Corridor

Resolviendo la máquina Corridor

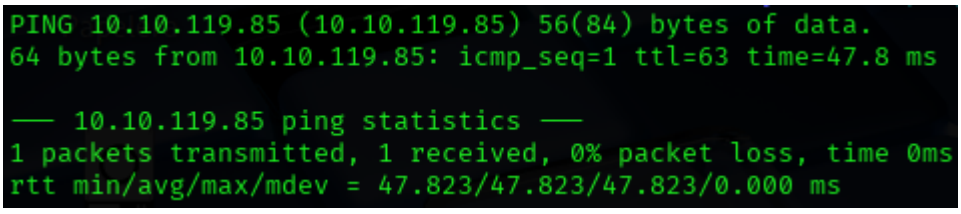
> En esta publicación, comparto cómo resolví la máquina Corridor de TryHackMe.

Enumeración

Ping

Ejecutamos un *ping* para comprobar la conectividad y obtener pistas sobre el sistema operativo.

```
ping -c 1 10.10.119.85
```



TTL=63 -> **Linux**

Nmap

Escaneo inicial de puertos.

```
nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn 10.10.119.85 -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 2025-07-12 19:08 CEST
Initiating SYN Stealth Scan at 19:08
Scanning 10.10.119.85 [65535 ports]
Discovered open port 80/tcp on 10.10.119.85
Completed SYN Stealth Scan at 19:08, 12.60s elapsed (65535 total ports)
Nmap scan report for 10.10.119.85
Host is up, received user-set (0.049s latency).
Scanned at 2025-07-12 19:08:40 CEST for 12s
Not shown: 65534 closed tcp ports (reset)
PORT   STATE SERVICE REASON
80/tcp open  http    syn-ack ttl 62

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 12.68 seconds
           Raw packets sent: 66639 (2.932MB) | Rcvd: 65782 (2.631MB)
```

`nmap -p80 -sCV 10.10.119.85 -oN targeted`

```
Starting Nmap 7.95 ( https://nmap.org ) at 2025-07-12 19:11 CEST
Nmap scan report for 10.10.119.85
Host is up (0.048s latency).

PORT   STATE SERVICE VERSION
80/tcp open  http    Werkzeug httpd 2.0.3 (Python 3.10.2)
|_http-title: Corridor

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 7.75 seconds
```

Explotación

HTTP

Al analizar el sitio web, observamos que los títulos parecen estar codificados en **MD5**.

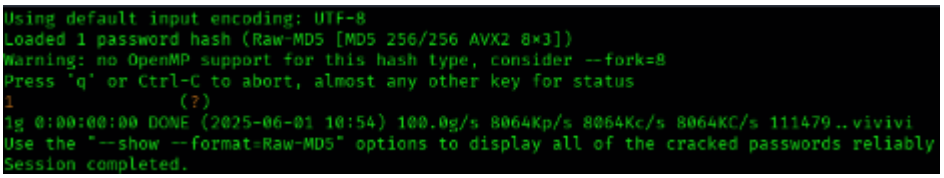
```
<!DOCTYPE html>
<html lang="en">
<head>
    <meta charset="utf-8">
    <meta name="viewport" content="width=device-width, initial-scale=1, shrink-to-fit=no">
    <link rel="stylesheet" href="https://stackpath.bootstrapcdn.com/bootstrap/4.5.0/css/bootstrap.min.css"
        integrity="sha384-9aIt2nRpC12Uk9gS9baDl411NQApFmC26EwAOH8WgZl5MYYxFfc+NcPb1dKGj7Sk" crossorigin="anonymous">
    <title>Corridor</title>

    <link rel="stylesheet" href="/static/css/main.css">
</head>

<body>


<img src="/static/img/corridor.png" usemap="#image-map">

    <map name="image-map">
        <area target="" alt="c4ca4238a0b923820dcc509a6f75849b" title="c4ca4238a0b923820dcc509a6f75849b" href="c4ca4238a0b923820dcc509a6f75849b" coords="257,893,258,332,325,351,325,860" shape="poly">
        <area target="" alt="c81e728d9d4c2f636f067f89cc14862c" title="c81e728d9d4c2f636f067f89cc14862c" href="c81e728d9d4c2f636f067f89cc14862c" coords="469,766,503,747,501,405,474,394" shape="poly">
        <area target="" alt="eccbc87e4b5ce2fe28308fd9f2a7baf3" title="eccbc87e4b5ce2fe28308fd9f2a7baf3" href="eccbc87e4b5ce2fe28308fd9f2a7baf3" coords="585,698,598,691,593,429,584,421" shape="poly">
        <area target="" alt="a87ff679a2f3e71d9181a67b7542122c" title="a87ff679a2f3e71d9181a67b7542122c" href="a87ff679a2f3e71d9181a67b7542122c" coords="650,658,644,437,658,652,655,437" shape="poly">
        <area target="" alt="e4da3b7fbbce2345d7772b0674a318d5" title="e4da3b7fbbce2345d7772b0674a318d5" href="e4da3b7fbbce2345d7772b0674a318d5" coords="692,637,690,455,695,628,695,467" shape="poly">
        <area target="" alt="1679091c5a880faf6fb5e6087eb1b2dc" title="1679091c5a880faf6fb5e6087eb1b2dc" href="1679091c5a880faf6fb5e6087eb1b2dc" coords="719,620,719,458,728,471,728,609" shape="poly">
        <area target="" alt="8f14e45fceea167a5a36dedd4bea2543" title="8f14e45fceea167a5a36dedd4bea2543" href="8f14e45fceea167a5a36dedd4bea2543" coords="857,612,933,610,936,456,852,455" shape="poly">
        <area target="" alt="c9f0f895fb98ab9159f51fd0297e236d" title="c9f0f895fb98ab9159f51fd0297e236d" href="c9f0f895fb98ab9159f51fd0297e236d" coords="1475,857,1473,354,1537,335,1541,901" shape="poly">
        <area target="" alt="45c48cce2e2d7fbdea1afc51c7c6ad26" title="45c48cce2e2d7fbdea1afc51c7c6ad26" href="45c48cce2e2d7fbdea1afc51c7c6ad26" coords="1324,766,1300,752,1303,401,1325,397" shape="poly">
        <area target="" alt="d3d9446802a44259755d38e6d163e820" title="d3d9446802a44259755d38e6d163e820" href="d3d9446802a44259755d38e6d163e820" coords="1202,695,1217,704,1222,423,1203,423" shape="poly">
        <area target="" alt="6512bd43d9caa6e02c990b0a82652dca" title="6512bd43d9caa6e02c990b0a82652dca" href="6512bd43d9caa6e02c990b0a82652dca" coords="1154,668,1146,661,1144,442,1157,442" shape="poly">
        <area target="" alt="c20ad4d76fe97759aa27a0c99bff6710" title="c20ad4d76fe97759aa27a0c99bff6710" href="c20ad4d76fe97759aa27a0c99bff6710" coords="1105,628,1116,633,1113,447,1102,447" shape="poly">
        <area target="" alt="c51ce410c124a10e0db5e4b97fc2af39" title="c51ce410c124a10e0db5e4b97fc2af39" href="c51ce410c124a10e0db5e4b97fc2af39" coords="1073,609,1081,620,1082,459,1073,463" shape="poly">
    </map>


</body>
</html>
```

John The Ripper

Utilizamos **John the Ripper** para descifrar uno de los hashes.

```
echo "c4ca4238a0b923820dcc509a6f75849b" > hash
```

```
john --format=Raw-MD5 --wordlist=/usr/share/wordlists/rockyou.txt hash
```



El hash corresponde al número **1**.

Descifrando todos los títulos, obtenemos una secuencia del **1 al 13**.

Para probar con el **número 0**, generamos su hash MD5 manualmente.

```
echo -n "0" | md5sum
```


```
http://10.10.119.85/cfcd208495d565ef66e7dff9f98764da
```

Se encuentra la flag.
