

Unix System Administration

Chris Schenk

Lecture 21 – Thursday Apr 05

CSCI 4113, Spring 2007

Logistics

- Avenade talk NEXT Tuesday after class in ECCR 155
 - April 10th
- Lab07 is out, Postfix and Dovecot with SASL
 - And a hint-'o-Perl
- DNS Delegation

.forward Files

- Users can forward mail to another location
 - .forward behaves similarly to alias files
- File exists in user's home directory
 - Permissions must be only readable and writable by owner!
- Can cause mail loops if not carefully managed
 - Internal alias loops are handled by servers, not forwarding loops
- **Syntax:** `\schenk , " | /usr/bin/vacation -f vacation.msg"`
 - The preceding `\` says force delivery of mail without forwarding

Postfix

- A much easier alternative to sendmail
 - <http://www.postfix.org>
 - Or so I tell myself, I've only used Postfix
- One main config file `/etc/postfix/main.cf`
- Important config lines:
 - `mydestination` – for whom I handle mail
 - `alias_maps`, `alias_database` – alias files
 - `smtpd_client_restrictions` – who can send mail
 - `smtpd_recipient_restrictions` – 'rcpt to' restrictions
- What about SSL between servers?

Dovecot IMAP server

- One of a couple of servers to use
 - Cyrus and Courier IMAP servers are alternatives
- Allows access to mailboxes
 - Either securely or insecurely, imap vs imaps (SSL!)
- This is only for reading email
 - Sending requires configuration on the MTA
 - Want to allow authenticated users from anywhere (SMTP AUTH) or users on 'mynetworks'

Security!

- ooooh...



He looks...
mildly crazy.

The Big Bad Internets

- We have machines and services externally accessible
 - What do we have to worry about?
 - Depends on the specific situation
- What do we want to protect against?
 - Loss of sensitive information, CC numbers, financial records
 - Who has access to a machine
 - Downtime of any service offered
 - What else?

Computer and Network Security

- What do we need to think about regarding a machine?
- What sorts of possible vulnerable points are there?
 - Any open port anywhere (SSH, web, etc)
 - Users on the machine
 - Why?
 - Physical access to the machine
 - Pulling the plug
 - Access to the bios
 - rebooting to privileged modes

The CSEL Setup

- The CSEL has a hard outside and a soft-n-chewy inside
 - Two (possibly three?) servers are externally visible
 - csel.cs and duos.cs (I think lesc.cs may be)
 - All 30-some-odd workstations are on an internal network
 - 10.138.202.x, routed through duos.cs
 - No workstation machines are visible to the outside world at all
 - Must first SSH to csel.cs before you can get to them
- Duos.cs is locked down from most access
 - Require SSH keys only to remotely connect from specific hosts

Soft'n'Chewy Insides

- What's the problem with the model of a hard candy shell surrounding squishy insides?
 - Any single crack in the shell can lead to gobbled insides
- What does a soft'n'chewy inside imply?
 - No infrastructure to detect intrusion
 - Once a user is inside, that user has free reign within their respective permissions
- This focuses on keeping the bad guys out at the border
 - Who is the bad guy??

The CSEL Hack

- How did we find out that our machines were hacked?
 - Only after half a day of wondering we found out
 - csel.cs was completely locked up around 10:45am
 - Rebooted back into a normal state
 - lesc.cs was still running, initial check looked ok
 - Turns out it was easily broken into
 - Root login was used from romania
- How can we detect potential problems on the fly?
 - And prevent this sort of post-incident discovery?

Logs are your Best Friend

- Without logging, how could you track anything?
 - Windows has it, anyone know where?
- Understanding your logging is your first step
 - `/var/log` contains most everything needed for forensics
 - NEVER ditch your logs when trying to track down a problem!
- Where is the first place you look for bad things that may happen on your system?
 - **auth** and **authpriv** logging facilities
 - Check `syslog.conf` to see where these are logged
 - `/var/log/auth.log` for Ubuntu

Logwatch – A Log Summary

- Simply a system log analyzer and reporter
- Available on most every linux machine I've seen
 - Installed by default on Fedora, Ubuntu
- Default install works right out of the box usually
 - Emails root once a day (around 4am) with a log summary
- Shows information from many different locations
 - httpd, PAM utilities, disk usage, SSHD errors

Proactive Log Scanning

- Logwatch can be configured to scan more frequently
 - But constant emails that large can be annoying
 - Tends to make people ignore the constant emails
- How can we proactively scan our log files?
 - What are we looking for?
 - Successful logins
 - Multiple attempts with incorrect logins
 - Which log files are important?