

# **Introduction**

# **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

## 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

- Welcome
- Overview of course
- Introduction to Free and Open Source Software (FOSS)
- Introduction to the Internet / TCP/IP Infrastructure
- Lab: Introduction to Linux Principles and Networking Overview

## Session II - Hardening the Security Tool System

- Introduction to Information Security
- Trusted Computing Base
- Lab: Bastille Linux and Basic Network tools
- Keeping informed about security

## Session III - Firewalls

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

## Session IV - Port Scanners

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

## Session V - 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 VI - 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 VII - 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 VIII - 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 IX - 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 X - Secure Connections and Remote Administration

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

## Session XI - Wireless Tools

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

## Session XII - 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

## Session XIII - Securing Email

- Mail server options
- Protecting mail servers
- securing SMTP server
- Relaying, Spam and Viruses
- Authenticating email
- Lab: Postfix, Cyrus, Spamassassin, Amavis