



An Introduction to Teaching & Developing Information Security Curriculum

Module 3 – Designing & Conducting InfoSec Labs

Michael E. Whitman, Ph.D., CISSP

Herbert J. Mattord, CISSP

Kennesaw State University



ABSTRACT

Information Security (InfoSec) is of great interest to many at
Colleges and Universities

Many institutions are creating InfoSec programs that can
benefit from laboratory experiences for students

It is important to plan the facilities and curriculum for InfoSec
labs to optimize:

- Hardware
- Network
- Operating Systems
- Software
- Curriculum Structure
- Curriculum Content
- Student and Lab Management



INTRODUCTION

Many institutions are beginning the task of creating information security programs

Compared to other IT related programs, there are fewer information security programs

Increasing demand from industry for qualified graduates and rising interest of students and faculty are driving adoption of InfoSec Curriculum



INTRODUCTION - 2

Like other IT programs, InfoSec must incorporate laboratory experiences

Training students with skills based on a solid theory is essential

Key topics are network and computer security and vulnerability assessment and system penetration

These skills complete the student's preparation and greatly enhance the value of graduates to employers



LAB DESIGN OPTIONS

Sometimes the lab's physical design is fully defined without the opportunity for redesign

Occasionally circumstances may allow for customization and the lab can be built for InfoSec curriculum

InfoSec labs will often find the student using multiple operating systems, sometimes within the same exercise

InfoSec lab students may perform activities that might place unwanted burdens on the campus network or draw unwanted attention from campus network administrators

Some functions will be dangerous to perform on a network that is not isolated



HARDWARE OPTIONS

- Hardware selection criteria:
 - Budget available for acquisition
 - Flexibility in purchasing
 - Shared use between InfoSec and other specialty topics
 - Campus network requirements and operating procedures
 - Physical plant and floor space nature and availability
 - Nature of interactive learning opportunities planned for the facility
- Approaches:
 - Standard / Small-footprint Desktop Systems
 - Terminal Server Solutions



HARDWARE OPTIONS - 2

- Laboratory Support Servers
 - Sized based on number and nature of clients in use
- Best Practice Recommendations
 - Fairly capable client computers with flexible OS images
 - Three (or more) administration servers to deliver:
 - Image management
 - Virus control
 - Central application and database support where needed
 - Manageable target using a virtual image system



NETWORK OPTIONS

Isolation is required for some InfoSec exercises

Keeping the use of some software tools away from the campus network is advised

It is necessary to maintain connectivity to outside resources

- Options
 - Default Route to Campus
 - Using Network Address Translation



NETWORK OPTIONS - 2

- Equipment
 - Residential
 - Small office/home office (SOHO)
 - Commercial Router/Switch
 - DMZ with Hardware Appliances
- Wiring and Configuration of Internal Lab Subnetworks
 - Home run for each computer to a central hub or switch
 - Clusters of client computer use small (4-8 port) hubs
- Best Practice Recommendations
 - SOHO router for NAT
 - A tier of 8-port true hubs for clusters of 3 to 4 client computers



OPERATING SYSTEM OPTIONS

It is very useful to have multiples operating systems, perhaps multiple configurations of multiple operating systems available to the each student in the lab

- Using Removable/Selectable Drives
- Using Multi-boot Systems
- Using Virtual Images allows students to operate multiple simultaneous different OS images, making them all available to a bridged local network inside the host computer and also to the lab network
 - VMWare (<http://www.vmware.com/>) is a software application that runs in Windows or a Unix variant.
 - Microsoft Virtual PC or VPC (<http://www.microsoft.com/windows/virtualpc/default.msp>) runs on Windows XP Professional
 - Many similarities to VMWare
 - One advantage is availability under the Microsoft Academic Alliance licensing program



OS BEST PRACTICES

Using a stable and consistent lab computer platform such as Windows XP

Locked down from student reconfiguration

Virtual images allow the student to access needed operating systems and even simultaneous execution of different operating systems

Allows unlimited and direct control of virtual images



SOFTWARE OPTIONS

- Categories are:
 - Freeware is software that freely available without licensing costs
 - Be cautious when using freeware, since not all of these applications will have the same degree of quality or reliability
 - It is possible that some freeware may conceal malicious intent
 - Demoware and Shareware are not free since the programs stops working after a trial period, or, the capabilities are limited
 - Demonstration versions of commercial grade software are often available for limited trials
 - Commercial Software
When the budget permits (or the generous vendor donates)
- Best Practice Recommendations
 - When possible use industry-proven commercial software tools
 - Otherwise use the perfectly capable and quite useful freeware and demoware titles



LAB CURRICULUM OPTIONS

- Tutorials
 - A tutorial is a set of step-by step instructions with explanations that are used to give a student some skill in a specific technical area
- Lab Exercise
 - A lab exercise demonstrates the capability of a tool or to shows the results of a sequence of activities
- Demonstration
 - When not practical for each student to perform the tutorial or exercise individually, it is useful to show the student how it is done
- Simulation
 - A simulation uses a software package to permit the student to experience conditions and outcomes that are not practical to implement in the real world



LAB CURRICULUM OPTIONS - 2

- Webinars
 - Many vendors and professional organizations broadcast seminars and training events over the Internet and the sessions may be available for the InfoSec student
- Films and Videos
 - Students appreciate the appropriate use of films and videos in the lab and classroom
- Best Practice Recommendations
 - Use a mixture of each to create the most useful learning environment
 - Some activities are too complex to prepare and deliver in a multi-computer lab and must be shown using demonstration
 - Some other activities are so restrictive (dangerous to the student or the academic institutions IT infrastructure) that they must be shown only through simulation
 - Economic considerations may also introduce limits



LAB CONTENT SOURCING OPTIONS

Labs require content for the learning experience

It is not always practical to create or easy to locate all of the content needed for a lab

Content options:

- Published Sources such as Course Technology and other publishers offer texts and lab support guides
- Web Sources such as NIATEC offer some lab content materials as do several National Security Agency Centers of Academic Excellence in Information Assurance Education
- Creating your own especially for targeted learning objectives and unique aspects of your interests and abilities



Lab Content Best Practices

Pull lab content from any and all sources

- Lots of content exists
- It takes effort by the instructor to locate and configure in lab setting
- Sometimes resources have uneven quality
- Can be a challenges for students of varying abilities



ORGANIZING STUDENTS

- Factors to consider:
 - Limited equipment
 - Varying skill levels of students
 - limits in the number or skill of lab assistants
 - distance learning constraints
 - requirements of other learning objectives (such as writing or teamwork objectives)
- Options to consider:
 - Individual Assignments
 - Ad Hoc Teams
 - Persistent Teams
- Best Practice Recommendations
 - Assign the bulk of the lab tutorials and exercises as individual assignments
 - Some assignments including activities with specialized equipment and project work are done using both ad hoc and persistent teams at the discretion of the instructor



LAB MANAGEMENT

Centrally administered antivirus solution (such as Symantec Norton Antivirus CE)

Image management package (such as Ghost) helps in the lab configuration of client computers

Resetting labs when used for multiple sections of similar courses, there is an issue of system state to consider. Options:

- Removable drives, each class section is assigned to a drive set and remounts the applicable drive set for use in the lab
- Partitioned multiboot drives, multiple versions of the same OS can be built and the image assigned to one of the class sections
- Ghost management of images to reset to a known condition prior to each lab meeting
- Virtual OS images allow each student or class section can be assigned a virtual image
- Instructed Labs vs. Self-paced Labs
 - Some lab assignments are well suited to individual effort
 - Other topics are better handled when the instructor leads the lab in a click-and-check model of instruction
 - Theoretical Preparation should be completed on a specific topic before taking the students into the lab



LAB MANAGEMENT - 2

- Building VA Targets
 - The InfoSec lab assignments that student seem to enjoy the most are vulnerability assessment and penetration testing
 - This activity gives the student the feeling of hacking while minimizing the risk
 - A challenge for the lab instructor is to prepare the targets for these assignments:
 - Avoid using stacks of old computers as targets unless this is the only option
 - Use a reasonably capable server using a virtual OS server (such as VMware or VPC) to bring up your targets on the lab network
- Last-minute Instruction & Errata are continuing challenges for the lab instructor
 - Input parameters, special instructions and errata need to be delivered
 - Use a projector (unless being used for a click-and-check session) to cycle through a set of PowerPoint slides with all input data and any corrections or special instructions needed for the lab



CONCLUSION

- The lab experiences of students are a critical to student success
- Many employers consider some degree of lab or practical experience as necessary
- Frequently, the only place a student will be able to use InfoSec-related applications freely is within the confines of the InfoSec lab
- Planning, building and operating the InfoSec lab is similar to those activities for any IT lab with a few special considerations
- Good planning after considering all of the options will lead to a more successful learning experience



APPENDIX – WEB RESOURCES

URLResources:

- www.cerias.purdue.edu
Research and teaching resources from the CERIAS project at Purdue University
- cistr.nps.navy.mil
Content from the Naval postgraduate School
- www.ee.ryerson.ca:8080/~hhinton/compsec/security.html
A Listing of Computer and Information Security Activities
- niatec.info/curriculum.htm
The National Information Assurance Training and Education Center curriculum page
- www.nsa.gov/ia/academia/caemap.cfm?MenuID=10.1.1.2
Resources from the National Security Agency
- cscr.nist.gov
Vast repository of best practices for the information security practitioners in both government and the private sector
- commonwealthfilms.com/
Commercial provider of training films and videos
- www.pbs.org
Documentary videos in InfoSec topics are available from a number of PBS series.
- infosec.kennesaw.edu
Variety of resources useful to information systems focused InfoSec programs



REFERENCES

- [1] Frank, C., Mason, S., Montante, R., Micco, M. and H. Rossman, "Panel Discussion: Laboratories for A Computer Security Course," <pub> (2002)
- [2] Hill, J. , Carver, C. , Humphries, J. and Pooch,U., "Using an Isolated Network Laboratory to Teach Advanced Newtworks and Security", <pub> (2001)
- [3] Huss, J. , "Laboratory Projects for Promoting Hands-On Learning in a Computer Security Course," ACM SIGCSE Bulletin, (27) (June 1995) pp 2-6
- [4] Tikekar, R. and Bacon, T. "The Challenges of Designing Lab Exercises for A Curriculum in Computer Security," <pub> (2003)
- [5]Wagner, P. and Wudi, J., "Designing and Implementing a Cyberwar Laboratory Exercise for a Computer Security Course," Proceedings of the 35th SIGCSE technical symposium on Computer Science education, (2004) pp. 402-406
- [6]National Information Assurance Training and Education Center Curriculum Page, Retrieved July 5, 2004 from <http://niatec.info/curriculum.htm>