Day 13: Cryptography and Capture The Flag Challenges

Date: July 2, 2025

Topics Covered:

- Basics of Cryptography
- Hands-on experience with TryHackMe's Capture the Flag (CTF) module
- Steganography using Steghide and spectrogram analysis
- Concept of Security Through Obscurity

What I Did:

Today, I practiced cryptography and steganography through **TryHackMe's CTF challenges**. I focused on decoding encrypted messages and learned how data can be hidden inside files using **tools like Steghide** and **audio spectrograms**. I also studied the concept of **security through obscurity** and its limitations.

TryHackMe Module: Capture the Flag

1. Decode and Translate Challenges

- Worked with encrypted messages such as Base64, hexadecimal, ROT13, and Caesar Cipher.
- Used **CyberChef**, an online tool that can automatically detect encoding formats and decode them with minimal effort.
- These types of transformations are common in beginner-level CTFs.

2. Hidden Data in Audio using Spectrograms

- Audio files can be modified to hide text or images in their frequency spectrum.
- Opened .wav or .mp3 files in **Audacity**.
- Switched to **spectrogram view** to visually analyze audio frequencies.
- Hidden messages often appear as shapes or text in the frequency bands.

3. Steganography using Steghide

- Learned how to embed a text file into an image using **Steghide**.
- The process involves providing a **cover file** (e.g., an image), a **secret file** (e.g., text), and a **passphrase**.
- Also practiced **extracting** hidden data from the image using the same tool.
- Steghide adds a layer of protection by requiring the correct password during extraction.

4. Security Through Obscurity

- Explored the idea of hiding security flaws or sensitive data in non-obvious places.
- Understood why **relying only on obscurity is not secure** — attackers with the right tools can still find hidden data.
- Emphasized that proper cryptographic and access control measures should be used instead.

Key Learnings:

- Basic encryption techniques are essential for solving CTF puzzles.
- CyberChef makes it easy to decode or analyze encrypted text.
- Steganography provides covert communication methods but is not foolproof.
- Spectrograms offer an interesting way to hide or extract messages from sound files.
- Security must rely on sound practices, not just hiding information.