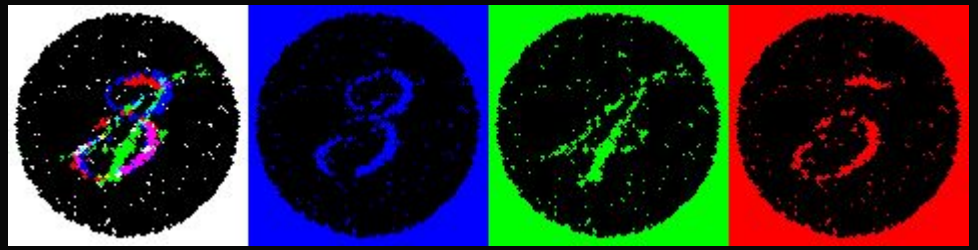
› Cybersecurity UW

Steganography Workshop

What is Steganography?

- “the practice of representing information within another message or physical object, in such a manner that the presence of the concealed information would not be evident to an unsuspecting person's examination”

- TLDR: hiding secret information in plain sight



Steganography vs Encryption

- Encryption: Information is scrambled (and sometimes also hidden), so that only a person with a specific key can decrypt it and access it

- Steganography: Information is hidden, but not scrambled. Anyone who knows of its existence can read it

Steganography vs Encryption

	Encryption	Steganography
Purpose	Scrambles a message	Hides a message
High-level idea	Convert data into ciphertext	Conceal data in another medium
Visibility	Message is visible, but unreadable	Message is not visible by standard methods
Security Focus	Confidentiality and privacy	Concealment and deception

File signatures

- How Unix determines the type of a file:
  - First few bytes in file (called magic bytes)
  - Examples:
    - 7F 45 4C 46 - elf file
    - 89 50 4E 47 0D 0A 1A 0A - png image
    - 25 50 44 46 - pdf file
- How Windows determines the type of a file:
  - Extension
  - Examples:
    - .dll - dll file
    - .png - png image
    - .pdf - pdf file

Common techniques and tools

- Images
  - EXIF data
  - LSB of pixel values
  - DCT compression coefficients (frequency domain steganography)
- Audio
  - Spectrogram
  - LSB/Phase of audio sample
  - Echo hiding
- Video
  - LSBs of pixel values in specific frames
  - Motion vectors
  - Compression coefficients
- Message
  - Whitespace
  - Font/formatting

Common techniques and tools

- Hexdump:

```
noah@laptop Downloads % hexdump -C image_with_secret.png
00000000  89 50 4e 47 0d 0a 1a 0a  00 00 00 0d 49 48 44 52  |.PNG........IHDR|
00000010  00 00 07 4a 00 00 03 8c  08 06 00 00 00 c3 b2 30  |...J.........ò0|
00000020  c6 00 00 0c 6b 69 43 43  50 49 43 43 20 50 72 6f  |?...kiCCPICC Pro|
00000030  66 69 6c 65 00 00 48 89  95 57 07 58 13 49 1b 9e  |file..H..W.X.I..|
00000040  2d 49 48 48 42 09 44 40  4a e8 4d 10 e9 45 4a 08  |-IHHB.D@J?M.?EJ.|
00000050  2d 82 80 54 c1 46 48 02  09 25 c6 84 a0 62 57 0e  |-..T?FH..%?.?bW.|
00000060  15 3c bb 88 62 c5 8a 28  7a 7a 02 72 a8 88 bd 1c  |.<?.b?.(zz.r?.?.|
00000070  8a dd b3 1c ea a1 a2 9c  87 05 45 51 f9 27 05 f4  |.\.E...EQ?'.?|
00000080  bc bf 3c ff f7 3c b3 f3  ee 3b df 7c 6d 67 76 77  |??<??<???;?|mgvw|
00000090  00 d0 e9 e5 49 a5 79 a8  2e 00 f9 92 02 59 42 64  |.???I?y?..?..YBd|
000000a0  28 6b 6c 5a 3a 8b d4 09  10 40 07 3a c0 16 18 f2  |(klZ:.?..@.:?..?|
000000b0  f8 72 29 3b 3e 3e 06 40  19 e8 ff 2e ef 6e 42 6d  |?r);>>.@.??.?nBm|
000000c0  28 d7 5c 94 b6 fe 39 fe  5f 45 5f 20 94 f3 01 40  |(?\.??9?_E_ .?.@|
000000d0  c6 43 9c 29 90 f3 f3 21  6e 06 00 df c0 97 ca 0a  |?C.).??!n..??.?.|
000000e0  00 20 2a 79 eb a9 05 52  25 9e 0b b1 81 0c 06 08  |. *y?.R%..?....|
```

- Binwalk:

```
craig@laptop:/tmp/firmware$ binwalk DIR-890L_Ax_FW110b07.bin

                                /tmp/firmware/DIR-890L_Ax_FW110b07.bin

DECIMAL                     HEXADECIMAL                 DESCRIPTION
--------------------------------------------------------------------------------
0                           0x0                         DLOB firmware header, header size: 116 bytes, data size: 19996704
116                         0x74                        LZMA compressed data, properties: 0x5D, dictionary size: 33554432 bytes, uncompressed size: 4897632 bytes
1835124                     0x1C0074                    PackImg firmware header, header size: 32 bytes, data size: 2102529 bytes
1835156                     0x1C0094                    SquashFS file system, little endian, version: 4.0, compression: xz, inode count: 2673, block size: 131072, image size: 18159869 bytes, created: 2016-05-24
                                                        09:50:50
--------------------------------------------------------------------------------

Analyzed 1 file for 71 file signatures (174 magic patterns) in 121.0 milliseconds
craig@laptop:/tmp/firmware$ binwalk DIR-890L_Ax_FW110b07.bin
```

Links and demos

- Example 1: LSB encoding
- Example 2: Spectrogram
- Example 3: Image Data Appending

Now you try:

- Demo 1: Simple byte append