



# **CERT Virtual Flow Collection and Analysis**

For Training and Simulation

**George Warnagiris**



---

© 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

Carnegie Mellon



Software Engineering Institute

Acquisition  
Support



Research  
Technology and  
Systems  
Solutions

Software  
Engineering  
Process

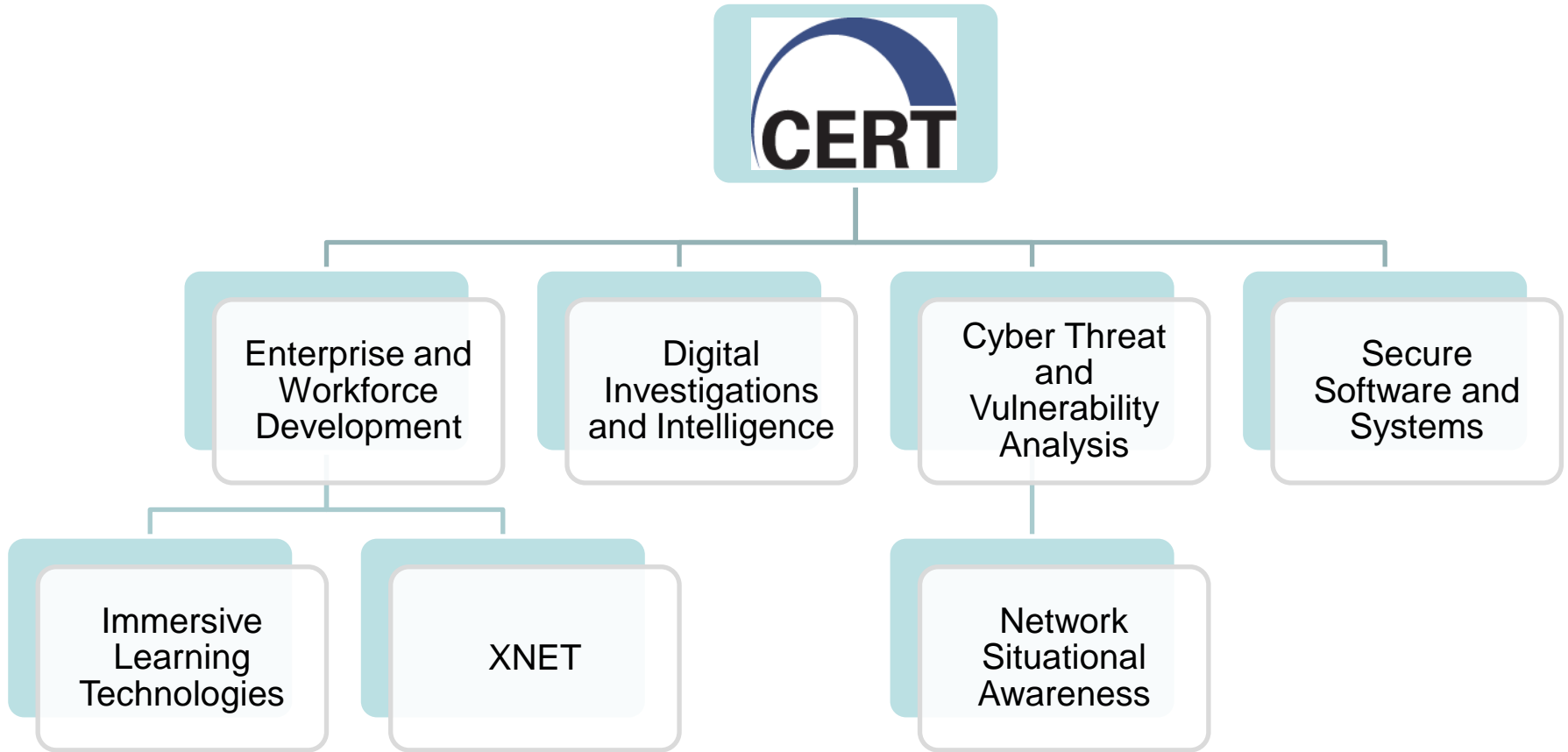
Enterprise and  
Workforce  
Development

Digital  
Investigations  
and Intelligence

Cyber Threat  
and  
Vulnerability  
Analysis

Secure  
Software and  
Systems

# Software Engineering Institute



# CERT Network Situational Awareness (“NetSA”)

---

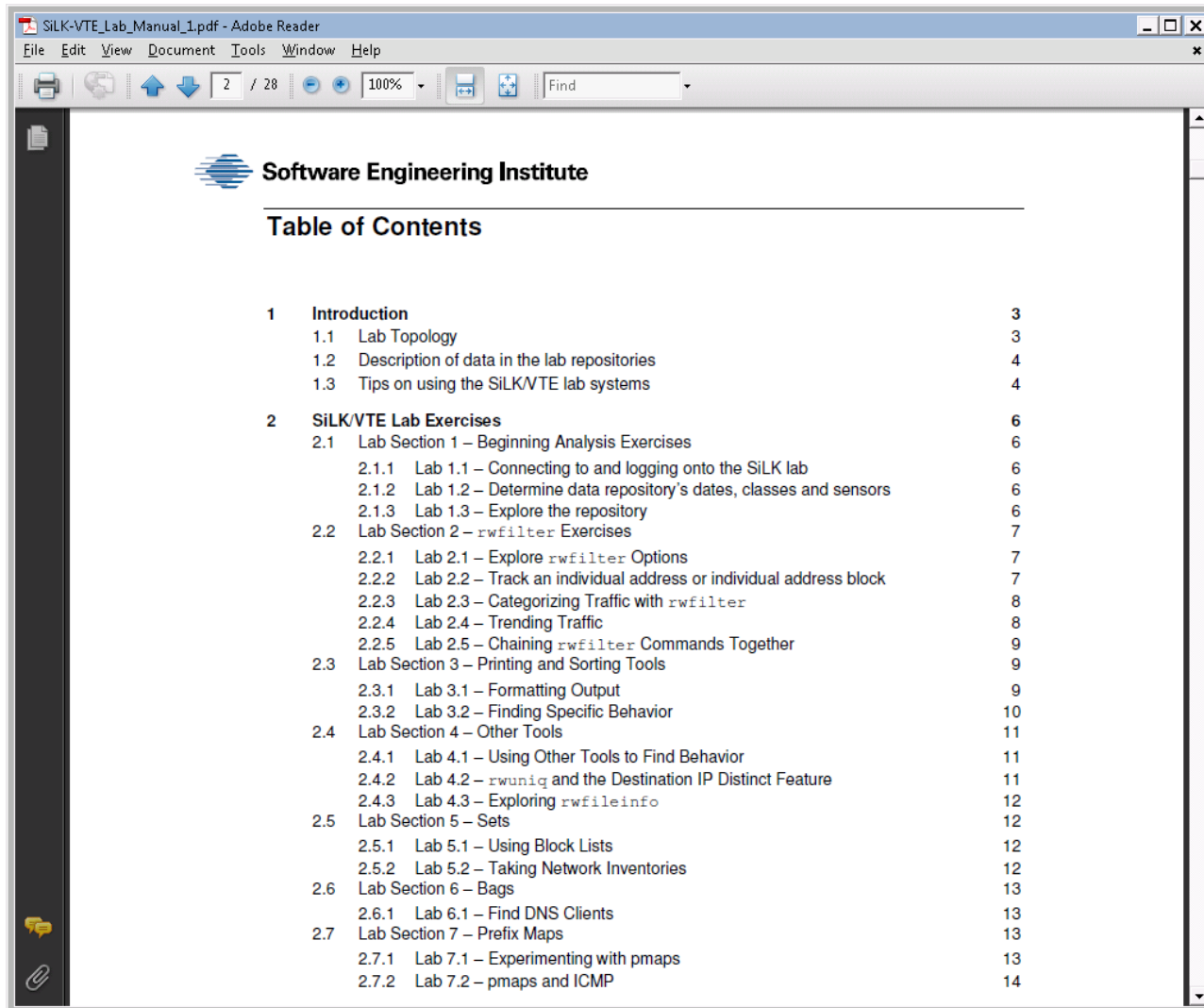
- Among other work:
  - Applied Research and Development
    - Maintains the SiLK tool suite
    - Analysis Pipeline
  - Operational Analysis
    - Private Network Analysis
    - Network Profiling of Waladec-Infected IP Space
  - Capacity Building
    - Open source software and publications
    - In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

# NetSA Online Training Modules

---

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

# NetSA Online Virtual Lab



The screenshot shows a window titled 'SILK-VTE\_Lab\_Manual\_1.pdf - Adobe Reader'. The window contains a 'Table of Contents' section with the following entries:

Software Engineering Institute	
Table of Contents	
<b>1</b>	<b>Introduction</b> <span style="float: right;"><b>3</b></span>
1.1	Lab Topology <span style="float: right;">3</span>
1.2	Description of data in the lab repositories <span style="float: right;">4</span>
1.3	Tips on using the SILK/VTE lab systems <span style="float: right;">4</span>
<b>2</b>	<b>SILK/VTE Lab Exercises</b> <span style="float: right;"><b>6</b></span>
2.1	Lab Section 1 – Beginning Analysis Exercises <span style="float: right;">6</span>
2.1.1	Lab 1.1 – Connecting to and logging onto the SILK lab <span style="float: right;">6</span>
2.1.2	Lab 1.2 – Determine data repository’s dates, classes and sensors <span style="float: right;">6</span>
2.1.3	Lab 1.3 – Explore the repository <span style="float: right;">6</span>
2.2	Lab Section 2 – <code>rwfilter</code> Exercises <span style="float: right;">7</span>
2.2.1	Lab 2.1 – Explore <code>rwfilter</code> Options <span style="float: right;">7</span>
2.2.2	Lab 2.2 – Track an individual address or individual address block <span style="float: right;">7</span>
2.2.3	Lab 2.3 – Categorizing Traffic with <code>rwfilter</code> <span style="float: right;">8</span>
2.2.4	Lab 2.4 – Trending Traffic <span style="float: right;">8</span>
2.2.5	Lab 2.5 – Chaining <code>rwfilter</code> Commands Together <span style="float: right;">9</span>
2.3	Lab Section 3 – Printing and Sorting Tools <span style="float: right;">9</span>
2.3.1	Lab 3.1 – Formatting Output <span style="float: right;">9</span>
2.3.2	Lab 3.2 – Finding Specific Behavior <span style="float: right;">10</span>
2.4	Lab Section 4 – Other Tools <span style="float: right;">11</span>
2.4.1	Lab 4.1 – Using Other Tools to Find Behavior <span style="float: right;">11</span>
2.4.2	Lab 4.2 – <code>rwuniq</code> and the Destination IP Distinct Feature <span style="float: right;">11</span>
2.4.3	Lab 4.3 – Exploring <code>rwfileinfo</code> <span style="float: right;">12</span>
2.5	Lab Section 5 – Sets <span style="float: right;">12</span>
2.5.1	Lab 5.1 – Using Block Lists <span style="float: right;">12</span>
2.5.2	Lab 5.2 – Taking Network Inventories <span style="float: right;">12</span>
2.6	Lab Section 6 – Bags <span style="float: right;">13</span>
2.6.1	Lab 6.1 – Find DNS Clients <span style="float: right;">13</span>
2.7	Lab Section 7 – Prefix Maps <span style="float: right;">13</span>
2.7.1	Lab 7.1 – Experimenting with <code>pmaps</code> <span style="float: right;">13</span>
2.7.2	Lab 7.2 – <code>pmaps</code> and ICMP <span style="float: right;">14</span>

# NetSA Online Virtual Lab

The screenshot displays a virtual lab environment. At the top, a Mozilla Firefox browser window shows the URL: `https://www.vte.cert.org/vteWeb/ContentPlayer/Labs/LabPlayer.aspx?instanceID=768d71af-e858-4cdb-a3bd-be59dfee895f&ContentItemID=2325&Java=true&ActiveX=false`. Below the browser is a desktop environment with a taskbar and a sidebar of icons. The taskbar includes the Start button, system tray icons, and a taskbar button for 'silk@training932:~'. The sidebar contains icons for Recycle Bin, Putty SSH Client, Email Client, Remote Desktop, SFTP client, WC Client.exe, Web Browser, WinFingerprint, Scan Tools, Microsoft Baseline Sec..., and NMapWin. The central terminal window shows the following text:

```
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):
```

At the bottom of the terminal window, the taskbar shows the Start button, system tray icons, and a taskbar button for 'silk@training932:~'. The system tray shows the time 11:49 AM. Below the terminal window, a control bar contains the following text: 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 with the address bar displaying `https://www.vte.cert.org/lms/Courses`. The page features a blue navigation bar with a logo and menu items: Home, Courses, Content, and Communities. On the right side of the navigation bar, there are links for Sign In and Register, along with a search icon. Below the navigation bar, the main content area is titled "Courses" and includes a search bar with the text "Search" and a result count of "1-10 of 63 results found." with pagination links "1 2 3 4 5 > >>". A "Create a New Course" button is visible in the top right corner. The course list includes:

- 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**: View Details. 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**

The footer of the page contains the text: "VTE © Carnegie Mellon University 2006-2010. All rights reserved. | [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