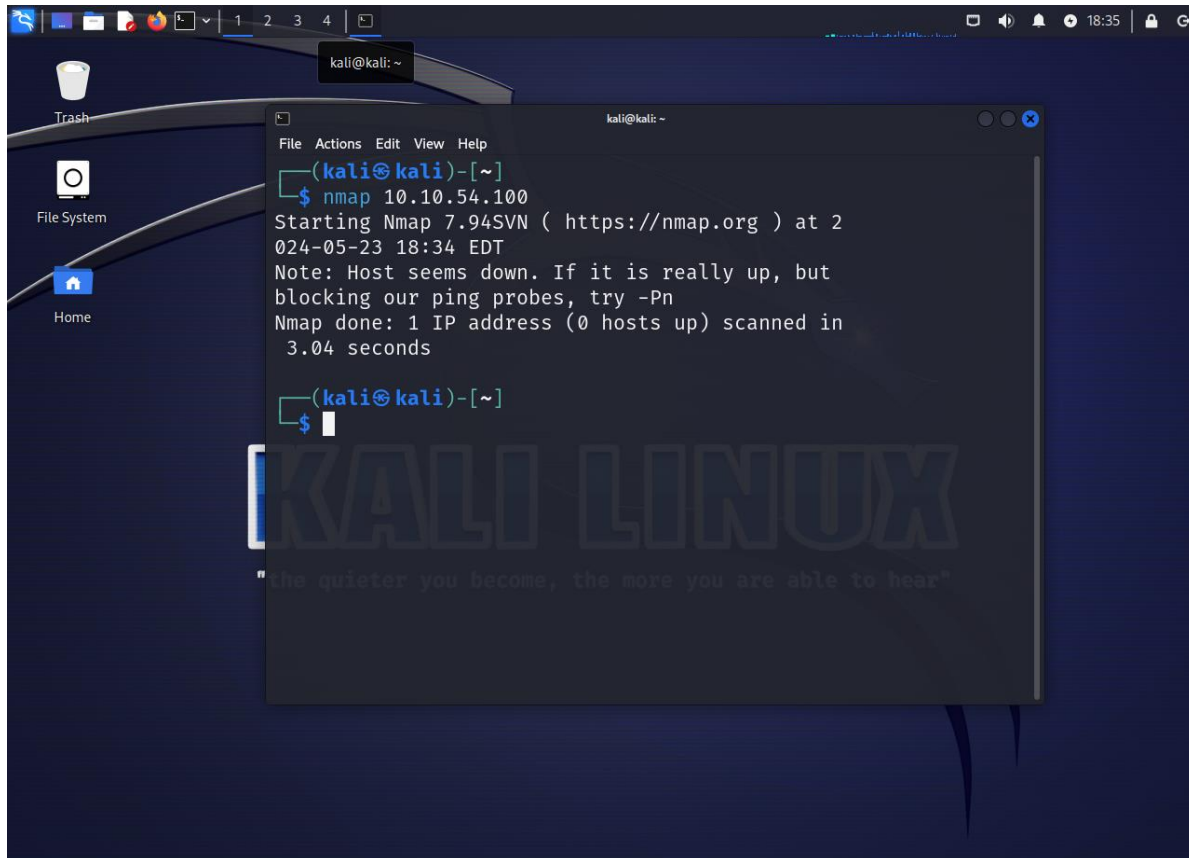


RELATÓRIO CP3 HACKERMINDSET

Gustavo Henrique Moura
Gabriela Beatriz

RM55643
RM558628

#Rodamos o comando **nmap**

A screenshot of a Kali Linux desktop environment. In the center, a terminal window is open, displaying the output of the 'nmap' command. The terminal shows the command 'nmap 10.10.54.100' being entered and executed. The output indicates that Nmap 7.94SVN is starting at 18:34 EDT, notes that the host seems down, and reports that 1 IP address was scanned in 3.04 seconds. The desktop background is dark blue with the Kali Linux logo and the text 'KALI LINUX' and 'the quieter you become, the more you are able to hear' visible. The top of the screen shows a taskbar with various application icons and a system clock indicating 18:35.

Como não achamos as portas por meio do comando NMAP, rodamos o comando com sudo abaixo

#rodamos o comando **sudo nmap** para achar as versões do SO e portas abertas

```
(kali㉿kali)-[~]
└─$ sudo nmap 10.10.54.100 -v -sS -sV --open
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 18:36 EDT
NSE: Loaded 46 scripts for scanning.
Initiating Ping Scan at 18:36
Scanning 10.10.54.100 [4 ports]
Completed Ping Scan at 18:36, 0.02s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 18:36
Completed Parallel DNS resolution of 1 host. at 18:36, 0.02s elapsed
Initiating SYN Stealth Scan at 18:36
Scanning L1504MICRO100.fiap.com.br (10.10.54.100) [1000 ports]
Discovered open port 135/tcp on 10.10.54.100
Discovered open port 139/tcp on 10.10.54.100
Discovered open port 445/tcp on 10.10.54.100
Completed SYN Stealth Scan at 18:36, 4.50s elapsed (1000 total ports)
Initiating Service scan at 18:36
Scanning 3 services on L1504MICRO100.fiap.com.br (10.10.54.100)
Completed Service scan at 18:36, 6.36s elapsed (3 services on 1 host)
NSE: Script scanning 10.10.54.100.
Initiating NSE at 18:36
Completed NSE at 18:36, 0.00s elapsed
Initiating NSE at 18:36
Completed NSE at 18:36, 0.03s elapsed
Nmap scan report for L1504MICRO100.fiap.com.br (10.10.54.100)
Host is up (0.00094s latency).
Not shown: 997 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit

Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Read data files from: /usr/bin/../../share/nmap
```

Assim conseguimos localizar quais portas estão abertas e quais versões da SO usada.

rodamos o comando `nmap -v -sT "ip" -open -p-`

```
(kali㉿kali)-[~]  
$ nmap -v -sT 10.10.54.100 --open -p-  
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-05-23 18:49 EDT  
Initiating Ping Scan at 18:49  
Scanning 10.10.54.100 [2 ports]  
Completed Ping Scan at 18:49, 3.01s elapsed (1 total hosts)  
Read data files from: /usr/bin/../share/nmap  
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 3.04 seconds  
  
(kali㉿kali)-[~]  
$
```

Rodamos esse comando para achar as portas TCP, vimos que um ip address foi achado.

#rodamos o comando **DIRB** com o ip para achar os Paths do alvo

```

GENERATED WORDS: 4612

— Scanning URL: http://10.10.54.100:3000/ —
+ http://10.10.54.100:3000/assets (CODE:301|SIZE:179)
→ Testing: http://10.10.54.100:3000/fsck
+ http://10.10.54.100:3000/ftp (CODE:200|SIZE:11072)
→ Testing: http://10.10.54.100:3000/future
+ http://10.10.54.100:3000/profile (CODE:500|SIZE:1154)
+ http://10.10.54.100:3000/promotion (CODE:200|SIZE:6586)
+ http://10.10.54.100:3000/redirect (CODE:500|SIZE:3119)
+ http://10.10.54.100:3000/robots.txt (CODE:200|SIZE:28)
+ http://10.10.54.100:3000/snippets (CODE:200|SIZE:792)
→ Testing: http://10.10.54.100:3000/usage
→ Testing: http://10.10.54.100:3000/userlist
→ Testing: http://10.10.54.100:3000/userlogin
→ Testing: http://10.10.54.100:3000/usermanager
→ Testing: http://10.10.54.100:3000/usernames
→ Testing: http://10.10.54.100:3000/usuario
+ http://10.10.54.100:3000/video (CODE:200|SIZE:10075518)
+ http://10.10.54.100:3000/Video (CODE:200|SIZE:10075518)
→ Testing: http://10.10.54.100:3000/W3SVC3
→ Testing: http://10.10.54.100:3000/wa

→ Testing: http://10.10.54.100:3000/wallpaper
→ Testing: http://10.10.54.100:3000/webcast

→ Testing: http://10.10.54.100:3000/webcasts
```

#rodamos esse comando **DIRB** para descobrir paths no alvo setando uma wordlist especifica

```
(kali@kali)-[~]
$ dirb http://10.10.54.100:3000 /usr/share/wordlists/wfuzz/general/common.txt

DIRB v2.22
By The Dark Raver

START_TIME: Thu May 23 19:02:00 2024
URL_BASE: http://10.10.54.100:3000/
WORDLIST_FILES: /usr/share/wordlists/wfuzz/general/common.txt

GENERATED WORDS: 951

— Scanning URL: http://10.10.54.100:3000/ —
+ http://10.10.54.100:3000/assets (CODE:301|SIZE:179)
+ http://10.10.54.100:3000/ftp (CODE:200|SIZE:11072)
+ http://10.10.54.100:3000/profile (CODE:500|SIZE:1154)
+ http://10.10.54.100:3000/redirect (CODE:500|SIZE:3119)

END_TIME: Thu May 23 19:02:24 2024
DOWNLOADED: 951 - FOUND: 4
```

Vimos que tem um padrão na pesquisa e tem o mesmo http

#rodamos o comando Dirb -N 404 para descobrir paths excluindo alguns status code

```
└─$ dirb http://10.10.54.100:3000 -N 404

DIRB v2.22
By The Dark Raver

START_TIME: Thu May 23 19:12:48 2024
URL_BASE: http://10.10.54.100:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Ignoring NOT_FOUND code → 404

GENERATED WORDS: 4612

--- Scanning URL: http://10.10.54.100:3000/ ---
+ http://10.10.54.100:3000/assets (CODE:301|SIZE:179)
+ http://10.10.54.100:3000/ftp (CODE:200|SIZE:11072)
+ http://10.10.54.100:3000/profile (CODE:500|SIZE:1154)
+ http://10.10.54.100:3000/promotion (CODE:200|SIZE:6586)
+ http://10.10.54.100:3000/redirect (CODE:500|SIZE:3119)
+ http://10.10.54.100:3000/robots.txt (CODE:200|SIZE:28)
+ http://10.10.54.100:3000/snippets (CODE:200|SIZE:792)
+ http://10.10.54.100:3000/video (CODE:200|SIZE:10075518)
+ http://10.10.54.100:3000/Video (CODE:200|SIZE:10075518)

END_TIME: Thu May 23 19:15:04 2024
DOWNLOADED: 4612 - FOUND: 9
```

#conseguimos acessar o OWASP Juice Shop por meio do endereço IP e o mesmo estava ativo.

kali-linux-2023.4-virtualbox-amd64 (Snapshot_130324) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help


Google Chrome Problem Location Add-ons Manager Blue reverse HackTools Installation bash%20 Wappalizer OWASP x

10.10.54.14:3000/#/


Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hack

OWASP Juice Shop


All Products




Apple Juice (1000ml)
1.99€




Apple Pommes
0.89€



Only 1 left
Best Juice Shop Salesman Artwork
5000€



Carrot Juice (1000ml)
2.99€



Eggfruit

This website uses fruit cookies to ensure you get the juiciest tracking experience. But me wait!

Me want it!

Wappalizer

TECHNOLOGIES MORE INFO Export

JavaScript frameworks

- Zone.js
- Angular 15.2.10

Programming languages

- Node.js
- TypeScript

Font scripts

- Font Awesome

CDN

- cdnjs
- Cloudflare

Miscellaneous

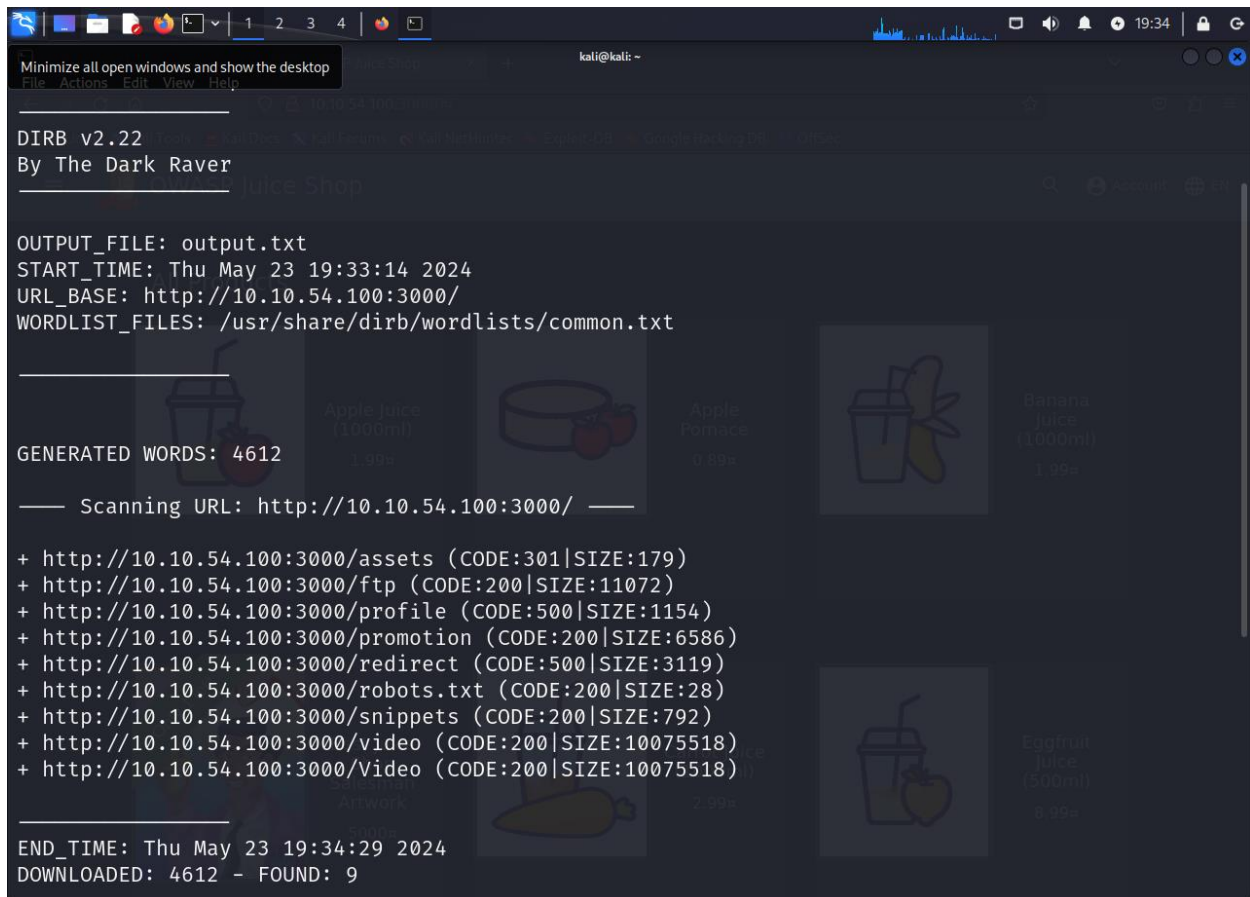
- Module Federation 50% sure
- Webpack 50% sure

JavaScript libraries

- jQuery 2.2.4
- core-js 3.37.0

Something wrong or missing?

#rodamos o comando **dirb -o output.txt**



```
Minimize all open windows and show the desktop
File Actions Edit View Help

DIRB v2.22
By The Dark Raver

OUTPUT_FILE: output.txt
START_TIME: Thu May 23 19:33:14 2024
URL_BASE: http://10.10.54.100:3000/
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt

GENERATED WORDS: 4612

— Scanning URL: http://10.10.54.100:3000/ —

+ http://10.10.54.100:3000/assets (CODE:301|SIZE:179)
+ http://10.10.54.100:3000/ftp (CODE:200|SIZE:11072)
+ http://10.10.54.100:3000/profile (CODE:500|SIZE:1154)
+ http://10.10.54.100:3000/promotion (CODE:200|SIZE:6586)
+ http://10.10.54.100:3000/redirect (CODE:500|SIZE:3119)
+ http://10.10.54.100:3000/robots.txt (CODE:200|SIZE:28)
+ http://10.10.54.100:3000/snippets (CODE:200|SIZE:792)
+ http://10.10.54.100:3000/video (CODE:200|SIZE:10075518)
+ http://10.10.54.100:3000/Video (CODE:200|SIZE:10075518)

END_TIME: Thu May 23 19:34:29 2024
DOWNLOADED: 4612 - FOUND: 9
```

Para descobrir paths no alvo e exportar o resultado para um arquivo

#extensão onde conseguimos ver portas abertas

