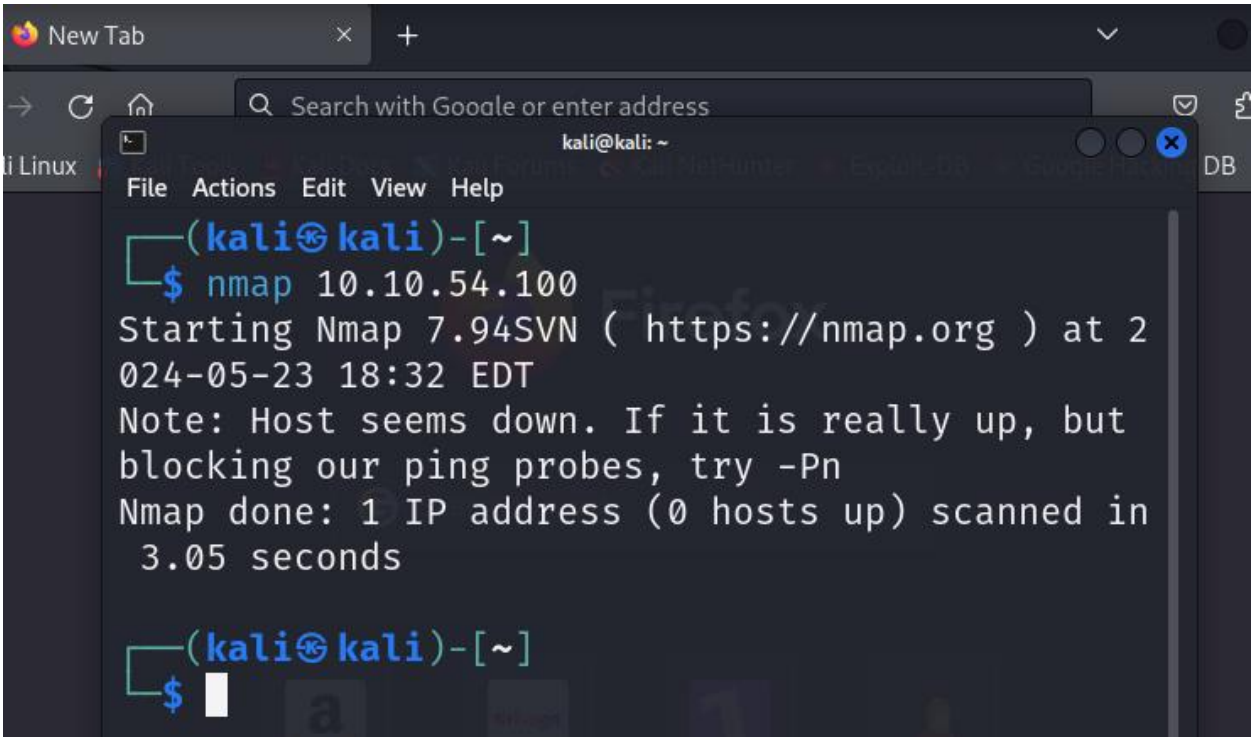
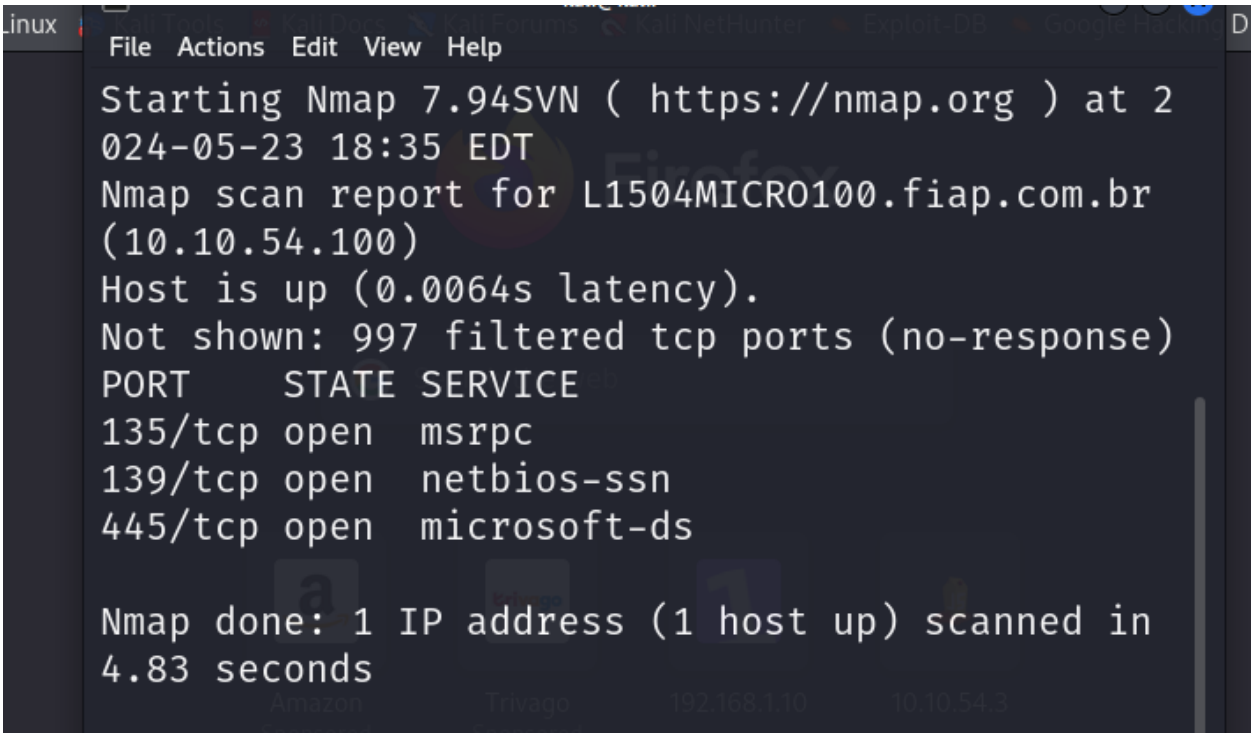
RELATÓRIO DE RISCO

#NMAP SIMPLES NO IP ALVO

Primeiramente executamos o comando NMAP 10.10.54.100.



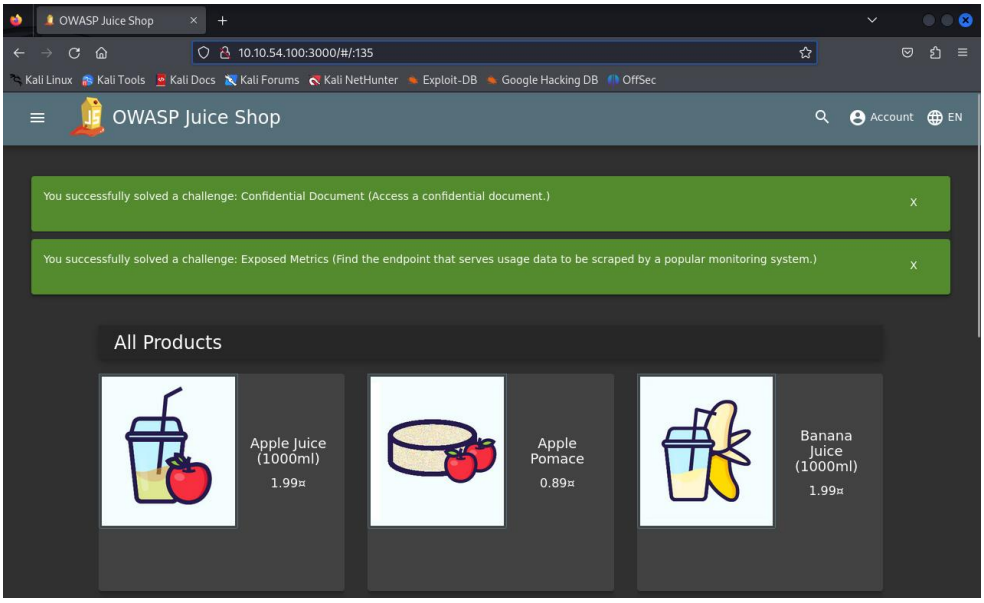
O servidor bloqueou nosso PING, então utilizamos o parametro –Pn.



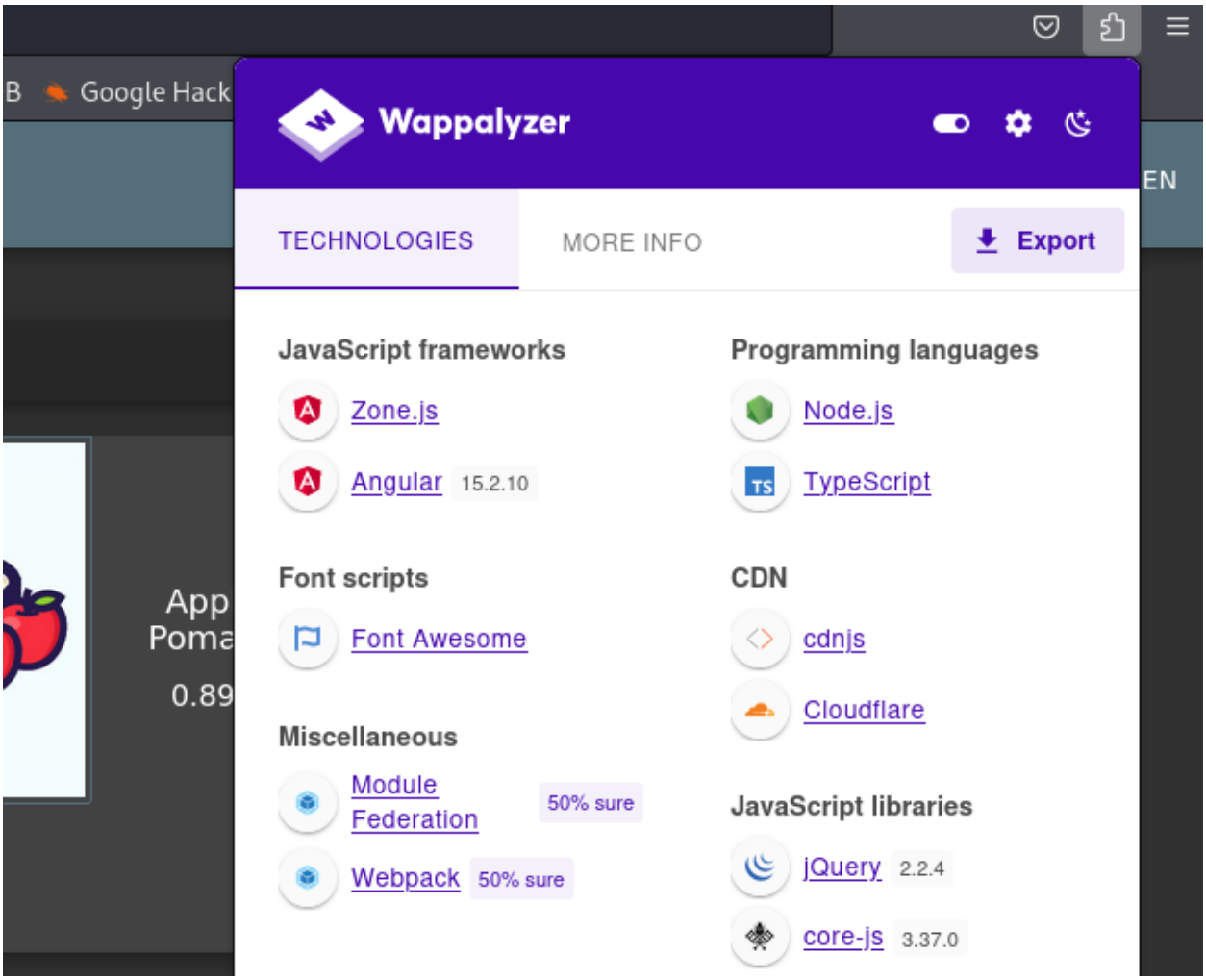
Encontramos as seguintes portas:

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

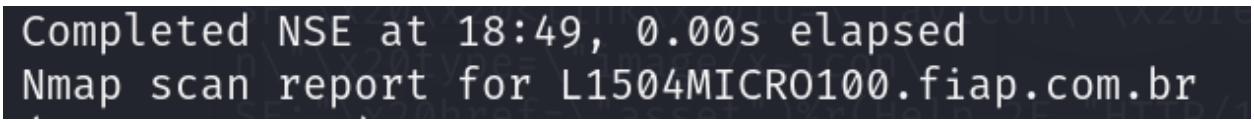
Adicionamos a porta 3000 junto ao IP e conseguimos acessar o site da porta 135/tcp.

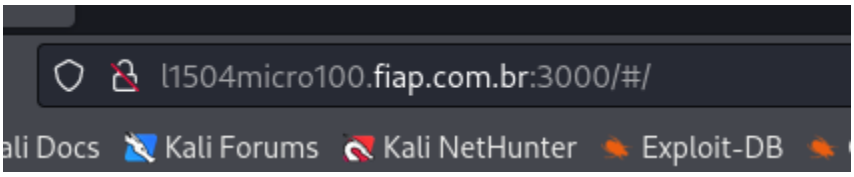


Com a extensão WAPPALIZER descobrimos as frameworks utilizadas, as linguagens de programação, as fontes e as bibliotecas.



Encontramos o DNS do servidor.





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

E as seguintes PATHS:

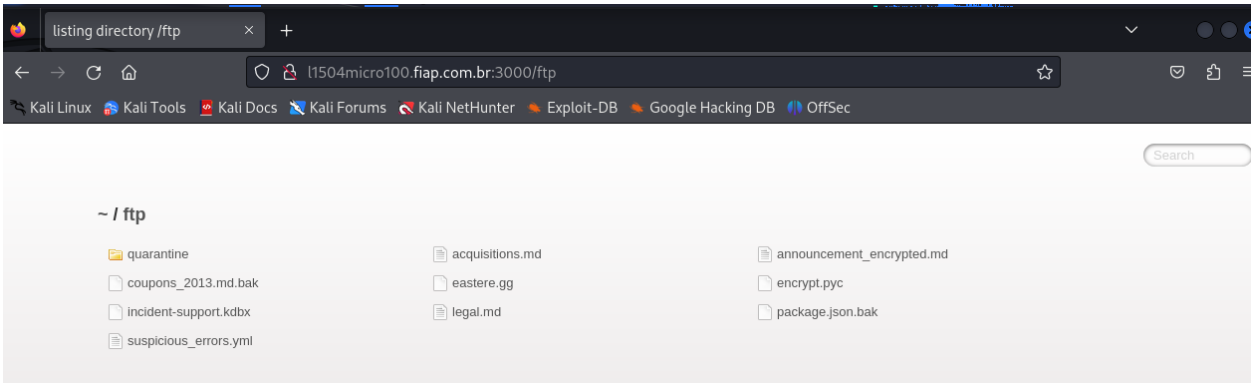
```
GENERATED WORDS: 4612

---- 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)

_____________________
```

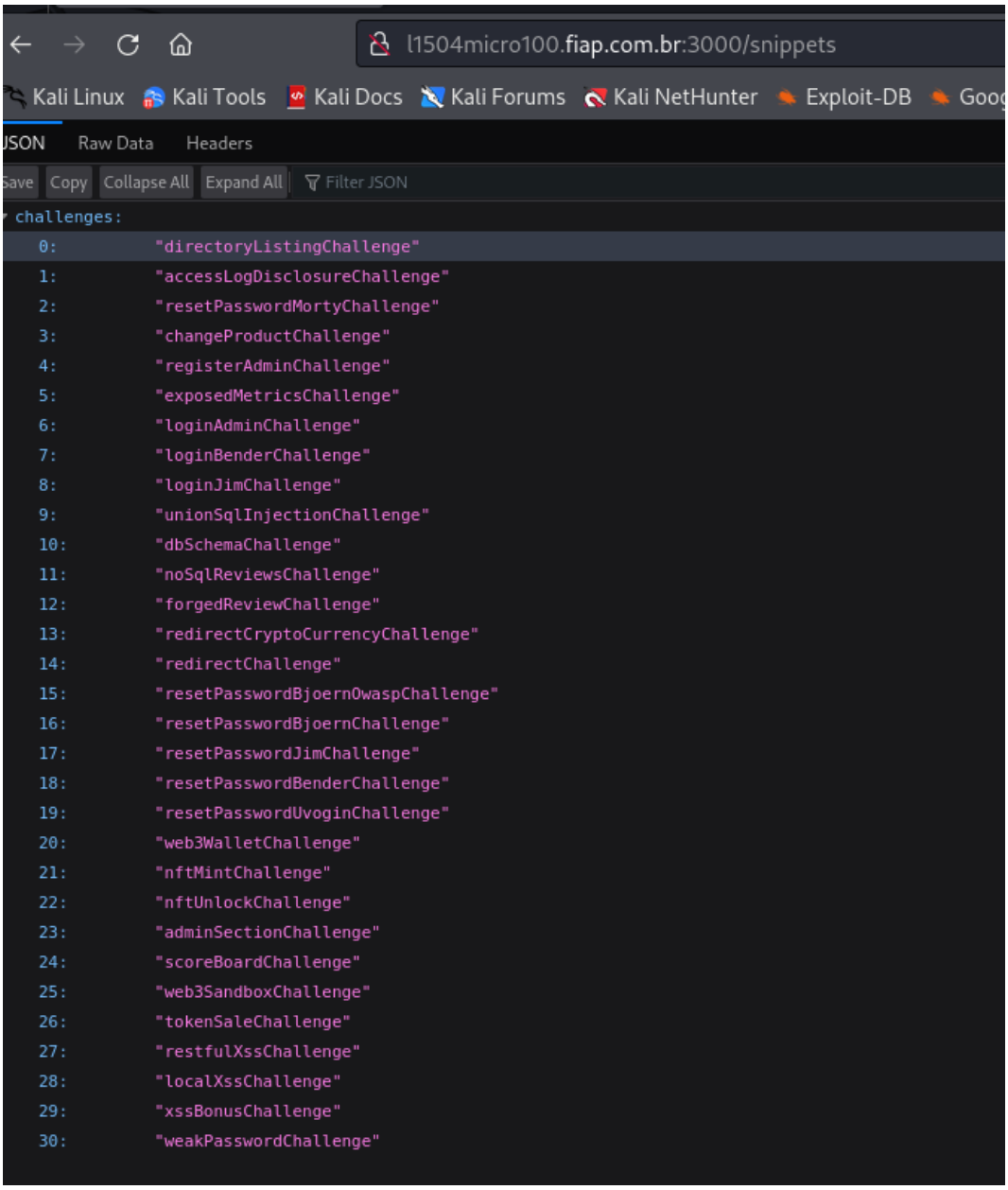
Dentre as paths do print acima encontramos vulnerabilidade nas seguintes:

/ftp - Diretórios com informações confidenciais expostas.



/profile - ERRO 500 – Bloqueado por atividade ilegal.

/snippets - Encontramos diretórios vulneraveis.


l1504micro100.fiap.com.br:3000/snippets
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
JSON
Raw Data
Headers
Save
Copy
Collapse All
Expand All
Filter JSON
challenges:
0: "directoryListingChallenge"
1: "accessLogDisclosureChallenge"
2: "resetPasswordMortyChallenge"
3: "changeProductChallenge"
4: "registerAdminChallenge"
5: "exposedMetricsChallenge"
6: "loginAdminChallenge"
7: "loginBenderChallenge"
8: "loginJimChallenge"
9: "unionSqlInjectionChallenge"
10: "dbSchemaChallenge"
11: "noSqlReviewsChallenge"
12: "forgedReviewChallenge"
13: "redirectCryptoCurrencyChallenge"
14: "redirectChallenge"
15: "resetPasswordBjoernOwaspChallenge"
16: "resetPasswordBjoernChallenge"
17: "resetPasswordJimChallenge"
18: "resetPasswordBenderChallenge"
19: "resetPasswordUvoginChallenge"
20: "web3WalletChallenge"
21: "nftMintChallenge"
22: "nftUnlockChallenge"
23: "adminSectionChallenge"
24: "scoreBoardChallenge"
25: "web3SandboxChallenge"
26: "tokenSaleChallenge"
27: "restfulXssChallenge"
28: "localXssChallenge"
29: "xssBonusChallenge"
30: "weakPasswordChallenge"