Passwords - A Cracking Christmas

Day 9

Learn how to crack password-based encrypted files.

- Attacks Against Encrypted Files

Attacks Against Encrypted Files

Overview

Room URL: https://tryhackme.com/room/attacks-on-ecrypted-files-aoc2025-asdfghj123

Difficulty: Easy

Category: Password Cracking

Date Completed: 12/9/2025

Objectives

- How password-based encryption protects files such as PDFs and ZIP archives.
- Why weak passwords make encrypted files vulnerable.
- How attackers use dictionary and brute-force attacks to recover passwords.
- A hands-on exercise: cracking the password of an encrypted file to reveal its contents.
- The importance of using strong, complex passwords to defend against these attacks.

Table of Contents

Introduction

In Wareville's ongoing battle against King Malhare's cyber operations, we've discovered that the true vulnerability lies not in modern encryption algorithms themselves, but in the passwords that protect them. Attackers rarely attempt to break encryption directly—it's computationally infeasible—instead focusing their efforts on password recovery through dictionary attacks and brute-force techniques. This challenge demonstrates how weak passwords create catastrophic

security failures and how defenders must understand these attack methodologies to identify and prevent them. By analyzing encrypted files and recovering their passwords using industry-standard tools like `pdfcrack` and `john`, we gain critical insight into both offensive and defensive password security practices.

Password Recovery Tools

`pdfcrack`

- Specialized tool for breaking PDF passwords
- Syntax: `pdfcrack -f [file.pdf] -w [wordlist.txt]`
- Works directly with PDF encryption
- Fast and effective for dictionary attacks

`john` (John the Riiper)

- Flexible, multi-format password cracker
- Supports hundreds of hash types and encryption methods
- Syntax: `john --wordlist=[wordlist] [hash_file]`
- Can be enhanced with rules (`--rules`) for pattern-based guessing
- Maintains a potfile (`~/.john/john.pot`) to track cracked passwords

Helper Utilities:

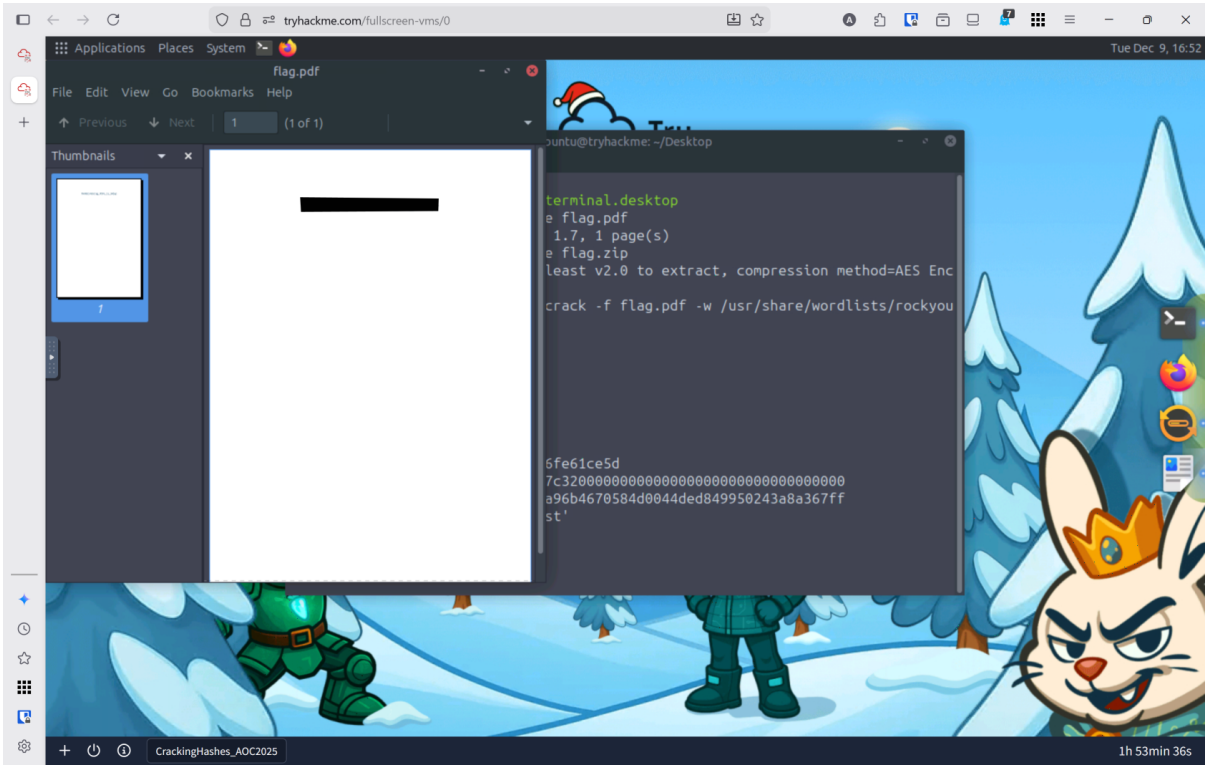
- `zip2john`: Converts ZIP encryption to john-compatible hash format
- `pdf2john`: Converts PDF encryption to john-compatible hash format

`hashcat` (Alternative)

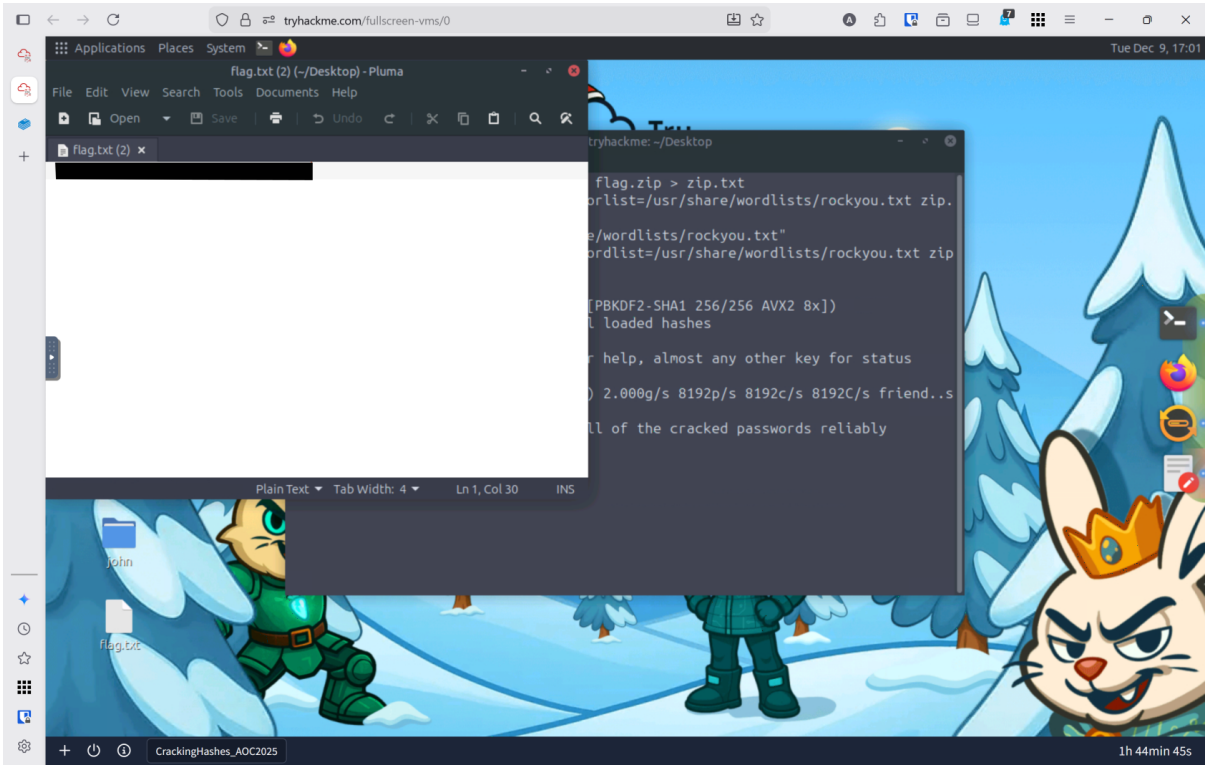
- GPU-accelerated password cracker
- Dramatically faster than CPU-only tools for large-scale attacks
- Supports mask attacks: `?l?l?l?d?d` (3 lowercase + 2 digits)
- More resource-intensive but essential for complex passwords

---

Walk Through

1. Start the target machine
2. What is the flag inside the encrypted PDF?
    1. Can either use `pdfcrack` or `pdf2john`
    2. Used `pdfcrack` and the `rockyou` breach to crack the password
        1. `pdfcrack -f flag.pdf -w /usr/share/wordlists/rockyou.txt`
        2. password: `naughtylist`
    3. The only page of the document is the flag
    4. 

3. What is the flag inside the encrypted zip file?
    1. Can use `fcrackzip` or `zip2john`
    2. `zip2john flag.zip > zip.txt`
    3. `john --wordlist=/usr/share/wordlists/rockyou.txt zip.txt`
        1. `winter4ever`

4. 

4.

Lessons Learned

- **Dictionary attacks remain devastatingly effective** because users consistently choose weak, predictable passwords from a limited pool of common choices. The `rockyou.txt` wordlist alone demonstrates the scale of password reuse across breached services.
- **Understanding attacker methodologies is essential for defense.** By mastering tools like `john`, `pdfcrack`, and `hashcat`, we can better detect unauthorized cracking attempts through process monitoring, GPU utilization analysis, and file activity telemetry—enabling Wareville's security teams to respond before data is compromised or exfiltrated.

Resources

TryHackMe

Hashcat

John the Ripper

PDF2John

Zip2John