ITSEED: Development of Instructional Laboratories for IT Security Education

Xinli Wang, Guy C. Hembroff
Michigan Technological University

Yan Bai
University of Washington Tacoma

Outline

- Motivation
- Lab design
- Lab topics
- Open questions

Security Component Is Needed

- **Security is one of the essential components in an IT curriculum**
  - Meet the needs by industry
  - Protect our valuable data
  - Maintain a working computing environment
- **Hands-on activities are critical in IT education**
  - Gain a better understanding of lecture materials
  - Learn skills useful in work
  - Gain experiences with useful tools

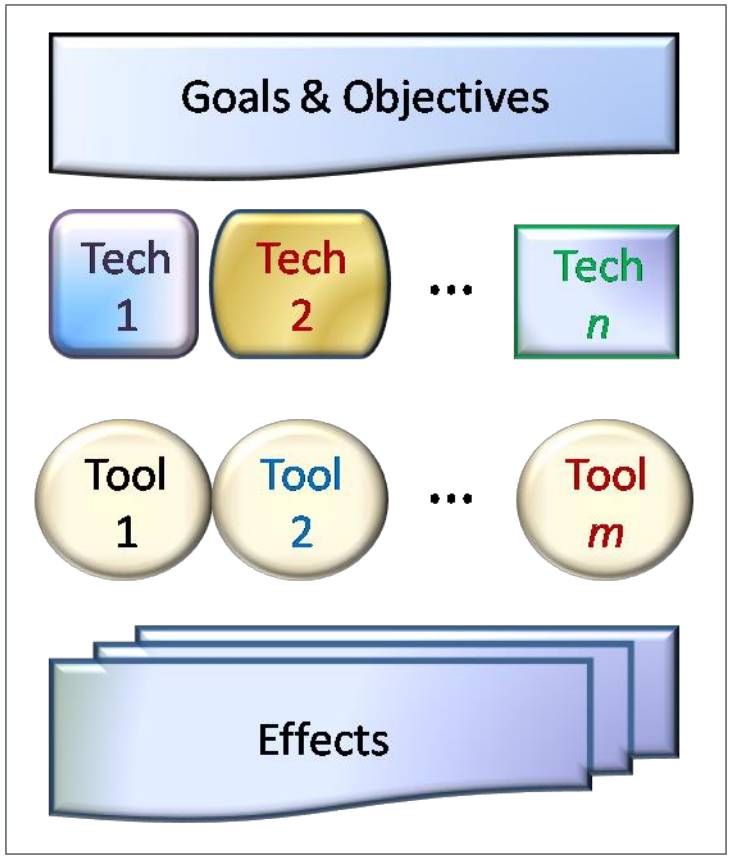
The Challenge

- **Security is new to educators**
  - Faculty from CS or other disciplines of IT
  - No background in security
  - No experience with security
- **Lack of existing materials**
  - Hard to find existing lab assignments
  - Not trivial to learn to use a tool for educational purpose
  - Not trivial to develop and write a lab assignment, more challenging in a tight schedule

Our Objective

- **Develop a collection of instructional laboratories to enhance the security component in IT education**
  - Test the labs in virtual environment
  - Post them on the Web
  - Test bed, guide online

Lab Design


Goals & Objectives
Tech 1
Tech 2
...
Tech n
Tool 1
Tool 2
...
Tool m
Effects

Lab Topics

- **Vulnerability assessment and industrial compliance**
  - Nessus scanner
  - OpenVAS scanner
  - PCI compliance research and OpenVAS PCI Compliance Scanning
- **Security audit**
  - Introduction to syslog
  - Centralized logging with syslog

Lab Topics

- **Common skills for system hardening**
  - Introduction to the principle of system hardening
  - Follow the guidance by NSA and CIS
  - General *vs* function specific hardening
- **Authentication and password management**
  - Password cracker
  - Password management
    - Strong password, rotation, etc.

Lab Topics

- **Network access protection (NAP)**
  - Introduction to NAP
  - DHCP NAP enforcement
- **Encryption**
  - Introduction to OpenSSL encryption libraries
  - Study the effects of different operation modes
    - ECB, CBC, CFB, OFB

Lab Topics

- **X. 509 public-key certificate and PKI**
  - Introduction to OpenSSL PKI libraries
  - Set up private PKI, CA, certificates
- **Firewall**
  - Open BSD package filter
  - Configuration and effect test

Lab Topics

- **IDS**
  - Snort
  - Rules
  - Integration with other components for analysis
- **VPN**
  - Introduction to OpenVPN
  - Configuration and test

Current Progress

- **Lab development**
  - Contents and format have been determined
  - Draft labs have been developed
  - A web page under construction
- **Evaluation**
  - Question set has been determined, for students and faculty
  - Web-based evaluation

Discussion

- **Materials and topics should be covered**
  - What is the basic knowledge to cover?
  - Update the tools used
  - Integrate recent advancement in IT security

Discussion

- **Format to conduct hands-on labs**
  - The step-by-step instructions
  - More challenging components

Discussion

- **The environment to conduct these hands-on activities**
  - Physical environment
  - Virtual environment
    - Virtual box
    - VMware player
    - VMware Work Station
    - VMware vCloud

Discussion

- **Hacking vs. defending**
  - Teach hacking and learn defending?
  - Teach defending by knowing the hacking?

Acknowledgment

- This work is supported by NSF TUES program

Questions?
Comments?