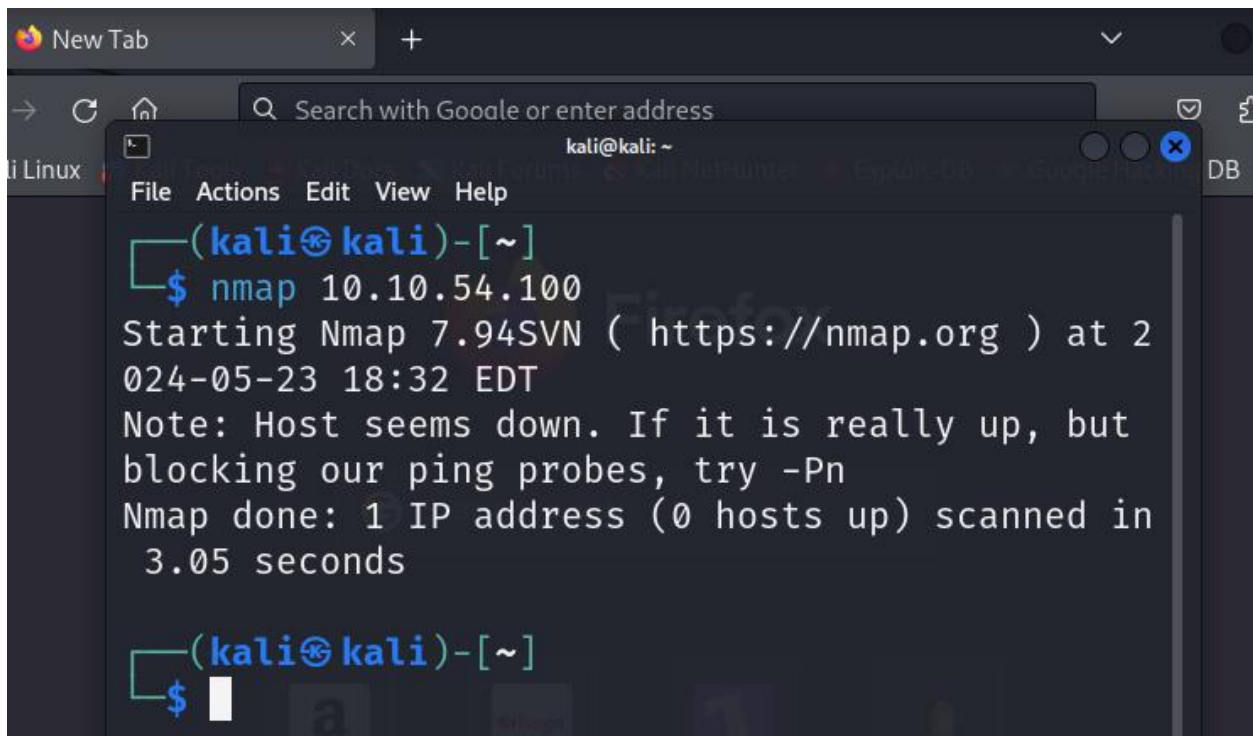


RELATÓRIO DE RISCO

#NMAP SIMPLES NO IP ALVO

Primeiramente executamos o comando NMAP 10.10.54.100.



```
(kali㉿kali)-[~]  
$ nmap 10.10.54.100  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 18:32 EDT  
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn  
Nmap done: 1 IP address (0 hosts up) scanned in 3.05 seconds  
  
(kali㉿kali)-[~]  
$
```

O servidor bloqueou nosso PING, então utilizamos o parametro -Pn.

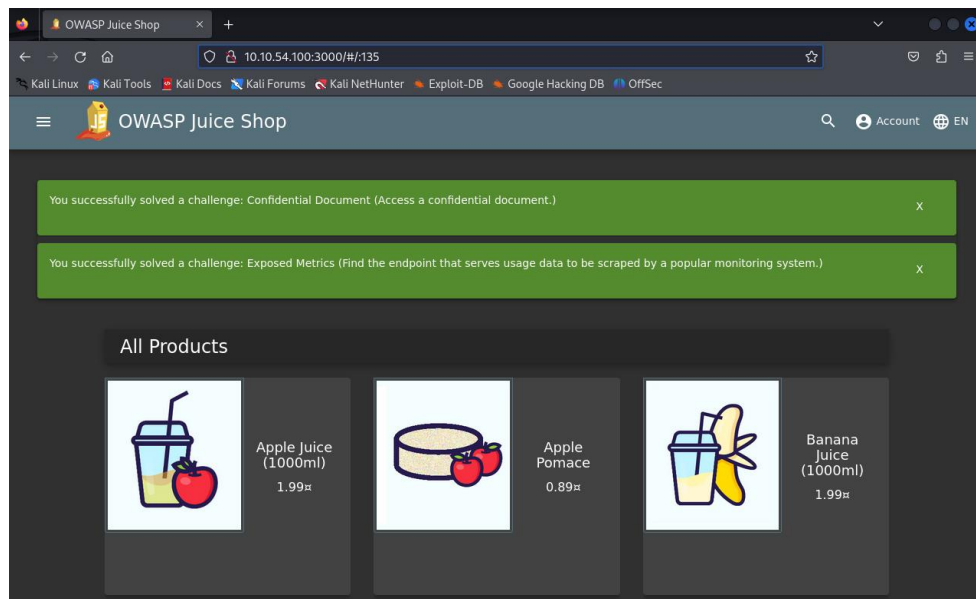
```
linux File Actions Edit View Help
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 18:35 EDT
Nmap scan report for L1504MICR0100.fiap.com.br (10.10.54.100)
Host is up (0.0064s latency).
Not shown: 997 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds

Nmap done: 1 IP address (1 host up) scanned in 4.83 seconds
```

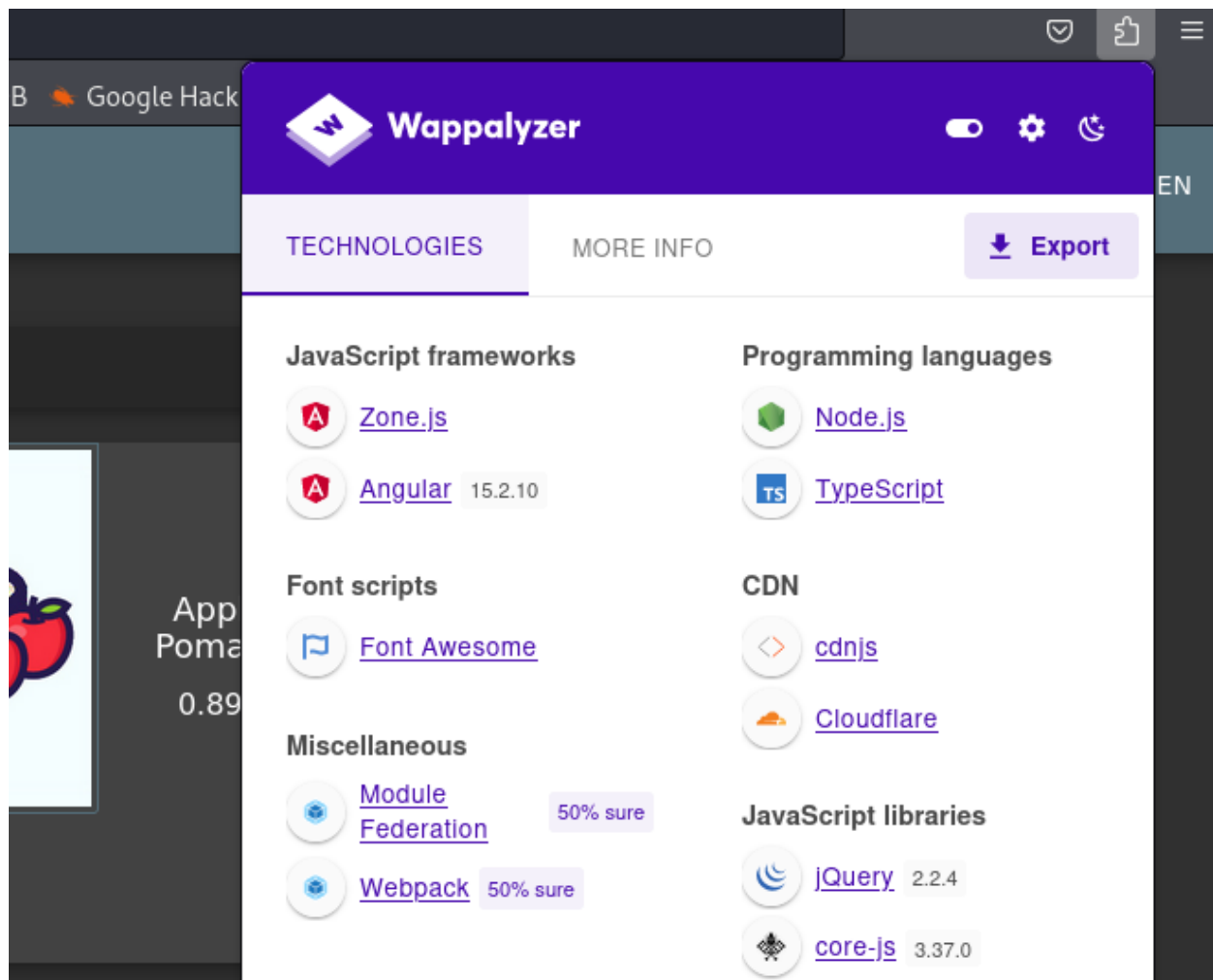
Encontramos as seguintes portas:

- 135/tcp: PORTA RESTRITA
- 139/tcp: PORTA RESTRITA
- 445/tcp: PORTA RESTRITA

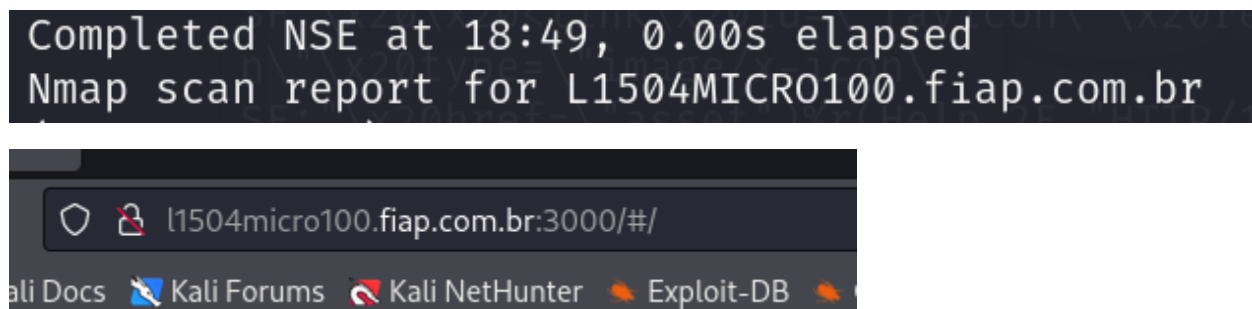
Adicionamos a porta 3000 junto ao IP e conseguimos acessar o site da porta 135/tcp.



Com a extensão WAPPALIZER descobrimos as frameworks utilizadas, as linguagens de programação, as fontes e as bibliotecas.



Encontramos o DNS do servidor.



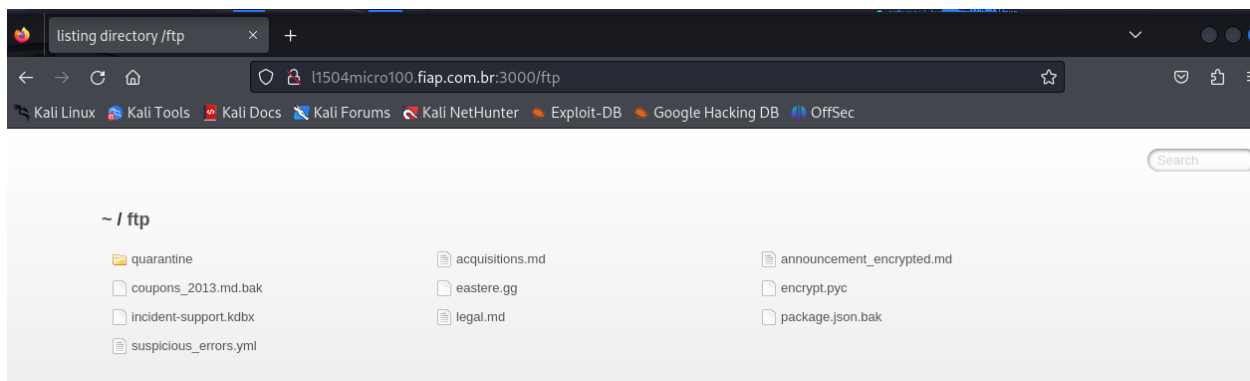
Com o DIRB conseguimos acessar a WORDLIST </usr/share/dirb/wordlists/common.txt>.

E as seguintes PATHS:

```
GENERATED WORDS: 4012  
1000ml Pomace  
—— Scanning URL: http://l1504micro100.fiap.com.br:3000/ ——  
+ http://l1504micro100.fiap.com.br:3000/assets (CODE:301|SIZE:179)  
+ http://l1504micro100.fiap.com.br:3000/ftp (CODE:200|SIZE:11072)  
+ http://l1504micro100.fiap.com.br:3000/profile (CODE:500|SIZE:1154)  
+ http://l1504micro100.fiap.com.br:3000/promotion (CODE:200|SIZE:6586)  
+ http://l1504micro100.fiap.com.br:3000/redirect (CODE:500|SIZE:3119)  
+ http://l1504micro100.fiap.com.br:3000/robots.txt (CODE:200|SIZE:28)  
+ http://l1504micro100.fiap.com.br:3000/snippets (CODE:200|SIZE:792)  
+ http://l1504micro100.fiap.com.br:3000/video (CODE:200|SIZE:10075518)  
+ http://l1504micro100.fiap.com.br:3000/Video (CODE:200|SIZE:10075518)  
Best Juice
```

Dentre as paths do print acima encontramos vulnerabilidade nas seguintes:

/ftp - Diretórios com informações confidenciais expostas.



/profile - ERRO 500 – Bloqueado por atividade ilegal.

/snippets - Encontramos diretórios vulneráveis.

