IoT: Client Devices

Binwalk

What is Binwalk?

Firmware Analysis

- Allows you to list the contents of a firmware file
- Perform entropy analysis
- Identify platform dependencies

Firmware Extraction

- Filesystems
- Operating systems
- Application software

Installation

Runs on Linux

- You'll need to use your linux VM

Complex installation process

- Many dependencies

Written in python

- Dependencies are in both Python and at OS level

Installation

Installation instructions *mostly* accurate

- Packages correct
- Some things better installed with APT, not PIP

Installation tools

- PIP: An installation framework for Python
- APT: An installation framework for Debian

You'll use both

- Python libs with PIP, OS packages with APT

Installation

Python 2 or Python 3?

- I use Python 2, but you can use Python 3
- Don't install both

How do I install?

- See https://github.com/devttys0/binwalk/blob/master/INSTALL.md
- I suggest you install libcapstone3 as well via APT
  - sudo apt install libcapstone3

Installation

How do I know it worked?

```
cclamb@angr:~$ binwalk

Binwalk v2.1.1
Craig Heffner, http://www.binwalk.org

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Disassembly Scan Options:
    -Y, --disasm                Identify the CPU architecture of a file using t
he capstone disassembler
    -T, --minsn=<int>           Minimum number of consecutive instructions to b
e considered valid (default: 500)
```

It didn't work!

LIBCAPSTONE3

- Try installing libcapstone3 from APT if you didn't originally.
- $ sudo apt install libcapstone3

PYTHON ERRORS

- Use only Python 2 or Python 3
- Deinstall all your python, they try again with one or the other, not both