

Open Source Security Tools for Information Technology Professionals

School of Professional Studies (SPS)

The City University of New York (CUNY)

Aron Trauring
Adjunct Professor
CEO, Zoteca

Class 1 September 12th, 2005

Class Agenda

6:30-6:45 Class Introductions

6:45-7:00 What this Course Is About (Presentation)

7:00-8:15 FOSS and the Community Development Model (Presentation)

8:15-8:30 Break

8:30-9:15 Lab: Introduction to Linux Principles and Networking Overview (Lab)

9:15-9:30 FourM website

Assignments

Instructor

Aron Trauring – Adjunct Professor, CUNY SPS / CEO, Zoteca

Email: atrauring@zoteca.com

Personal Website: <http://aronst.org/>

Zoteca Corporate Website: <http://www.zoteca.com/>

FOSS Resources: <http://www.fourm.info/>

What This Course Is

What This Course Is Not

- Advanced course in networking
- Advanced course in security
- Certification Prep

Protecting our organization matters

- Saves Time
- Save Money
- Save Lives

Course Biases

- Triage — protection commensurate with threat
- Security is an inconvenience
- SysAdmins serve the customers — not “LUs3rs”
- Security from a SysAdmin perspective

Course Outline

Session I — Introductory and FOSS

- Welcome
- Overview of course
- Introduction to Free and Open Source Software (FOSS)
- Lab: Introduction to Linux Principles and Networking Overview
- Keeping informed about security

Session II — Introduction to Network and Security

- Introduction to the Internet / TCP/IP Infrastructure
- Internet Lab
- Introduction to Information Security

Session III — Hardening

- Assessment Exercise
- Trusted Computing Base
- Lab: Bastille Linux and Basic Network tools

Session IV — Secure Connections and Remote Administration

- Encryption Protocols
- SSH
- VPN
- Lab: OpenSSH, FreeS/Wan

Session V — Firewalls

- How Does a Firewall work?
- Adding rules
- Choosing filtering criteria
- iptables
- Creating a basic firewall
- Advanced concepts
- Lab: iptables, SmoothWall

Session VI - Port Scanners

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

Session VII - 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 VIII - 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 IX - 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 X - 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 systemLab: ACID, NPI, NCC

Session XI - Encryption Tools

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

Session XII - Wireless Tools

- Wireless LAN concepts
- 802.11 protocols
- Weaknesses of wireless LANs
- Wireless assessment equipment
- Lab: NetStumbler, Kismet, AirSnort

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

Bibliography

Required Text:

Open Source Security Tools: A Practical Guide to Security Applications by Tony Howlett (ISBN: 0-321-19443)

Core Curriculum Texts:

Network Security Hacks: 100 Industrial-Strength Tips & Tools by Andrew Lockhart (ISBN: 0-596-00643-8)

Hardening Linux by James Turnball (ISBN: 1-59059-444-4)

Computer Security Fundamentals by Chuck Easttom (ISBN: 0-13-171129-6)

Other Useful Books:

Linux in a Nutshell: A Desktop Quick Reference by Ellen Siever, Stephen Figgins & Aaron Weber (ISBN: 0-596-00482-6)

Security Warrior by Cyrus Peikari & Anton Chuvakin (ISBN: 0-596-00545-8)

FOSS and the Community Development Model

Richard Stallman and the GNU Project

- September 27, 1983 — Richard Stallman sends out the initial announcement (<http://www.gnu.org/gnu/initial-announcement.html>)
- Calls for the creation of a totally free Unix-compatible operating system
- GNU is Not Unix

Four Characteristics of Free Software

1. The freedom to run the program, for any purpose
2. The freedom to modify the program to suit your needs
3. The freedom to redistribute copies, either gratis or for a fee
4. The freedom to distribute modified versions of the program, so that the community can benefit from your improvements.

CopyLeft — the GNU General Public License (GPL)

- Structured in a way to guarantee the four freedoms
- GNU Project Website *<http://www.gnu.org/gnu/the-gnu-project.html>
- Can distribute or modify but must distribute source code along with the binary
- LGPL — to allow linking of non-free software to free libraries

Eight Years in Wilderness

- undeterred by the financial and technical difficulties he faced over the years
- created a large infrastructure of compilers, editors, and utilities
- History of the project *<http://www.gnu.org/gnu/the-gnu-project.html>

Why Free Software Matters

- Software technology is the basis of information exchange in modern society
- Free exchange of information is a fundamental right and the basis of democracy
- Essential that software be free and unencumbered as well.
- Software be “free as in speech”
- GNU/Linux *<http://www.gnu.org/gnu/gnu-linux-faq.html>
- Free Philosophy *<http://www.gnu.org/philosophy/why-free.html>
- Digital Millennium Digital Act (DMCA) — Diebold case
- Without free software, corporations could build mechanisms into software to restrict dissemination of information
- Right to read story *<http://www.gnu.org/philosophy/right-to-read.html>

Linus Torvalds and Linux

- 1991 — Linus Torvalds second year student of Computer Science at the University of Helsinki
- Looking for something more sophisticated and useful than DOS for his 386/486 PC. Specifically, he w
- Wanted a Unix clone — begins work in April, 1991
- August 21, 1991 — Torvalds posted an announcement in a news group about his project, asking for help
- September 1991, version 0.1 of what was to become Linux was released to the world

Torvalds Two Critical Choices

- To build Linux on top of Stallman's GNU infrastructure
- To adopt the copyleft GNU GPL for the Linux software license

GPL Encourages Sharing

- Free software as development method.
- Sharing and mutual co-operation
- GPL guarantees that no one party can benefit from the sharing at the expense of others
- Whatever anyone contributes is shared equally by everyone
- No one can exploit your work at your expense
- You equally benefit from the work of others.

Contributing Factors to Linux Success

- Explosive growth of the Internet made collaboration easier
- Unix OS TCP/IP native so natural platform for Internet

Open Source and the Corporate World

- Advocates with a more pragmatic perspective than Stallman
- Open Source Initiative <http://www.opensource.org/>

The Pragmatic Freedoms

- “Free as in Beer” — economic benefit
- “Free as in Exchange of Ideas” — secure and robust
- “Free as in Market” — no vendor lock-in

Other benefits

- Customer-centric rather than marketing-centric
- Open standards mean you own your own data

FOSS Economic Model

- If developer X devotes 5 days a month to developing FOSS
- Lost \$5,000 of opportunity cost in consulting work or salary
- 20 other developers are doing the same
- Software now worth \$100,000 — 20x ROI

What about the Free Rider?

- A rational economic model requires that one only calculate the benefit to oneself
- Find bugs and test the software in varied environments — contribute to security and robustness
- Network effect - bring in new “investors”

The Linux Bandwagon

- IBM leader of the pack
- The GNU/Linux ecosystem

FOSS Field Guide

- FOSS Field Guide http://www.fourm.info/Tools/Tools_Item.2004-03-22.2637
- Infoworld Field Guide <http://www.infoworld.com/reports/32SRoss.html>

Lab: Introduction to Linux Principles

Distributions

- Alternatives
- Packaging
- Live CD
- Debian
- Red Hat
- Novell SUSE

Shell Basics

- Command — `command [-options] [--full-options] [parameters]`
- Help — `man`, `man -k`
- Redirection
- Filesystem

Filesystem Basics

- Devices vs. filesystem tree
- Hierarchies — Shareable vs. Non-Shareable, Static vs. Variable
- Pathnames
- Shortcuts — `~` `.` `..`
- Command completion
- Hidden Files
- Metacharacters

Filesystem Commands

- Navigation — `cd`
- Display — `pwd` `ls`
- Creation — `touch` `mkdir`
- Manipulation — `cp` `mv` `rm` `rmdir` `mc`
- Find — `locate` `grep` `find`

Filesystem Permissions

- Users and Groups
- RWX
- ACL

Permission Commands

- chown chgrp
- chmod
- umask

Editing

- mcedit
- vi

Root

- su
- sudo

Tour of the GUI

Assignments

1. Live CD - play around with Linux
2. Security article of the week