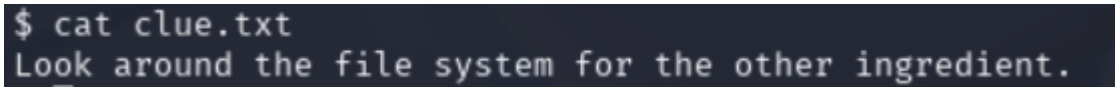


FLAGS E ESCALONAMENTO DE PRIVILÉGIOS

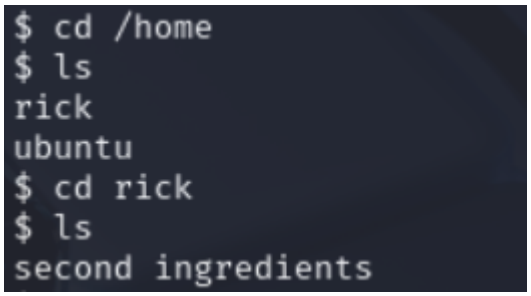
Utilizando os comandos abaixo no diretório inicial ao obter a shell, encontra-se a primeira flag necessária.



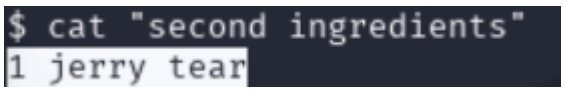
No mesmo diretório podemos ainda obter uma pista para a próxima flag.



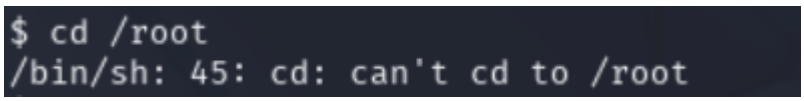
Seguindo a pista e navegando até o diretório home/rick, encontra-se a segunda flag necessária.



Como o arquivo contendo a próxima flag possui um espaço vazio entre as palavras de seu nome, é necessário que o nome seja posto entre aspas ao utilizar o comando cat para obter a flag.



Vasculhando pelos diretórios restantes, nenhuma outra flag é encontrada, cabendo supor que a última está no diretório root, cujo usuário atual não tem a permissão necessária para acessar.



No entanto, executando os comandos abaixo, nota-se uma má configuração das permissões do usuário www-data, na qual este pode escalonar seus privilégios para

sem a necessidade de uma senha, permitindo o acesso ao diretório root e a obtenção da última flag.