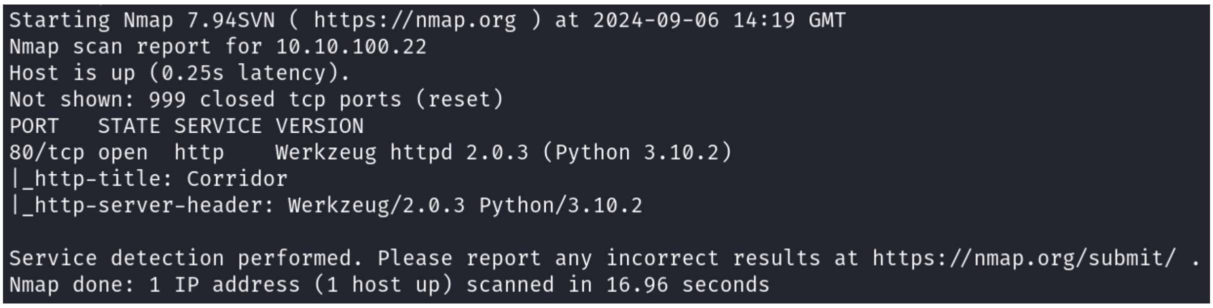
TryHackMe - Corridor (easy)

Summay

Enumeration

Nmap scan

`sudo nmap -sV -sC -T4 -oN nmap.txt <ip-adress>`



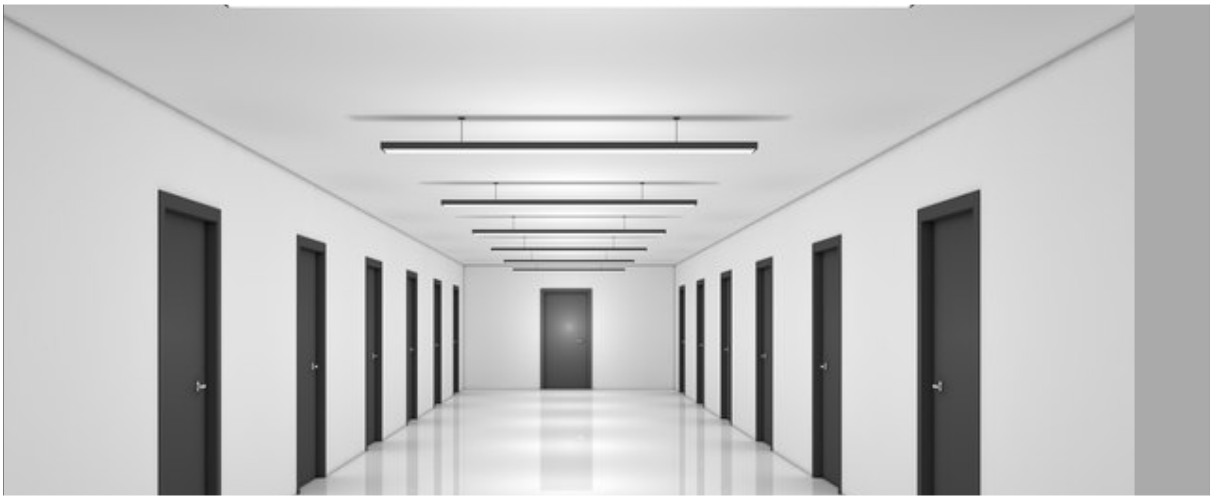
```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-06 14:19 GMT
Nmap scan report for 10.10.100.22
Host is up (0.25s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
80/tcp open  http    Werkzeug httpd 2.0.3 (Python 3.10.2)
|_http-title: Corridor
|_http-server-header: Werkzeug/2.0.3 Python/3.10.2

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 16.96 seconds
```

We only one open port. The `80` for `HTTP`

Web enumeration

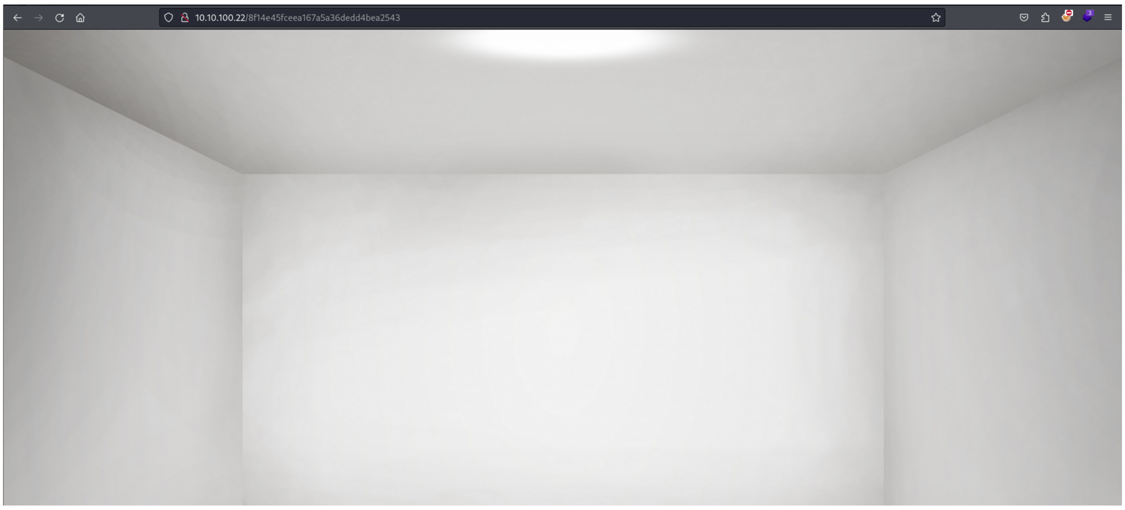
We go to see what we have there



Exploitation

IDOR Vulnerability

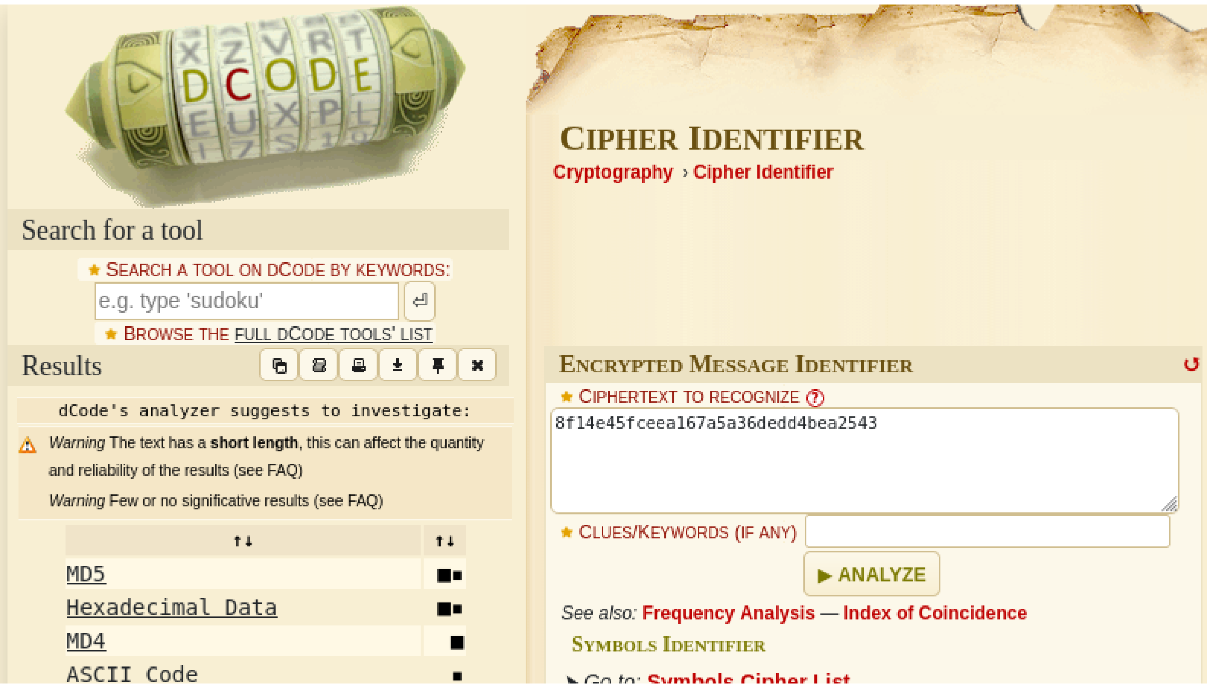
when we click on one of the doors we're redirected to an empty room



10.10.100.22/8f14e45fceea167a5a36dedd4bea2543

If we look at the URL we can see that there are some characters

We go to `https://www.dcode.fr/cipher-identifier` to see what it is



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'sudoku'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

dCode's analyzer suggests to investigate:

Warning The text has a **short length**, this can affect the quantity and reliability of the results (see FAQ)

Warning Few or no significative results (see FAQ)

↑↓	↑↓
MD5	■■
Hexadecimal Data	■■
MD4	■
ASCII Code	▪

CIPHER IDENTIFIER

Cryptography › Cipher Identifier

ENCRYPTED MESSAGE IDENTIFIER

★ CIPHERTEXT TO RECOGNIZE

```
8f14e45fceea167a5a36dedd4bea2543
```

★ CLUES/KEYWORDS (IF ANY)

▶ ANALYZE

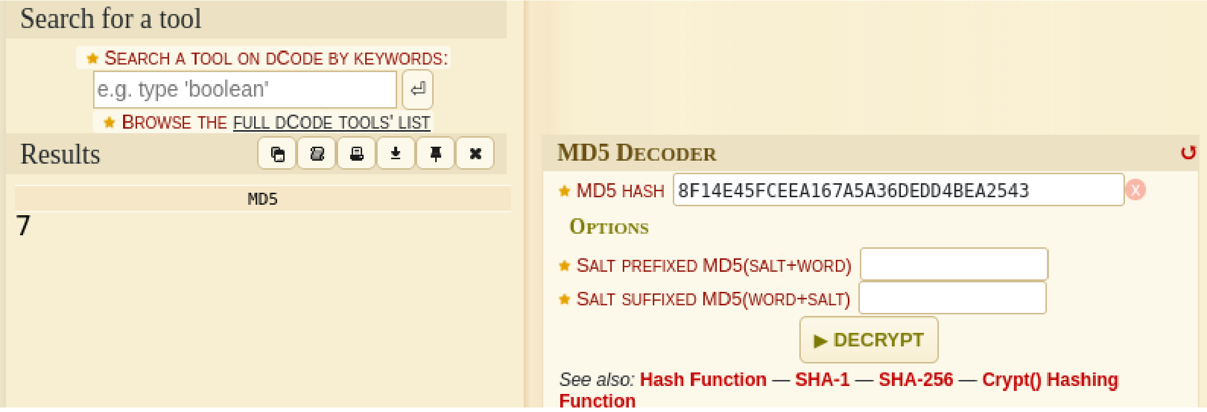
See also: Frequency Analysis — Index of Coincidence

SYMBOLS IDENTIFIER

▶ Go to: Symbols Cipher List

It's a `MD5` hash

We decipher it and the result is `7`



Search for a tool

★ SEARCH A TOOL ON DCODE BY KEYWORDS:

e.g. type 'boolean'

★ BROWSE THE FULL DCODE TOOLS' LIST

Results

MD5

7

MD5 DECODER

★ MD5 HASH 8F14E45FCEEA167A5A36DEDD4BEA2543

OPTIONS

★ SALT PREFIXED MD5(SALT+WORD)

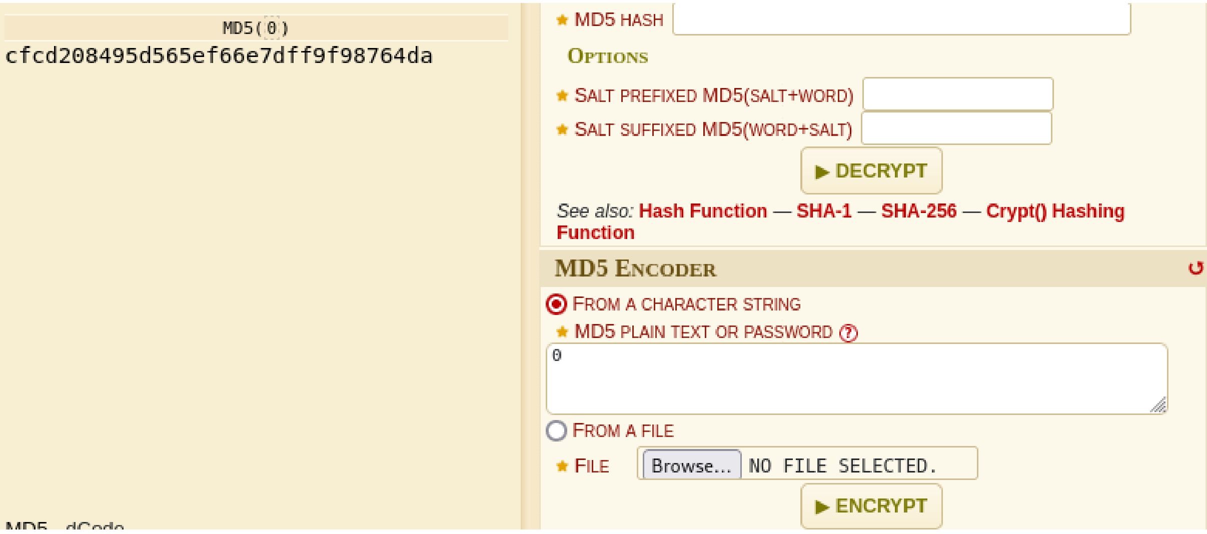
★ SALT SUFFIXED MD5(WORD+SALT)

▶ DECRYPT

See also: Hash Function — SHA-1 — SHA-256 — Crypt() Hashing Function

After multiple investigations, the doors are numerated from `1` to `13`. And we can only access with the URL by using the hash

We hash `0` in `MD5`



MD5(0)

cfcd208495d565ef66e7dff9f98764da

★ MD5 HASH

OPTIONS

★ SALT PREFIXED MD5(SALT+WORD)

★ SALT SUFFIXED MD5(WORD+SALT)

See also: Hash Function — SHA-1 — SHA-256 — Crypt() Hashing Function

MD5 ENCODER

● FROM A CHARACTER STRING

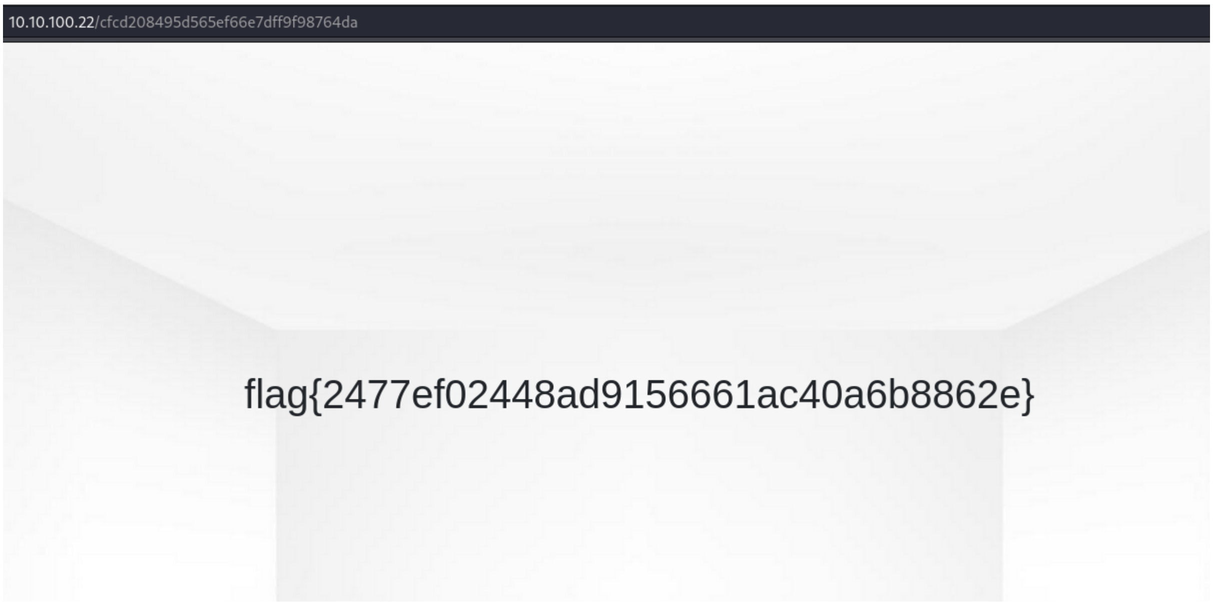
★ MD5 PLAIN TEXT OR PASSWORD ⓘ

0

○ FROM A FILE

★ FILE Browse... NO FILE SELECTED.

Then we go to the door 0 to see what happens



10.10.100.22/cfcd208495d565ef66e7dff9f98764da

flag{2477ef02448ad9156661ac40a6b8862e}

And Booomm!!! We have our flag