🃏 TryHackMe - HA Joker CTF Writeup

🧠 Overview

This is a medium-level Capture The Flag (CTF) challenge focused on web exploitation and privilege escalation. The goal is to gain root access by chaining multiple vulnerabilities.

🔍 1. Service Enumeration

Use `nmap` to scan open ports:

```
nmap -sV -sC -A <IP>
```

You'll see these open:

- **22** – SSH
- **80** – HTTP
- **8080** – HTTP with basic authentication

🌐 2. Port 80: HTTP Web Page

Visit the site and run a directory brute-force using:

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

You may discover:

- `secret.txt` – contains a chat between Joker and Batman, hinting a username
- `phpinfo.php` – exposes PHP config info

👤 3. Discovering Username

From the `secret.txt`, we learn the user is **joker**.

🔐 4. Port 8080: Brute-Forcing Credentials

Use Hydra to brute-force login:

```
hydra -l joker -P /usr/share/wordlists/rockyou.txt http-get://<IP>:8080
```

Password found: **hannah**

🛠️ 5. Admin Portal (Joomla)

After logging into port 8080 with `joker:hannah`, you find it's a Joomla CMS site.

Run Gobuster or Nikto again to find:

- `/administrator/` – Joomla admin login
- `backup.zip` – a downloadable backup file

🔓 6. Cracking backup.zip

Download the zip file and crack its password:

```
zip2john backup.zip > hash.txt
john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
```

After cracking, extract it. It contains:

- Joomla config
- Database file with credentials

🐚 7. Get Reverse Shell

Use Joomla admin access to upload a PHP reverse shell:

Steps:

1. Go to Templates in admin panel
2. Edit `index.php` of any template
3. Paste your reverse shell code
4. Set up listener:

```
nc -lvnp 4444
```

1. Visit the template page to trigger shell

⬆️ 8. Privilege Escalation (LXD Group)

Check group membership:

```
id
```

You'll see `lxd`. This means the user can run privileged containers.

Steps:

1. Create an Alpine Linux container tarball
2. Import it using `lxc image import`
3. Launch it and mount root filesystem
4. Gain access to `/root`

🏁 Final: Read the Flag

Now you're root!

Check `/root/root.txt` and `/home/<user>/user.txt` for the flags.