Forensic CTF Challenge Write-up

Category: Forensics • Challenge Type: Steganography + Dictionary Attack • Author: Karthik

Challenge Description

In this challenge, players are given an image file named **pirates-2-1678290544036.jpg**, which contains hidden data embedded using **Steghide**. The embedding was done using a weak or common passphrase, requiring a dictionary attack to recover the hidden file and extract the flag.

Tools Used

- **stegcracker**: Dictionary-based attack tool for Steghide
- **rockyou.txt**: Common password wordlist (or a provided list)
- **steghide**: For embedding and extracting files in/from image files

Steps to Solve

1. Start Dictionary Attack

Use `stegcracker` with a wordlist to crack the passphrase:

```
stegcracker pirates-2-1678290544036.jpg /usr/share/wordlists/rockyou.txt
```

2. Extract the Hidden File

Once the correct password is found, extract the hidden file:

```
steghide extract -sf pirates-2-1678290544036.jpg -p <password>
```

3. Recover the Flag

The extracted file will contain the flag in the format:

PIRATE{t0rr3nt_of_tr4cks}

Skills Tested

- Understanding of steganography techniques
- Performing dictionary attacks using stegcracker
- Efficient use of forensic tools in a CLI environment
- Awareness of weak password practices in data hiding

🏁 Final Flag

PIRATE{t0rr3nt_of_tr4cks}

Created by Karthik | Forensics & Ethical Hacking Enthusiast