This material is based upon work supported by the Defense
Advanced Research Projects Agency (DARPA) under Contract No.
HR001119C0102. The opinions, findings, and conclusions stated
herein are those of the authors and do not necessarily reflect
those of DARPA.

IBR tools

Introduction

Internet background radiation (IBR) are packets gathered from dark (unpopulated) networks, which are known in the IBR community as *telescopes*.

This software contains tools to help gather and analyze IPv4 IBR packets.

Getting started

This file documents how to build and prepare to use the IBR tools, how to build and install them in your local directory, and guidance about how to configure the tools to use on your system with your own data.

Many of these tools are designed to take their parameters from parameter files that define things like the path to the input pcap or CSV files, and where to store the output. You will need to create parameter files for your local setup before you use most of the analysis tools. For more information about the parameter files, look in the `./params` directory and read the documentation in the example parameter files.

For information about the tools for preprocessing pcap files and doing some analyses on them, and the general workflow of analyzing pcap files, look at the README in the `./tools` directory. This directory contains tools to capture pcaps, pre-process them into formats used by the rest of the tools, and perform some analyses.

For examples of quick-look analyses, look at the README and COOKBOOK files in the `./firecracker` directory.

Platform assumptions

These tools were developed and tested on Ubuntu 20.04 and Ubuntu 22.04. Some are known to work correctly on other platforms (or in some cases, they may be easily ported), but these are the only platforms for which we have tested all of the tools.

Some of the tools use libraries or tools that are Linux-specific, and will not work on non-Linux platforms without additional engineering.

Installing and configuring the IBR tools

Installing prerequisite software

Run the `setup-sysadmin.sh` script in this directory. Note that this script requires `sudo` permissions (including permission to install software) to run some of its commands. This script will install software used to build and run the IBR tools.

Building the IBR tools

Run the `setup.sh` script in this directory. The setup script will build the executables that are part of this package, and install them in the `bin` subdirectory of this directory. Note that this will fail if the required packages have not already been installed (usually accomplished using `setup-sysadmin.sh`).

Configuration of the parameter files

Many of the scripts read their parameters from parameter files, and these parameter files must be created and edited before the scripts will work correctly.

The top-level parameter files defines the paths to the input and output directories, and some related paths. If you have more than one IBR telescope (or other data

source), then you will need to have different parameter files for each telescope, in order to avoid overwriting the output files from one telescope with those for another.

A template for the top-level parameter file is given in `params/example.params`.

A key parameter in the top-level parameter file is DATANAME. This variable is used to define other values, and MUST be unique for each different telescope or data source. (if it is not unique, you risk having the analysis files from different telescopes overwrite each other)

The names of two of the other parameter files are defined by DATANAME. These parameter files list the allowed destinations (the addresses within the telescope) and omitted sources (any sources that are ignored by the analysis steps). These are located in the `params` directory, and examples are given in `params/example-allowed-dsts.dat` and `params/example-omitted-srcs.dat`.

Next steps

To begin to capture and analyze data, consult the README file in `./tools`, and the README and COOKBOOK files in `./firecracker`.