TryHackMe — Escape the Office

1. Reconnaissance

Start by identifying open ports on the target machine. Run a service version scan on the machine. The scan reveals two important ports:

- Port 80: an HTTP service hosting the room's story content.
- Port 22: an SSH service that allows remote login.

Since the goal involves escaping the office, the SSH service is the most important entry point.

ssh

2. Password Attack

You see a riddle that says to use gobuster to find hidden rooms. When you find it you will get a option door and then you find the door.
In there there will be another riddle and you manage to find the user name in the source code.

It says that he used a weak password. This suggests a brute force attack against SSH. The password can be found in rockyou.txt, which is the standard location in most Kali or Ubuntu based systems.

Use Hydra to perform a password attack on SSH with:

- one static username
- rockyou.txt as the password list

Hydra eventually identifies a valid password that grants SSH access to the abandoned account.

Finding: The account uses a weak password from rockyou.txt.

3. Exploring the User Account

Once logged in, examine the home directory. A small set of files is present. One of these files contains the only clue needed for the next step of the challenge. Listing the directory reveals a file. Opening the file shows a short message and a four digit number. This number is the code required to unlock the door on the web page.

4. Retrieving the Code

Display the content of the file. The four digit sequence is clearly visible and intended to be used directly.

Example content:

I was supposed to remember the code for the exit door, but I keep forgetting it.
If someone finds this, use it wisely and get out of this place.
The door code is: 4392

4392.

5. Escaping the Office

Return to the web interface on port 80. Enter the discovered code into the keypad page. The door unlocks, and the final page displays the flag that confirms a successful escape.

THM{ESCAPED_THE_OFFICE}