### Title and Subtitle
CERT Virtual Flow Collection and Analysis: For Training and Simulation

### Author(s)
Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213

### Distribution/Availability Statement
Approved for public release; distribution unlimited

### Abstract
FloCon 2011, in Salt Lake City, Utah, on January 10-13, 2011.

### Subject Terms
unclassified

### Security Classification of:
- a. Report: unclassified
- b. Abstract: unclassified
- c. This Page: unclassified

### Limitation of Abstract
Same as Report (SAR)

### Number of Pages
14

---

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std Z39-18
© 2011 Carnegie Mellon University

NO WARRANTY

THIS MATERIAL OF CARNEGIE MELLON UNIVERSITY AND ITS SOFTWARE ENGINEERING INSTITUTE IS FURNISHED ON AN “AS-IS” BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

This presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

This work was created in the performance of Federal Government Contract Number FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The government of the United States has a royalty-free government-purpose license to use, duplicate, or disclose the work, in whole or in part and in any manner, and to have or permit others to do so, for government purposes pursuant to the copyright license under the clause at 252.227-7013.

CERT® is a registered mark owned by Carnegie Mellon University.
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

## Table of Contents

1. **Introduction**
   1.1 Lab Topology 3
   1.2 Description of data in the lab repositories 4
   1.3 Tips on using the SILK lab systems 4

2. **SILK Lab Exercises**
   2.1 Lab Section 1 – Beginning Analysis Exercises 6
      2.1.1 Lab 1.1 – Connecting to and logging onto the SILK lab 6
      2.1.2 Lab 1.2 – Determine data repository’s dates, classes and sensors 6
      2.1.3 Lab 1.3 – Explore the repository 6
   2.2 Lab Section 2 – rwfilter Exercises 7
      2.2.1 Lab 2.1 – Explore rwfilter Options 7
      2.2.2 Lab 2.2 – Track an individual address or individual address block 7
      2.2.3 Lab 2.3 – Categorizing Traffic with rwfilter 8
      2.2.4 Lab 2.4 – Tracking Traffic 8
      2.2.5 Lab 2.5 – Chaining rwfilter Commands Together 9
   2.3 Lab Section 3 – Printing and Sorting Tools 9
      2.3.1 Lab 3.1 – Formatting Output 9
      2.3.2 Lab 3.2 – Finding Specific Behavior 10
   2.4 Lab Section 4 – Other Tools 11
      2.4.1 Lab 4.1 – Using Other Tools to Find Behavior 11
      2.4.2 Lab 4.2 – eventid and the Destination IP Distinct Feature 11
      2.4.3 Lab 4.3 – Exploring rwfileinfo 12
   2.5 Lab Section 5 – Sets 12
      2.5.1 Lab 5.1 – Using Block Lists 12
      2.5.2 Lab 5.2 – Taking Network Inventories 12
   2.6 Lab Section 6 – Bags 13
      2.6.1 Lab 6.1 – Find DNS Clients 13
   2.7 Lab Section 7 – Prefix Maps 13
      2.7.1 Lab 7.1 – Experimenting with pmaps 13
      2.7.2 Lab 7.2 – pmaps and ICMP 14
NetSA Online Virtual Lab
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

Courses

Search: Gea·c1

Wireless Comms and Wireless Network Security
This class covers signal theory, RF propagation, antennas, and wireless network mapping. It also includes the 802.11 protocol series, security implications of wireless networking, and best practices.
Sections: 0
Members: 0

Vulnerability Assessment and Remediation
Vulnerability Assessment and Remediation
Sections: 1
Members: 1

Using SILK for Network Traffic Analysis
Using SILK for Network Traffic Analysis Description
Sections: 0
Members: 0

Using Einstein for Network Traffic Analysis
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