



# **CERT Virtual Flow Collection and Analysis**

For Training and Simulation

**George Warnagiris**



| Report Documentation Page                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                    |                                     |                                                           | Form Approved<br>OMB No. 0704-0188                  |                                 |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------|-------------------------------------|-----------------------------------------------------------|-----------------------------------------------------|---------------------------------|
| Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. |                                    |                                     |                                                           |                                                     |                                 |
| 1. REPORT DATE<br><b>JAN 2011</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                    | 2. REPORT TYPE                      |                                                           | 3. DATES COVERED<br><b>00-00-2011 to 00-00-2011</b> |                                 |
| 4. TITLE AND SUBTITLE<br><b>CERT Virtual Flow Collection and Analysis: For Training and Simulation</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                    |                                     |                                                           | 5a. CONTRACT NUMBER                                 |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5b. GRANT NUMBER                                    |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5c. PROGRAM ELEMENT NUMBER                          |                                 |
| 6. AUTHOR(S)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                    |                                     |                                                           | 5d. PROJECT NUMBER                                  |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5e. TASK NUMBER                                     |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 5f. WORK UNIT NUMBER                                |                                 |
| 7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)<br><b>Carnegie Mellon University, Software Engineering Institute, Pittsburgh, PA, 15213</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                    |                                     |                                                           | 8. PERFORMING ORGANIZATION REPORT NUMBER            |                                 |
| 9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                    |                                     |                                                           | 10. SPONSOR/MONITOR'S ACRONYM(S)                    |                                 |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           | 11. SPONSOR/MONITOR'S REPORT NUMBER(S)              |                                 |
| 12. DISTRIBUTION/AVAILABILITY STATEMENT<br><b>Approved for public release; distribution unlimited</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                    |                                     |                                                           |                                                     |                                 |
| 13. SUPPLEMENTARY NOTES<br><b>FloCon 2011, in Salt Lake City, Utah, on January 10-13, 2011.</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     |                                                           |                                                     |                                 |
| 14. ABSTRACT                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                    |                                     |                                                           |                                                     |                                 |
| 15. SUBJECT TERMS                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                                    |                                     |                                                           |                                                     |                                 |
| 16. SECURITY CLASSIFICATION OF:                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |                                    |                                     | 17. LIMITATION OF ABSTRACT<br><b>Same as Report (SAR)</b> | 18. NUMBER OF PAGES<br><b>14</b>                    | 19a. NAME OF RESPONSIBLE PERSON |
| a. REPORT<br><b>unclassified</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | b. ABSTRACT<br><b>unclassified</b> | c. THIS PAGE<br><b>unclassified</b> |                                                           |                                                     |                                 |

---

© 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.

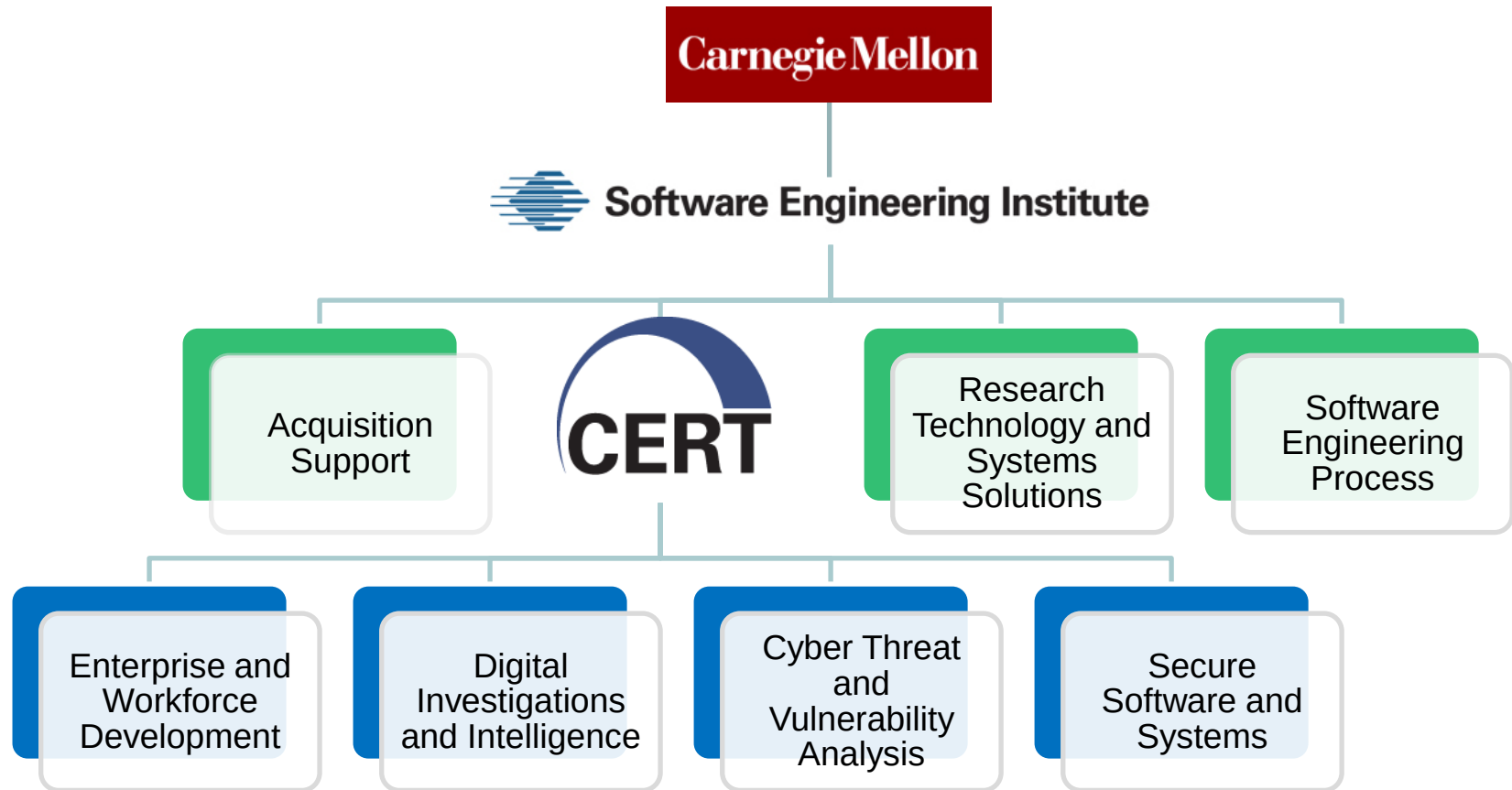
This presentation may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at [permission@sei.cmu.edu](mailto:permission@sei.cmu.edu).

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.



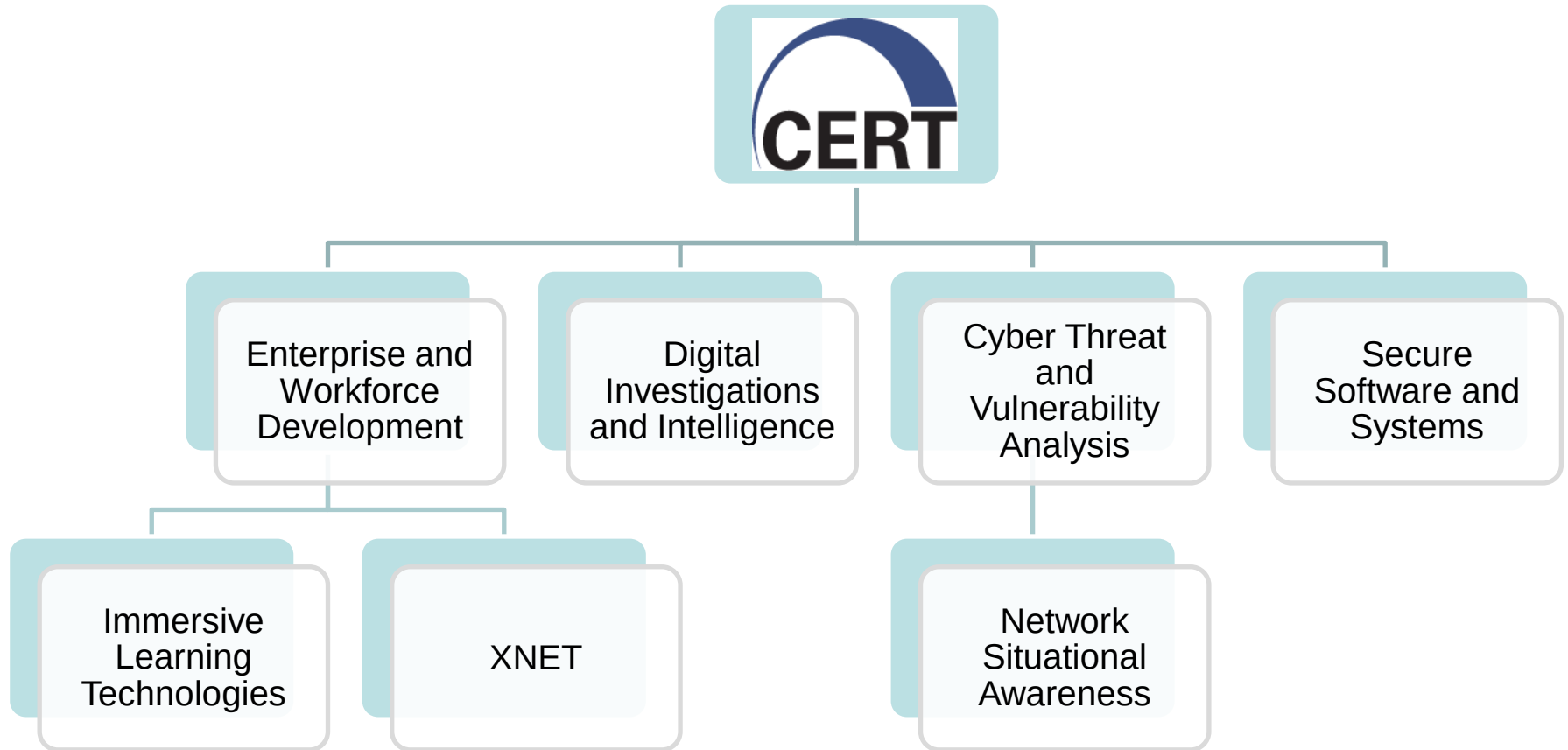
# Software Engineering Institute





# Software Engineering Institute

---



# CERT Network Situational Awareness ("NetSA")

---

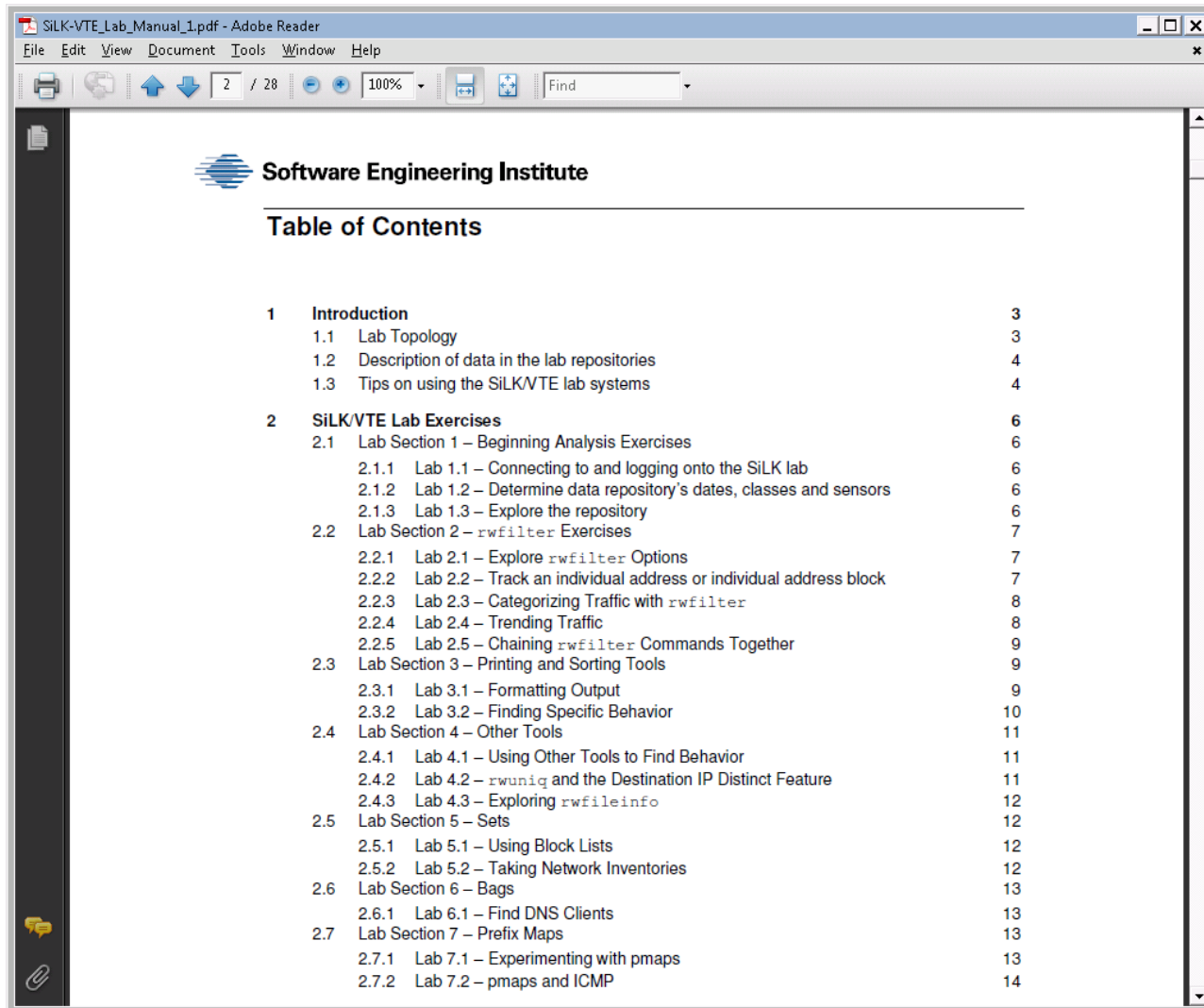
- Among other work:
  - Applied Research and Development
    - Maintains the SiLK tool suite
    - Analysis Pipeline
  - Operational Analysis
    - Private Network Analysis
    - Network Profiling of Waladec-Infected IP Space
  - Capacity Building
    - Open source software and publications
    - In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

# NetSA Online Training Modules

---

- Network Flow
- SiLK Beginning Flow Analysis
- rfilter
- Counting Tools: rwcoun, rwstats, rwuniq
- rwappend-rwsplit
- rwfileinfo-rwglob
- rwcut and rwcatt
- rwsort
- Sets
- Prefix Maps (pmaps)
- Advanced SiLK Tools: Bags
- Using Tuples with SiLK
- LAB: SiLK Training

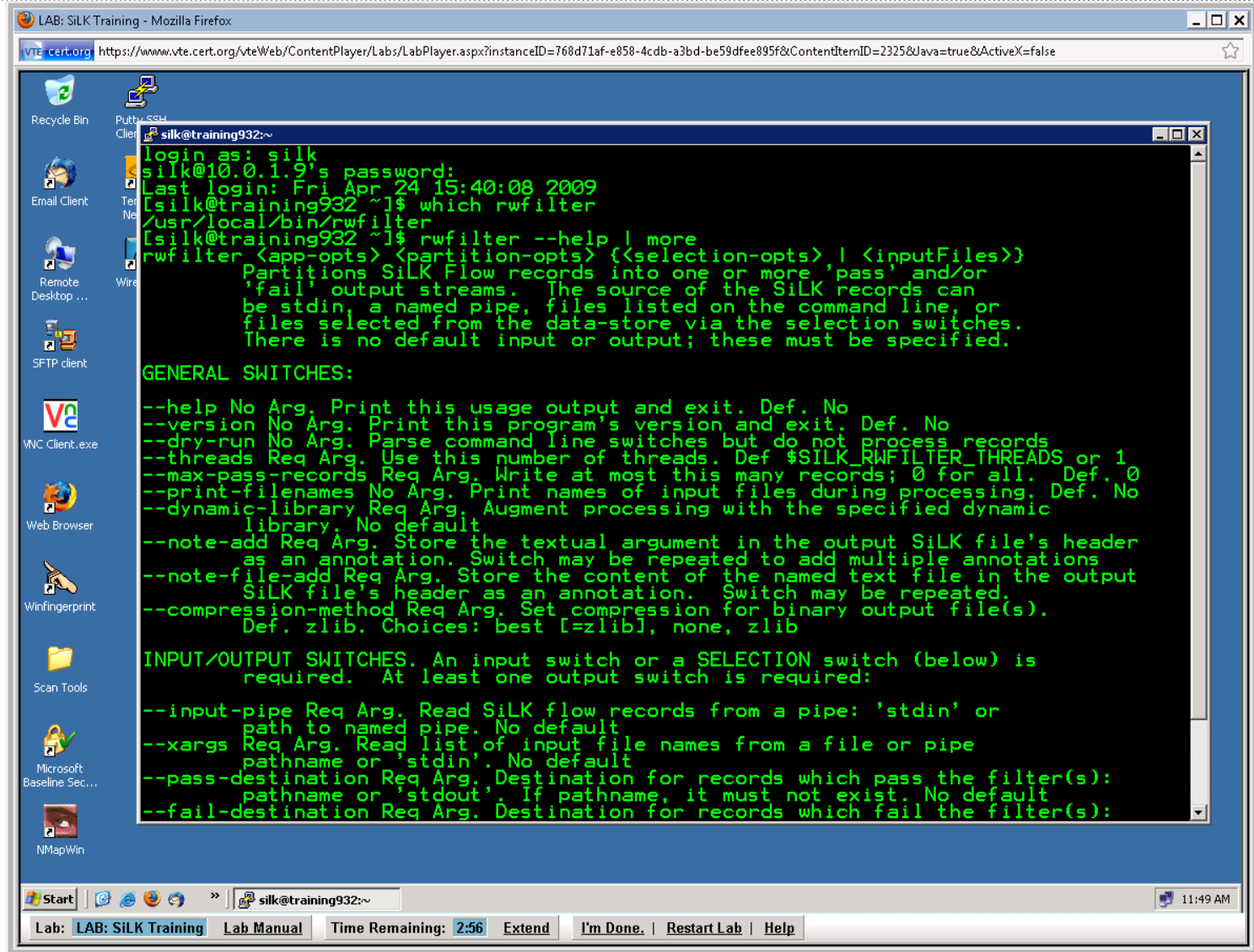
# NetSA Online Virtual Lab



|                                                                                                                         |                                                                       |          |
|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------|----------|
|  <b>Software Engineering Institute</b> |                                                                       |          |
| <hr/>                                                                                                                   |                                                                       |          |
| <b>Table of Contents</b>                                                                                                |                                                                       |          |
| <b>1</b>                                                                                                                | <b>Introduction</b>                                                   | <b>3</b> |
| 1.1                                                                                                                     | Lab Topology                                                          | 3        |
| 1.2                                                                                                                     | Description of data in the lab repositories                           | 4        |
| 1.3                                                                                                                     | Tips on using the SILK/VTE lab systems                                | 4        |
| <b>2</b>                                                                                                                | <b>SILK/VTE Lab Exercises</b>                                         | <b>6</b> |
| 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 – <code>rwfilter</code> Exercises                       | 7        |
| 2.2.1                                                                                                                   | Lab 2.1 – Explore <code>rwfilter</code> 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 <code>rwfilter</code>             | 8        |
| 2.2.4                                                                                                                   | Lab 2.4 – Trending Traffic                                            | 8        |
| 2.2.5                                                                                                                   | Lab 2.5 – Chaining <code>rwfilter</code> 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 – <code>rwuniq</code> and the Destination IP Distinct Feature | 11       |
| 2.4.3                                                                                                                   | Lab 4.3 – Exploring <code>rwfileinfo</code>                           | 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 <code>pmaps</code>                       | 13       |
| 2.7.2                                                                                                                   | Lab 7.2 – <code>pmaps</code> and ICMP                                 | 14       |



# NetSA Online Virtual Lab



```
LAB: SiLK Training - Mozilla Firefox
vte cert.org https://www.vte.cert.org/vteWeb/ContentPlayer/Labs/LabPlayer.aspx?instanceID=768d71af-e858-4cdb-a3bd-be59dfee895f&ContentItemID=2325&Java=true&ActiveX=false

Recycle Bin Putty SSH Client
silk@training932:~
login as: silk
silk@10.0.1.9's password:
Last login: Fri Apr 24 15:40:08 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. Write at most this many records; 0 for all. 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):
```

Start | silk@training932:~ | 11:49 AM

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

The screenshot shows a web browser window titled "Courses | VTE - Mozilla Firefox". The address bar displays "https://www.vte.cert.org/lms/Courses". The browser's menu bar includes "File", "Edit", "View", "History", "Bookmarks", "Tools", and "Help". The page's navigation bar is blue and contains a logo, links for "Home", "Courses", "Content", and "Communities", and buttons for "Sign In" and "Register".

The main content area is titled "Courses" and features a search bar with the text "Search" and a result count of "1-10 of 63 results found." Below the search bar, there are three course listings:

- Wireless Comms and Wireless Network Security**: This class covers signal theory, RF propagation, antennas, and wireless network mapping all the way to 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. A link to "View Details" is provided.
- Using SILK for Network Traffic Analysis**: Using SILK for Network Traffic Analysis Description. Sections: 0, Members: 0.

At the bottom of the page, there is a footer that reads "VTE © Carnegie Mellon University 2006-2010. All rights reserved." and a link to "Terms and Conditions".

# 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