

# **Hardening Exercise**

## **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

# 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