Security

Beginning System Administration Decal

Week 9

Web Server Security

- What happens when Apache is compromised?
  - Files accessible by Apache
  - Writable and executable content exploits
  - Local user accounts compromised
- Solutions?

User Privilege Separation

- Apache runs as user apache or www-data
  - Must grant privileges to user to show content
  - On compromise, all users affected
- Alternative – apache runs as each user
  - suExec, cgiwrap
  - Apache temporarily becomes the user to access a user’s files.
  - Performance Considerations
    - Excessive forking, no caching

Auditing Log Files

- /var/log
  - Auth.log – login attempts
  - Daemon.log – server daemons
  - User.log – user actions
- Tools
  - Logcheck – automatically emails sysadmins with important log entries
  - Webalizer – parses apache access.log, error.log

Patching

- Software is not perfect
- In the wild
  - Hackers present exploits which take advantage of security holes
  - Security companies provide security advisories and proof of concept
- Patches provided by Software Vendors
  - Sysadmins head advisories and test patches before deployment
  - Package managers makes patching easy
  - Newsgroups and mailing lists

Automating Tasks

- Tasks become repetive
- Scripting
  - Cleanup.sh

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

  - ./cleanup.sh

Cron

- Execute scripts at specific times and/or intervals
- Specify
  minute;hour;day of the month;month of the year;day of the week;command
  - 0,20,40 * * * * ./20-minute-snapshot.sh
  - 0 23 0 * 5 ./monthly-backup.sh
- Crontab –e, crontab -l

User Access Restriction

- Restrict what users can do with their logins
  - No login – change shell to /bin/false
  - Command restrictions
    - Scponly – can only use sftp and scp
    - Public Key Authentication
- Public Key Authentication
  - Alternate identification mechanism using signatures and challenge responses

Public Key Authentication

- ssh-keygen to generate a public/private key pair
- Keep the private key and place the public key in the remote server's authorized_keys file
- Restrictions
  - From="ocf.berkeley.edu",command="uptime"
  - No-port-forwarding,no-X11-forwarding,no-agent-forwarding, no-pty