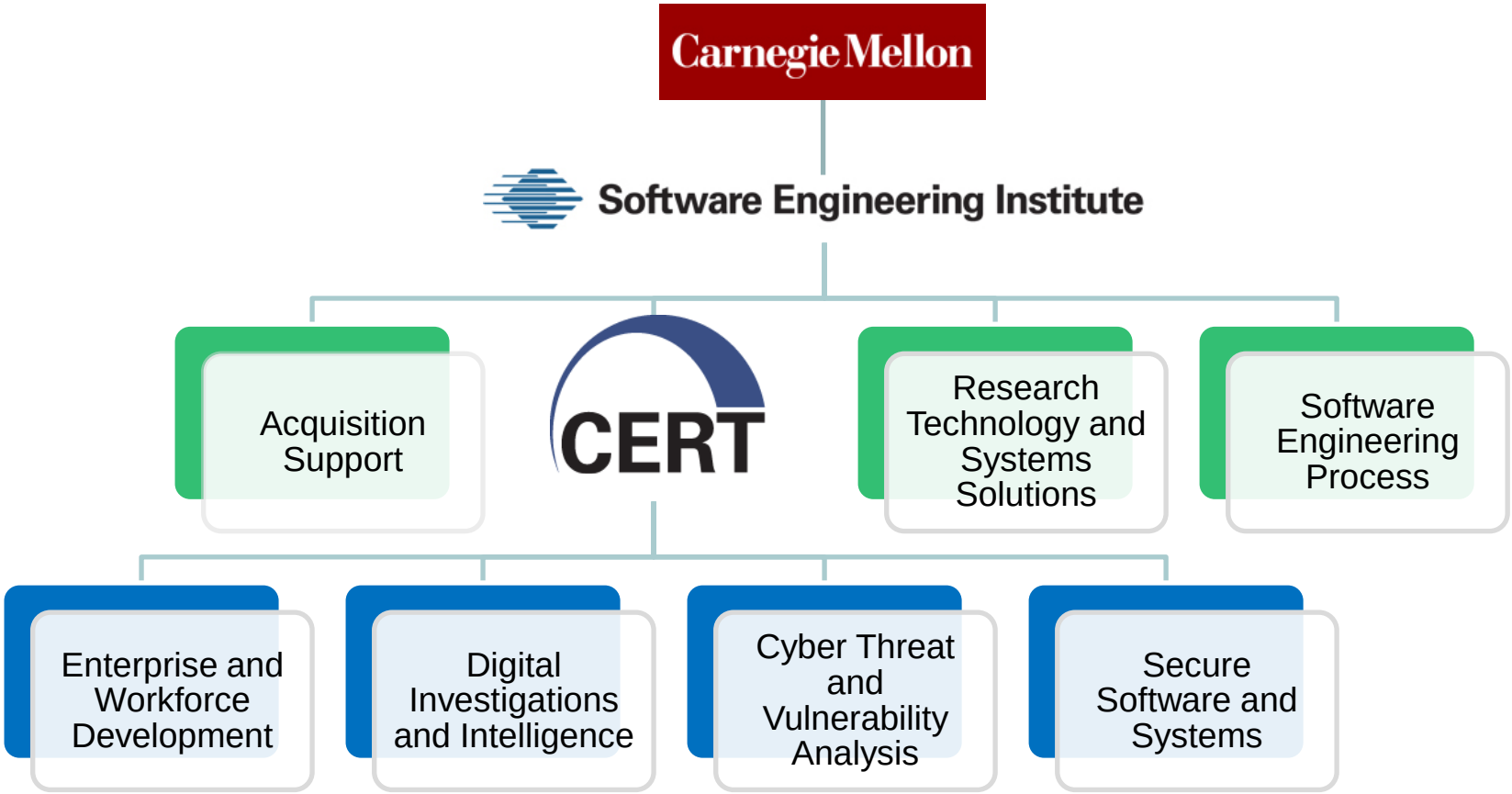
CERT Virtual Flow Collection and Analysis

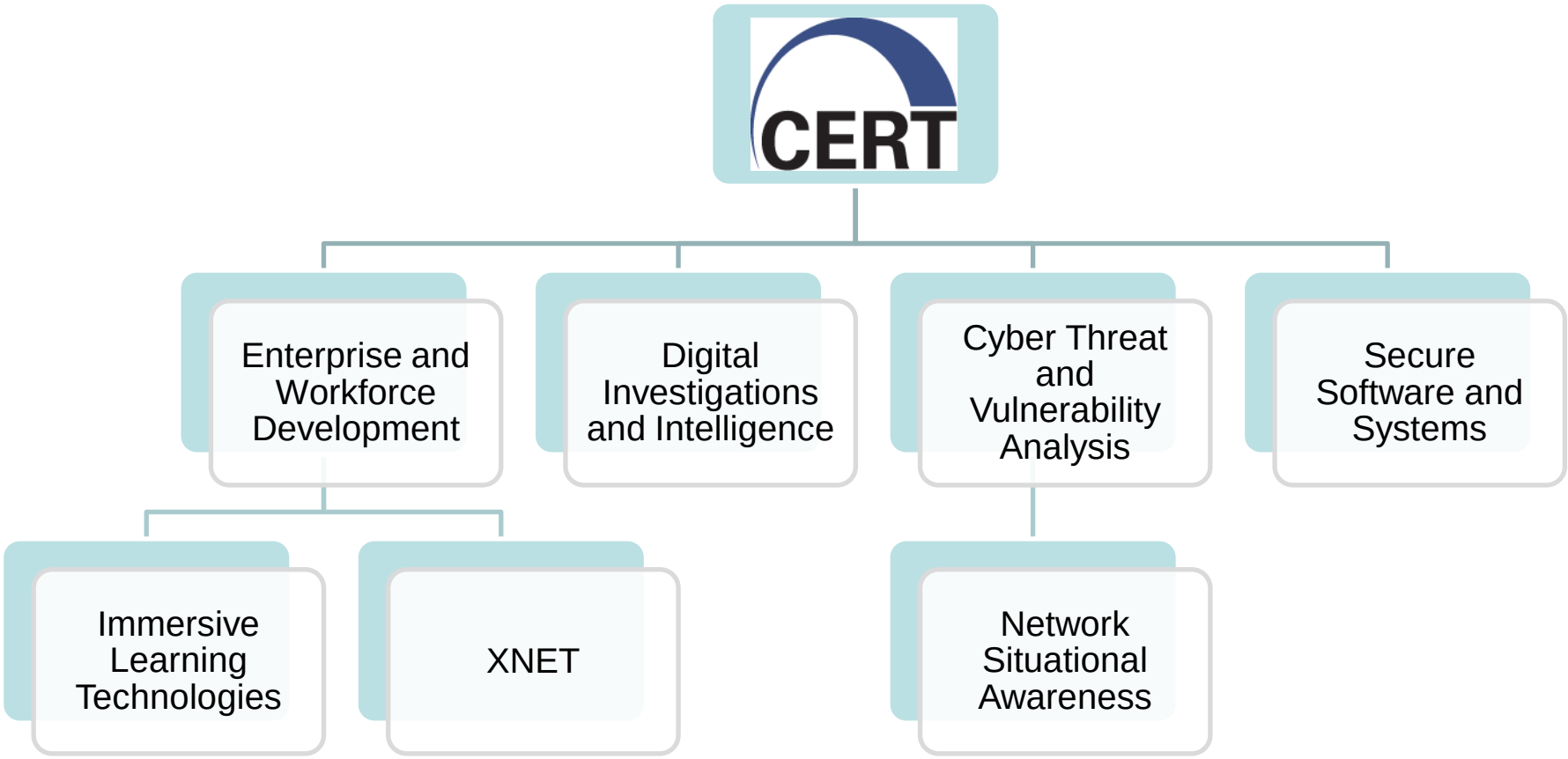
For Training and Simulation

George Warnagiris

Software Engineering Institute



Software Engineering Institute



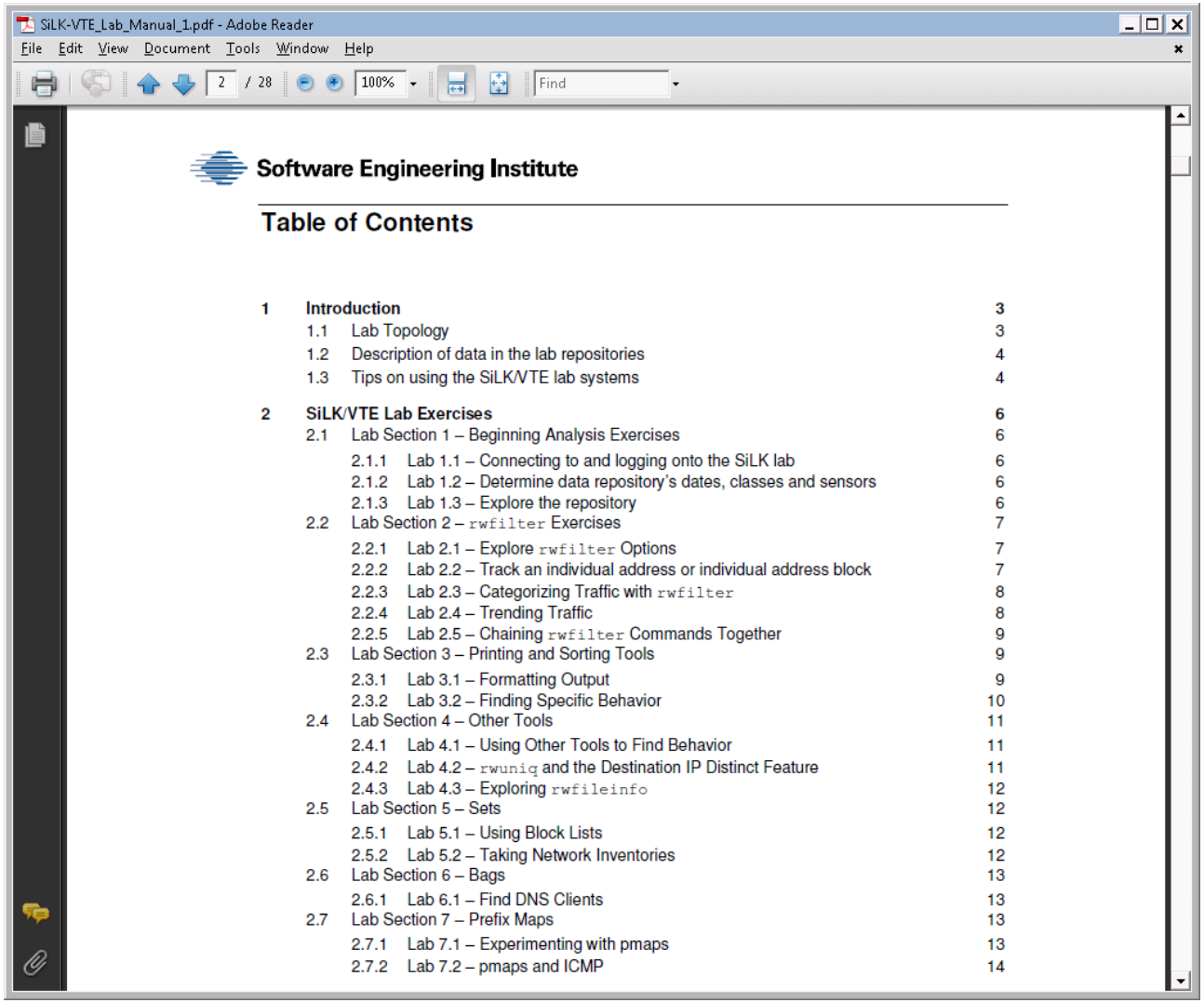
CERT Network Situational Awareness ("NetSA")

- 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

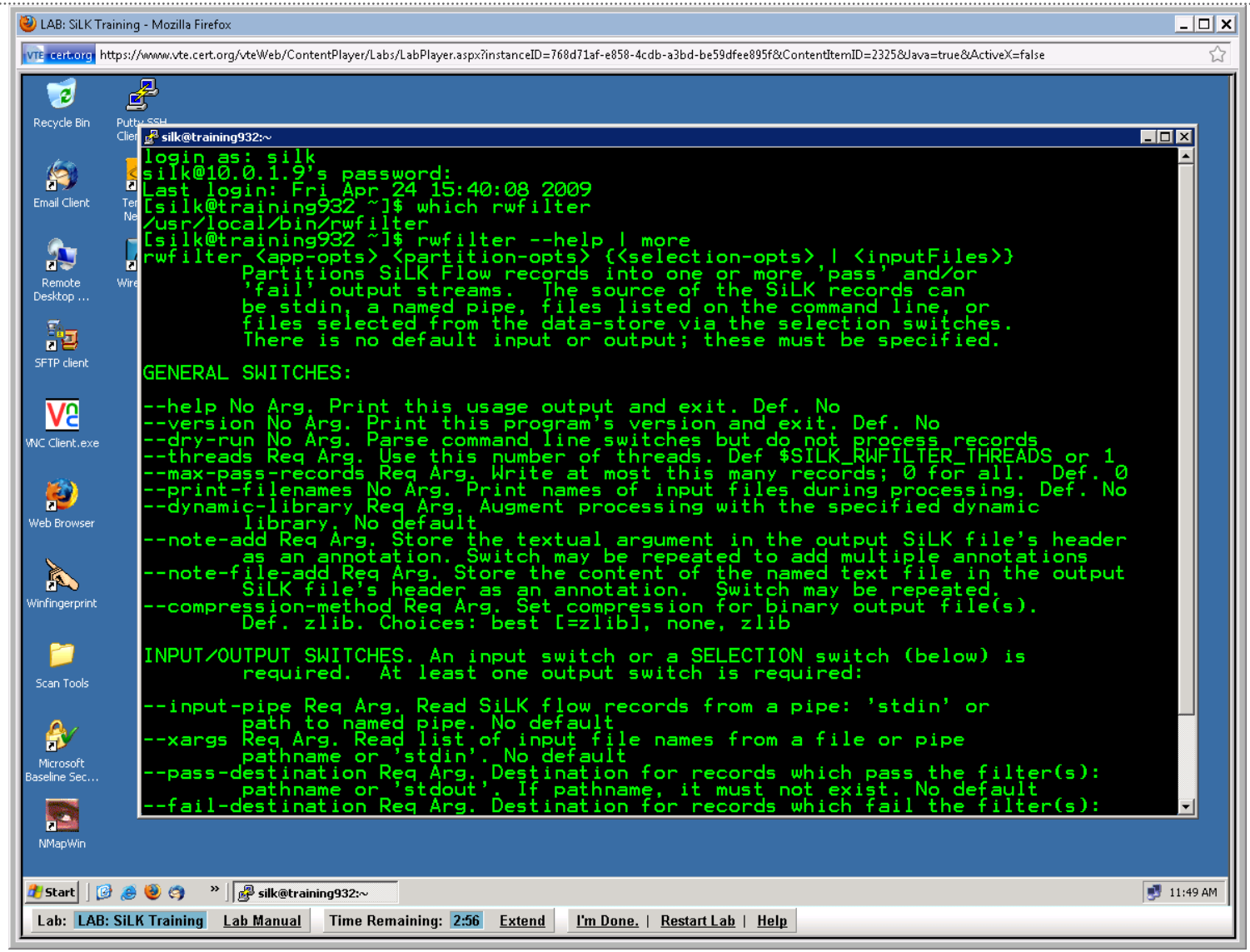
NetSA Online Training Modules

- Network Flow
- SiLK Beginning Flow Analysis
- 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



NetSA Online Virtual Lab



New Training Modules in 2010

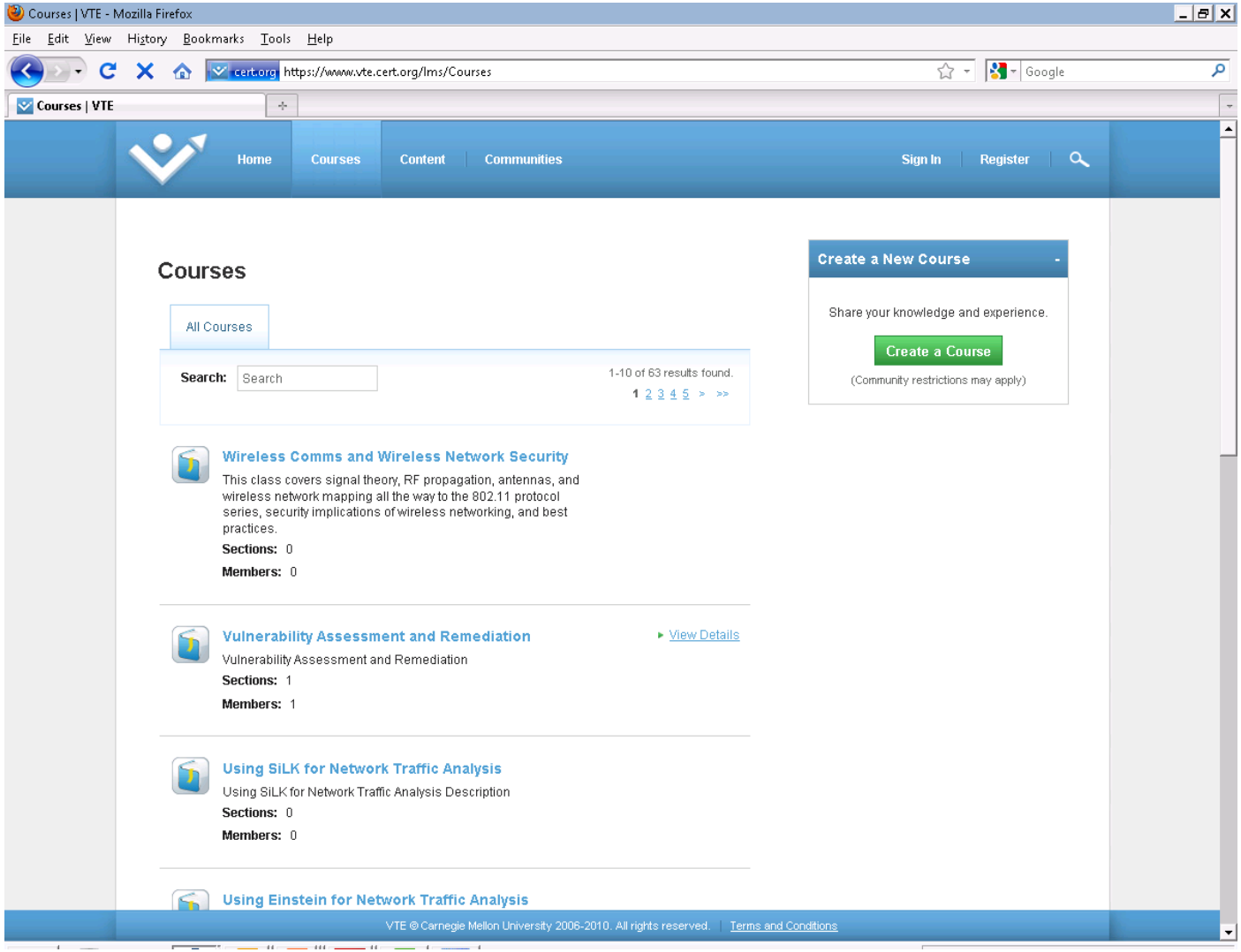
- Introduction to iSiLK
- Overview of PySiLK
- Basic PySiLK Objects

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