CERT Virtual Flow Collection and Analysis

For Training and Simulation

George Warnagiris
Software Engineering Institute

Acquisition Support

Research Technology and Systems Solutions

Software Engineering Process

Enterprise and Workforce Development

Digital Investigations and Intelligence

Cyber Threat and Vulnerability Analysis

Secure Software and Systems
Software Engineering Institute

Enterprise and Workforce Development

Digital Investigations and Intelligence

Cyber Threat and Vulnerability Analysis

Secure Software and Systems

Immersive Learning Technologies

XNET

Network Situational Awareness
CERT Network Situational Awareness ("NetSA")

- Among other work:
  - Applied Research and Development
    - Maintains the SiLK tool suite
    - Analysis Pipeline
  - Operational Analysis
    - Private Network Analysis
    - Network Profiling of Waladec-Infected IP Space
  - Capacity Building
    - Open source software and publications
    - In person and online training
NetSA Online Training Modules

- Network Flow
- SiLK Beginning Flow Analysis
- rwfilter
- Counting Tools: rwcount, rwstats, rwuniq
- rwappend-rwsplit
- rwfileinfo-rwglob
- rwcut and rwcat
- rwsort
- Sets
- Prefix Maps (pmaps)
- Advanced SiLK Tools: Bags
- Using Tuples with SiLK
- LAB: SiLK Training
NetSA Online Virtual Lab

```
login as: silk
silk@10.0.1.9's password:
Last login: Fri Oct 24 15:40:00 2009
[silk@training932 ~]$ which rwfilter
/usr/local/bin/rwfilter
[silk@training932 ~]$ rwfilter --help
More
rwfilter [app-opts] [partition-opts] [<selection-opts>] [<inputFiles>]
Partitions SILK Flow records into one or more 'pass' and/or 'fail' output streams. The source of the SILK records can be stdin, a named pipe, files listed on the command line, or files selected from the data-store via the selection switches. There is no default input or output; these must be specified.

GENERAL SWITCHES:
--help No Arg. Print this usage output and exit. Def. No
--version No Arg. Print this program's version and exit. Def. No
-dry-run No Arg. Parse command line switches but do not process records
-threads Req Arg. Use this number of threads. Def. $SILK_RWFILTER_THREADS or 1
-max-pass-records Req Arg. Set max number of records to pass for all streams. Def. 0
-print- filenames No Arg. Print names of input files during processing. Def. No
--dynamic-library Req Arg. Augment processing with the specified dynamic library. No default
-note-add Req Arg. Store the textual argument in the output SILK file's header as an annotation. Switch may be repeated to add multiple annotations
--note-file-add Req Arg. Store the content of the named text file in the output SILK file's header as an annotation. Switch may be repeated.
-compression-method Req Arg. Set compression for binary output file(s). Def. zlib. Choices: best [-zlib], none, zlib

INPUT/OUTPUT SWITCHES. An input switch or a SELECTION switch (below) is required. At least one output switch is required:
--input-pipe Req Arg. Read SILK flow records from a pipe: 'stdin' or path to named pipe. No default
--xargs Req Arg. Read list of input file names from a file or pipe pathname or 'stdin'. No default
--pass-destination Req Arg. Destination for records which pass the filter(s): pathname or stdout. If pathname, it must not exist. No default
--fail-destination Req Arg. Destination for records which fail the filter(s):
```

Lab: LAB: SILK Training   Lab Manual   Time Remaining: 2:56   Extend   I'm Done   Restart Lab   Help
New Training Modules in 2010

- Introduction to iSiLK
- Overview of PySiLK
- Basic PySiLK Objects
Modules Proposed for 2011
Virtual Training Environment (‘‘VTE’’)

- Training from anywhere with a web browser and Internet connection
- Recorded lectures on a variety of topics
- Hands-on training labs
- Narrated demonstrations
- XXX modules and counting!
- Topics range from CompTIA Network+ to Malware Analysis
Next Generation: VTE3
VTE3

New site design
Faster, more robust
Authoring environment
Labs based on the next generation of VMWare
Communities
Social networking
CERT – Exercise Network ("XNET")

New site design
Faster, more robust
Authoring environment
Labs based on the next generation of VMWare
Communities
Social networking