CERT Virtual Flow Collection and Analysis
For Training and Simulation
George Warnagiris
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

Carnegie Mellon

Software Engineering Institute

Acquisition Support

CERT

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
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
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