Steganography!

CTF Café Term 2, Week 4

Presentation by Miguel

What is Steganography?

- Steganography, or Steg for short, is a CTF category focused on hiding data in data.
- Steg challenges are sometimes listed in the Forensics category…
- Steg can often be a bit frustrating, as its about finding the right tool or technique to extract hidden information.

Types of Steg Challenges

- All steg challenges follow the same structure of having data hidden in data.
- However, I've tried to broadly categorise them! We have:
  - Image challenges
  - Audio challenges
  - Text challenges
  - PDF challenges
  - ZIP challenges
- There are toolsets used for each type of challenge – knowing what tool to use when comes with experience!

Initial Methodology

Remember the Forensics presentation from last term? Use the file command as a starting point for steg challenges too!

General Tools

- strings
  - View strings in a file
- Magic Bytes
  - Check the file signature of a file
- Stegsolve
  - Can sometimes help auto-solve a challenge
- Binwalk
  - For extracting/file carving on otherwise innocuous files

Image Challenges – Resources

- steghide
- pngcheck
- zsteg
- https://futureboy.us/stegano/decinput.html
- http://stylesuxx.github.io/steganography/
- https://www.mobilefish.com/services/steganography/steganography.php
- https://manytools.org/hacker-tools/steganography-encode-text-into-image/
- https://steganosaur.us/dissertation/tools/image
- https://georgeom.net/StegOnline
- http://magiceye.ecksdee.co.uk/

Audio Challenges – Resources

- Audacity
- Sonic Visualiser
- Deepsound
- SilentEye
- https://steganosaur.us/dissertation/tools/audio

What About More Advanced Steg Techniques?

Let’s talk about significant bytes…

MSB/LSB Steganography

- Images use pixel intensities to determine what colour shows for each pixel.
- We can use tools such as Python to manipulate each pixel by a tiny amount using its most or least significant byte.
- These challenges often involve scripting…
- Python Image Library (also known as PIL or Pillow) is your best friend!!

Challenges to try on PicoGym!

- hideme (100 points)
- MSB (200 points)

Plus, check out stego-toolkit for a good list of tools for steg challenges!

Want Something Harder?

Try finishing these first two challenges, and I can provide more as you go along and help walk you through ☺

Thanks for coming!