# Beginning System Administration DeCal

Week 9 - Security

April 12, 2010

# A compromised server daemon

- Imagine the scenario in which Apache is compromised
  - What parts of the filesystem are accessible by Aapche?
  - Writable and executable files and locations can be exploited
  - Local user accounts might be compromised
- What is the solution to this?

# User Privilege Separation

- Apache runs as user apache or `www-data`
  - Must grant user access to your data
  - On compromise, apache has access to user data
- Apache runs as each user
  - `suExec`, `cgiwrap`
  - Apache temporarily becomes the user to access user files
  - Performance Considerations - excessive forking, no caching

# Auditing Log Files

- /var/log
  - `auth.log` - login attempts
  - `daemon.log` - server daemon messages
  - `user.log` - user action logs
- Auditing Tools
  - `logcheck` - automatically sends emails with important data
  - `webalizer` - graphical analysis of apache logs

# Software Pataches

- Software is not perfect
- In the wild
  - Hackers continually discover security holes and produce exploits for them
  - Security companies provides security advisaries and proof of concepts
- Patches provided by Software Vendors
  - Sysadmins must monitor advisories and test patches before deployment
  - Package management makes patching easy
  - Newsgroups and mailing lists

# Scripting

- Tasks become repetitive
- Scripts

  `cleanup.sh`

  ```
  #!/bin/bash
  rm *.tmp *aux
  ```

- and run as...

  ```
  ./cleanup.sh
  ```

# Cron

- Execute scripts at specific times or intervals
- Specify times and the command
- `crontab -e`, `crontab -l`

# Access retrictions

- Restrict what users can do with logins
  - No logins - change shell to `/bin/false`
  - Command restrictions
    - `scponly` - can only use `sftp` and `scp`
    - Public Key Authentication

# Public Key Authentication

- ssh-keygen to generate a public/private key pair
- Keep private key safe and distribute public key to remove servers in authorized_keys file
- Restrictions
  - From="ocf.berkeley.edu", command="uptime"
  - No-port-forwarding, no-X11-forwarding, etc