

# 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 3 September 26th, 2005

# Class Agenda

**6:30-6:45** Article of the Week

**6:45-7:15** Internet review

**7:15-7:45** Security Review and Completion

**7:45-8:00** Break

**8:00-8:30** Assessment Exercise

**8:30-9:00** Hardening/Trusted Computer Base

**9:00-9:30** Hardening Linux Lab

## Instructor

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

**Email:** [atrauring@zoteca.com](mailto:atrauring@zoteca.com)

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

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

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

## Review — Network Basics

### Internet Protocol

- Logical address — no IP, no network communication
- IPv4 — 32 bits long: four octets of eight bits each — 4,294,967,296 addresses.
- Structured — A,B,C Networks
- Network — 192.168.1.0 (Subnet Mask 255.255.255.0)
- Individual computer — 192.168.1.45
- Private versus Public Addresses
- NAT — Network Address Translation
- DHCP — Dynamic assignment of IP
- IPv6 — 128 bits — Structured (64 bits = physical layer address)

### Basic IP Routing

- Routers — move traffic from one part of network to another (standardize on IP address)
- Bridge — links LANs
- Repeaters — boosts signals
- Gateway — links LANs to mid-level networks, or between larger networks
- Mid-level networks — WAN (one organization), ISP, regional networks
- NAP — Network Access Point — link to main backbones (155 megabits/second)
- Internet2 Backbones — 9.6 billion bits/second

### IP Network Class

- A — 1-126 — supports 16 million hosts on each of 126 networks
- 127 — localhost
- B — 128-191 — supports 65,000 hosts on each of 16,000 networks
- C — 192-223 — supports 254 hosts on each of 2 million networks
- D — 224-247 (Multicasting)
- E — 248-254 (Experimental)

## Classless Inter-Domain Routing (CIDR)

- A replacement for the old process of assigning Class A, B and C addresses with a generalized network "prefix".
- Old system: network identifiers (or "prefixes") of 8, 16 or 24 bits
- CIDR: prefixes anywhere from 13 to 27 bits
- Blocks of addresses can be assigned to networks as small as 32 hosts or to those with over 500,000 hosts
- 32-bit IP address plus how many bits are used for the network prefix. For example, in the
- CIDR address 206.13.01.48/25, the "/25" indicates the first 25 bits are used to identify the unique network leaving the remaining bits to identify the specific host.

## IP Addresses

- 127.0.0.1 — “me, myself” — never leaves computer
- 192.168.1.124 — local network
- 64.110.168.5 — standard address
- DNS — mapping between IP number and name

## Domain Names

- TLD — Top Level Domains
- Zones
- Arbitrary number of sub-levels

## Transport

- Moving Packets
- Data broken up into parts which include data and “headers”
- Routers move data from client to server and back
- Look at headers and determine most efficient route
- Sometime stay within own network
- Otherwise move through a gateway
- Reassembled at other end
- TCP — with acknowledgment
- UDP — where speed is more important

**Application**

- IP address + Port
- Each application has its own standard port
- Web — 80
- SSH — 22
- SMTP — 25
- Client-Server Model

## Review — Information Security

### Main Concepts

- Vulnerability
- Threat
- Risk
- Exposure
- Safeguard (Countermeasure)
- The CIA Triad
- Organizational Security Model
- Risk Management

## Intro to IS — Conclusion

### Basic Security Tenets

- Minimalism
- Defense in Depth
- Vigilance

### Minimalism (KISS)

- Safest way to avoid risk is not to introduce it in first place
- Only install what you need
- Only run what you need
- Do not have users you don't need
- Change control system or journal changes

### Defense in Depth

- Multi-layered approach to defense
- Example: external firewall, host firewall, IDS, regular penetration testing

### Vigilance

- Bit-rot — situation deteriorates if you do nothing
- System changes and threats change
- Check logs, audit users and groups, monitor files
- Keep patches up-to-date
- Test constantly
- Keep on your reading

**Summary**

- Security is expensive and time-consuming
- Constantly measure risk vs. reward
- Tools are needed both for testing and safeguarding
- FOSS lowers the costs of tools Trusted Computer Base

## **Assessment Exercise [Based on Chuck Easttom *Computer Security Fundamentals*]**

1. A simple metric for risk assessment is the following.

**Step 1** On a scale of 1 to 10 rate two areas of your system: *profile* and *value*. *Profile* means how important you are and therefore how likely crackers are to want to attack you. *Value* means how costly a security breach would be. 10 is high end of scale.

**Step 2** Add the two numbers from above.

**Step 3** On a scale of 1 to 10 rate current security, 10 being excellent, 1 being non-existent.

**Step 4** Subtract the second number from the first. -8 being lowest possible 19 being highest. Low numbers are better.

2. Break up into groups. Describe your current situation to your fellow group members and have them rate you using the above metric. Take 5 minutes per person to go through exercise.

3. Present to class.

# Hardening

## Trusted Computer Base

- Need a base computer to run security tools
- Heart of the security operation must itself be as secure as possible
- Entire list of elements that provide security: OS, programs, hardware, physical protection, procedures
- Critical that the OS, which underlies everything, be totally secure

## Problem

- Modern OSES violate the minimalist principle in the extreme
- Operating systems are extremely complex and getting more so
- Tons of other software installed on top of the OS
- Vendors tendency to make things “easy to use”
- Standard installations add to much software and services

## TCB Dangers

- Vulnerable to attack by intruders who e.g. can shut off your IDS
- Intruders can alter data to deceive you into feeling secure
- Commandeered security box makes intruders’ job easier
- Ensuring your base system is secure is the first task of security administration

## Why GNU/Linux?

- Unix modularity — minimalist principle
- Unix layered approach to security — defense in depth
- FOSS review — vigilance

## TCSEC standard (“Orange Book”)

- TCSEC is the Trusted Computer System Evaluation Criteria (“Orange Book”) for single computer systems with terminal access
- first standard definition of a trusted computer system and how to evaluate and ensure them (original spec Aug 83, revised Dec 85)
- National Computer Security Center (NCSC) of the National Security Agency (NSA)
- Must have an explicit, enforced security policy
- Access to information must be controlled by rights of subjects vs class of information
- Audit trails must be kept
- System must contain mechanisms which can be independently evaluated to provide sufficient assurance that they enforce the stated requirements

### **TCSEC Rainbow Series**

- “Red Book” — Trusted Network Interpretation
- “Yellow Book” — Methodology for Security Risk Assessment
- “Lavendar Book” — Database Security Evaluation

### **Evaluation Criteria Classes**

- D — Minimal Protection
- C1 — Discretionary Security Protection
- C2 — Controlled Access Protection
- B1 — Labelled Security Protection
- B2 — Structured Protection
- B3 — Security Domains
- A1 — Verified Design

### **Other Government Baselines and Standards**

- Information Technology Security Evaluation Criteria (ITSEC) is the harmonized European trusted evaluation standard
- Common Criteria is being developed as an ISO standard (JTC1.SC27), based on existing TCSEC, ITSEC, CTCPEC (Canadian), Federal (US) standards

### **Minimalism and Hardening**

- Only what is needed should be made available.
- Only permit access to what you really need.
- Unless explicitly permitted, access is strictly forbidden.
- Hardening means applying minimalist principles to your system.

### **Linux Options**

- Bastille Linux
- grsecurity — kernel modifications and patches
- LIDS — Linux Intrusion Defense System
- RSBAC — full-featured kernel security tool-kit
- SELinux — NSA initiative
- CIS Guidelines/Scoring Tools <http://cisecurity.org/> — for all OSes

**General Hardening Tasks**

1. Disable or remove all unneeded services
2. Run latest version of services that are required
3. Disable or remove all unused user accounts
4. Keep up-to-date with security patches
5. Check and maintain system logs
6. Restrict access to special services (e.g. cron) to root
7. Review and fix file permissions on critical system files
8. Review and fix general system file permissions (e.g. no world write)
9. Remove development tools if you can
10. Limit the number of daemon processes permitted
11. Run local firewalls and not just perimeter firewalls
12. Run a system hardening script
13. Use sudo

**Securing Network Services**

1. Only use the secure version of a service (SSH, SFTP)
2. Disable insecure protocols (r\*, FTP, Telenet)
3. Prevent service processes from having access to data they don't need through virtualization
4. Specify logging and access control for all services giving them only the minimal rights necessary
5. Services should have special users and not run as root (if possible)
6. Drop packets at the router firewall so they never reach server (prevent DoS)
7. Harden network infrastructure
8. Address wireless issues

# Hardening Linux Lab

## Update Options

- apt-get update / apt-get upgrade — CLI
- System -> Administration -> Update Manager (just patches)
- System -> Administration -> Synaptic Package Manager (updates and additions)
- Repositories
- Places where packages are stored on the Internet

## Synaptic Update/Upgrade

- Reload
- Mark All Upgrades
- Apply
- Choose “smart upgrade”

## Ubuntu Components

- Main — free software supported by Ubuntu distribution
- Restricted — non-free software essential to Ubuntu (e.g. binary hardware drivers)
- Universe — free software from rest of Debian; no guarantees of security updates
- Multiverse — non-free software with no guarantees at all

## Ubuntu two versions — stable and development

- Hoary Hedgehog — current stable
- Breezy Badger – current development (Oct release)
- 6 month or so increments

## Changing Repositories, Versions, Components

- “sudo gedit /etc/apt/sources.list” and remove comments on universe and comment CD
- Choose Settings -> Repositories
- Don’t forget to reload (apt-get update)
- Can’t run Synaptic and/or Update and/or apt simultaneously

## Create root password

- “sudo passwd root”

## Webmin

- Add: webmin, webmin-core, webmin-cpan, webmin-status, webmin-xinetd
- Start up Firefox
- `https://localhost:10000/`
- Login as root (never save password)

## Hardening Webmin

- Ubuntu automatically sets it up as
- http secure SSL
- Only localhost, and with n
- New certificate (not necessarily so for other distributions)
- Only one user (root)

## Users

### Xinetd

- More secure version of inetd
- Internet daemons
- Basic internet services
- Xinetd allows you to restrict access / number of connections / number of processes
- Nothing turned on by default
- Ubuntu doesn't even install by default

## System Logs

### Cron

- Disable to other than root

## Bootup and Shutdown

- What processes get started at boot

## Running Processes

- More detail than ps or top
- Since on web need to refresh manually

**Filesystem Permissions**

- “ls -al /”
- “ls -al /etc”

**Bastille Linux**

- Jay Beale
- Install