🛠️ TryHackMe Room: Team — Walkthrough

1. 🔍 Initial Scanning

- Used **Nmap** to scan the target.
- Found open ports:
  - **21 (FTP)**
  - **22 (SSH)**
  - **80 (HTTP)**

---

2. 🌐 Website Enumeration

- Visited the site on port 80.
- Found a hint in the page source to add `team.thm` to `/etc/hosts`.
- After adding it, the real website loaded.

---

3. 📁 Directory Discovery

- Ran directory brute-forcing using Gobuster.
- Found interesting paths like:
  - `/robots.txt` → revealed a username: **dale**
  - `/scripts/` → contained a file called `script.txt`

---

4. 🔑 Finding Credentials

- In `/scripts/script.txt`, found a reference to an older file.
- Accessed `script.old`, which contained **FTP credentials**.

---

5. 📦 FTP Login

- Logged into FTP using the credentials.
- Found a file named `New_site.txt`.

- This hinted at a new subdomain: **dev.team.thm**

---

6. 🖥️ Subdomain Access & LFI

- Added `dev.team.thm` to `/etc/hosts`.
- Visited the new subdomain and found a page vulnerable to **Local File Inclusion (LFI)**.
- Used LFI to read system files like `/etc/passwd` and `/etc/ssh/sshd_config`.
- Found an **SSH private key** for user **dale**.

---

7. 🧑‍💻 SSH Access as dale

- Logged into the machine using SSH and the recovered private key.
- Successfully accessed dale's account.
- Retrieved the **user flag**.

---

8. 🔼 Privilege Escalation to gyles

- Found a script named `admin_checks` owned by user **gyles**.
- Discovered it could be run with `sudo` as gyles.
- Passed `/bin/bash` as a command → gained shell as **gyles**.

---

9. 🔝 Root Privilege Escalation

- Searched for scheduled tasks (cron jobs).
- Found a backup script being run as root.
- Modified the script to include a reverse shell command.
- Set up a listener and waited for root to execute the script.
- Got a root shell and grabbed the **root flag**.