Behind the Pixels

Category: Forensics/Steganography

Difficulty: Medium

1.Discovery & Extraction:

Initial analysis with binwalk reveals a hidden zip archive appended to challenge.jpg.

- **Command:** binwalk -e challenge.jpg
- **Result:** A password-protected zip file is extracted from the image.

2. Cracking the Password:

We use **John the Ripper** to crack the archive's password.

- **Generate Hash:** Convert the zip to a hash format. zip2john extracted_data.zip > hash.txt
- **Brute Force:** Run the hash against the rockyou.txt wordlist. john --wordlist=/usr/share/wordlists/rockyou.txt hash.txt
- **Result:** John successfully identifies the password: princess123

3. Solving:

Unzipping the archive with the recovered password reveals flag.txt.

- **Flag:** LNM{H1dd3N_B3H1ND}