

Open Source Security Tools for Information Technology Professionals

**CUNY SPS
Course Syllabus**

**Aron Trauring
May 23, 2005**
(rev October 21, 2005)

Course Description

Information security is a top priority for information technology professionals and their employers. A bewildering number of security tools are available in the market, many costing thousands of dollars. Yet few system administrators have sufficient time or resources to properly address potential security problems. One option is to use “open source” software, where the code used to create the software is available for public use. Open source products are often at low cost and of high-quality, but few IT professionals have the expertise or time to evaluate these alternatives.

This new course is a practical, hands-on introduction to the topics of open source software and computer security, and several specific open source security tools. While most of the tools run on Linux or other Unix platforms, they address security issues in, and solutions for, Microsoft Windows-based networks as well.

The course will be a combination of lectures and labs, which will provide students a hands-on opportunity to use and apply these tools. Through using these tools, students will learn about core security threats in the modern IT networked environment and how to handle them. While addressing security issues for all major IT platforms, the students will also learn some basic skills for using the most famous open source product, the Linux operating system.

Required Text

Howlett, Tony *Open Source Security Tools: A Practical Guide to Security Applications*. New York: Prentice Hall. 2005

Optional Texts and Labs

Instructor chosen material on the O'Reilly's online Safari University (online text resource center)

Labs: Linux personal computer and network servers.

Course Expectations/Grading Rubric

- 1) Students must attend all classes. More than one absence will affect the grade and a student with more than two absences will be dropped from the course. Two late arrivals will be considered one absence.
- 2) Students must actively participate in all class sessions.
- 3) Students must complete all class labs.
- 4) Students must prepare an electronic notebook which includes topical articles about computer security issues found in the trade press during the period the course is offered. An introductory essay must relate the articles to the topics

- covered in the course, including suggestions on how the tools we learn may be used to address some of the issues raised in the articles.
- 5) Students must complete weekly quizzes that cover cumulative material and a final exam.
 - 6) Grading:
 - Class Labs – 20%
 - Electronic notebook – 20%
 - Class Participation – 10%
 - Weekly Quizzes – 30%
 - Final examination – 20%

Competencies that Students will Develop in the Course

Overarching Objectives:

At the conclusion of the course, the student will be able to

- 1) Identify fundamental network computer security issues.
- 2) Understand what open source software is and when it is advantageous to use for network security applications.
- 3) Understand how to apply specific open source tools to uncover security breaches.
- 4) Deploy specific tools to monitor and protect a computer network against attack.

Content-specific objectives:

At the conclusion of the course, the student will be able to

- 1) Harden their security tool system
- 2) Deploy secure remote administration tools
- 3) Deploy firewalls
- 4) Use a port scanner and analyze its results
- 5) Use a vulnerability scanner and analyze its results
- 6) Use a network sniffer and analyze its results
- 7) Deploy and use intrusion detection systems
- 8) Make use of security analysis and management tools
- 9) Deploy and use encryption tools
- 10) Deploy and use forensic tools

Strands

Laboratory Technology: In each lesson, there will be extensive use of individual computers to install, deploy, and activate specific security applications.

Theoretical Underpinnings: Each lesson will examine the underlying computer network technology's theory and practice of the tools used in the labs, as well as of the specific network security threats these tools address.

Problem Solving: Built into each lesson, there will be opportunities for students to learn and apply general problem solving techniques to common network administration issues.

Online Resources: In each lesson, students will be provided relevant online resources and have the opportunity to explore and make use of these.

In addition to these strands that are contained in every lesson, there will be many different strategies employed in the classroom setting, including group and individual work, teacher lectures, questions and answers, teacher demonstrations, student discussions, active learning and note taking.

Course Outline

Session I - Introductory FOSS

Welcome

Overview of course

Introduction to Free and Open Source Software (FOSS)

Introduction to GNU/Linux

Session II - Introductory TCP/IP / Security

Overview of TCP/IP network principles

Introduction to information security

Lab: Linux Principles and Networking Overview, ping, traceroute, whois, dig, finger, ps

Session III - Hardening the Security Tool System

Trusted Computing Base

Installing the GNU/Linux distribution securely

Secure booting and boot loaders

Consoles

Users and Groups

Process accounting

PAM

Keeping informed about security

Lab: TCB

Session IV - Secure Connections and Remote Administration

Symmetric and asymmetric encryption

SSH

VNC

Lab: OpenSSH, VNC

Session V/VI - Firewalls

How Does a Firewall work?

Adding rules
Choosing filtering criteria
iptables
Creating a basic firewall
Advanced concepts
Lab: iptables, SmoothWall

Session VII - Port Scanners

TCP/UDP ports
TCP fingerprinting
How port scanning works
Port scanning configuration
Port Scanning Techniques
Lab: Nmap, Nlog

Session VIII - Vulnerability Scanners

Typical application-level vulnerabilities
Vulnerability scanning setup and configuration
How to do safe and ethical vulnerability scanning
Sample scan configurations
What vulnerability scanning doesn't do
Lab: Nessus

Session IX - Network Sniffers

Network sniffer fundamentals
Ethernet history and operation
How to do safe and ethical network sniffing
Sample sniffer configurations
Network sniffer applications
Lab: TcpDump, Ethereal

Session X - Intrusion Detection Systems

Types of intrusion detection systems
Signatures for network intrusion detection systems
False positives in network intrusion detection systems
Proper intrusion detection system placement
Tuning an intrusion detection system
File integrity checking
Lab: Snort, Tripwire

Session XI - Analysis and Management Tools

Managing server log files
Using databases and web servers for security data
Analyzing IDS data

Managing vulnerability scan data
Running a vulnerability scan management system
Lab: ACID, NPI, NCC

Session XII - Encryption Tools

Different encryption algorithms
Encryption applications
Certificate authority security model
Web of trust security model
Lab: PGP, GnuPG, Certificates

Session XIII - Forensic Tools

Uses for forensic tools
Incident response concepts
Preparing for forensic investigation
Tenets of good forensic investigation
Lab: Sleuth Kit, Autopsy Forensic Browser, The Forensic Toolkit