Darcy – HuntressCTF 2025 (Forensics)

Category: Forensics

Difficulty: Easy/Medium

Points: TBD

Challenge Description

> Darcy has apparently been having a lot of fun with a unique version control system. She told me she hid a flag somewhere with her new tool and wants me to find it… I can't make any sense of it, can you?

Given: `darcy.tar.gz`

Solution

Step 1: Extract the Archive

First, we extract the provided archive to examine its contents:

```bash
mkdir darcy_extracted
tar -xvzf darcy.tar.gz -C darcy_extracted
cd darcy_extracted
```

Inside, we find a directory called `darcy/` containing many files with hash-like names and a suspicious folder: `_darcs/`.

Step 2: Identify the Version Control System

The presence of the `_darcs/` directory is the key clue. This indicates we're dealing with a **Darcs repository** — a distributed version control system that's less commonly known than Git or SVN.

The challenge title "Darcy" is a play on "Darcs," hinting at this connection.

Step 3: Search for the Flag

Rather than manually parsing through Darcs patches and history, we can take advantage of the fact that version control systems often store metadata in plaintext files.

A simple recursive grep through the repository reveals the flag:

```bash
grep -r "flag{" .
```

Output:

```
./_darcs/hashed_inventory:[routine update; details: flag{a0c1e852e1281d134f0ac2b8615183a3}
```

The flag was embedded directly in the Darcs inventory file, likely as part of a commit message or patch description.

Alternative Solution: Direct File Inspection

If you want to avoid grepping the entire directory, you can target the Darcs metadata specifically:

```bash
grep -r "flag{" _darcs/
```

Or even more precisely, inspect the inventory file directly:

```bash
cat _darcs/hashed_inventory | grep "flag{"
```

This approach is cleaner and focuses only on the version control metadata where such information is typically stored.

Flag

```
flag{a0c1e852e1281d134f0ac2b8615183a3}
```

Key Takeaways

1. **Recognize the VCS:** The `_darcs/` directory is the signature of a Darcs repository. Knowing obscure version control systems can be crucial in forensics challenges.

2. **Metadata is evidence:** Version control systems store rich metadata — commit messages, patch descriptions, author info — that can leak sensitive information.

3. **Simple tools work:** You don't always need specialized commands. Basic tools like `grep` can quickly surface hidden data in VCS metadata.

4. **The challenge name is a hint:** "Darcy" → "Darcs" was a clever nudge toward identifying the technology in use.

Resources

- Darcs Documentation

- Understanding VCS forensics and metadata analysis

Solved by: TUMhacks
Date: October 20, 2025