

# Linux Server Security

Fernando Duran  
CTO WaterlooSecurity Inc.

[www.fduan.com](http://www.fduan.com)  
[www.watsec.com](http://www.watsec.com)

# Internet Server Security Plan

## 1. Risk analysis

1. Legal, cost of the asset, time to recover
2. What are the most likely threats
3. Consider outsourcing

## 2. Recovery plan (backups, fail-over, VMs)

## 3. Patch management (software updates)

## 4. (strong or no) Password, access management

## 5. Detection & monitoring plan

# Information Security is about Risk Management



Risk  $\sim$  Asset Value x Threats x Vulnerabilities - Countermeasures

# Handling Risk

- Risk Transfer
  - Outsourcing (ex mail, web)
  - Insurance
- Risk Avoidance (we won't use x)
- Risk Mitigation
- Risk Acceptance

# Risk Mitigation

- Protection

- Minimize exposed services, use secure versions
- Strong passwords, no exposed Control Panels
- Updated Software

- Detection

- Logs, IDS, monitoring tools

- Recovery

- Good backups are: automatic, comprehensive, off-site, tested, duplicated

- VMs

# Random IT Security Slide

- CIA Triad: Confidentiality, Integrity, Availability
- Security vs. Convenience (or vs. Time & Money)
- Data classification: secret, confidential, public
- Data at rest (gpg) and data in motion (SSL)
- Laws (PIPEDA, PCI), Get-out-of-jail card.

# C, I, A: which is most important?

- Web server with blog making \$ Google ads
- Web server with security company's site
- Web server processing customer's credit cards
- Asterix (VoIP) server
- Mail server
- Server acting as firewall/gateway/VPN
- Military server - "wikileaks"

# Most Likely Security Issues

## Ex: Web Server

1. Brute-force scanner guessing user password
2. Human error or physical problem (HD fails, natural disaster etc) with data loss
3. Vulnerability in out-of-date software
4. (distributed) Denial of service DoS, DdoS
5. Intruder defacing web site
6. Intruder changing critical system files

# I'm supposed to talk about Linux at some point: Apps

- Install Apps: repository (apt/yum) vs compiling
- Update automatically with cron script
- Subscribe to application security bulletin
- What's exposed: netstat -tlnpu, nmap, lsof
- Vulnerabilities: highly related to patch management. Scanners: nessus, many others.

# Backups & Recovery

- Backups (too many options)
  - rsync over ssh
  - db replication
- Should we trust dropbox (amazon etc)?
- Pre-encrypted backup in the cloud
  - spideroak.com, wuala.com
- Virtual Machines: Xen, VMware (VirtualBox)...

# Firewall (iptables)

- Almost useless if you are just blocking unused ports
- IP source blacklisting (see also [maxmind.com](http://maxmind.com) , OS version too) for too many login failures (fail2ban) or DoS
- DoS mitigation with max number connections

# Detection I

- Inside monitoring tools
  - Monit (alerts, restarts...) with respawn
  - Munin, 'quick look' etc, mrt type graphing tool
  - Bash scripts, ex: <http://pastebin.com/SqhT6zFr>
  - Host IDS (change): Tripwire (AIDE etc)
  - Network IDS: snort (usually not practical)

# Detection II

- (free) Outside monitoring tools
  - Uptime: [mon.itor.us](http://mon.itor.us), [wasitup.com](http://wasitup.com), [pingdom.com](http://pingdom.com)
  - Uptime (another server): [nagios](http://nagios), [monit](http://monit)
  - Web change: [versionista.com](http://versionista.com), [changedetection.com](http://changedetection.com)
  - Google Analytics alerts for low, high traffic

# Detection III

- Rootkit detection (limited value)
  - chkrootkit
  - rkhunter
  - See for example: <http://pastebin.com/nEZE4esQ>

# Internet Server Security Plan

## 1. Risk analysis

1. Legal, cost of the asset, time to recover
2. What are the most likely threats
3. Consider outsourcing

## 2. Recovery plan (backups, fail-over, VMs)

## 3. Patch management (software updates)

## 4. (strong or no) Password, access management

## 5. Detection & monitoring plan