Overview

- Last Lecture
  - Scripting
- This Lecture
  - Basic system/network administration
  - Reference:
    - *Linux Network Administrators Guide*, O. Kirch & T. Dawson, O-Reilly
    - http://en.tldp.org/LDP/nag2/index.html
- Next Lecture
  - System installation

Security Awareness

- When a computer is connected to a network, it is under potential attack!
- Physical network/machine protection
- Attacks are from the network and through servers run by the computer
  - Remove the services if you don't need them
- Internet attacks
  - Worms
  - Viruses
  - Malware
  - Denial of Service (DoS), Distributed DoS (DDoS)

Security Awareness (cont.)

- Computer/Internet hazards
  - SPAM/UCE (Unsolicited Commercial Email)
  - Phishing
  - Disk crashes/data loss
  - Loss of services due to outage
  - TCP/IP spoofing and sniffing (privacy)
  - Pornography
  - Ignorant users
  - Grumpy (former) employees
  - Administrators of the untrained kind
  - …

Softlink attack

- Suppose program foo is setuid
- It retrieves the information for machines or usernames by user and sorts the information into a temporary file /tmp/foo
- Malicious user Trudy creates a symbolic link to /root/.rhosts named /tmp/foo
- After foo is run, /root/.rhosts will have the <hostname, username> information as Trudy wishes.
- Then everyone can login as superuser to the attacked machine.
- Luckily Linux now forbids softlink for programs with setuid.

Broken symlink risk

- Broken symlink could be a risk
- If it is pointing to a location that is accessible by an attacker, it ends up retrieving a file belong to the attacker.
- If it is a web server, you end up retrieve and present the attacker's information.
- Solution: NO_FOLLOW flag to stop following the symlink.

Roles in a Network Community

- To be a good system admin, you should be aware of the roles in a network community and their strengths and weaknesses.
- Important roles include users, hosts, network components e.g. routers and operating systems.
  - Users - should be trained to be aware of the community. **Human beings are usually the weakest link.**
  - Host machines - should be allocated different tasks on different server machines
  - Routers/gateways – affect network security and performance
  - OS - have different pros and cons
    - UNIX/Linux, Windows, MAC OS, Netware

User Management

- User account
  - Includes all the files, resources, and info belonging to one user. For commercial systems, it may include billing info.
- Create a new account
  - **adduser**
  - Account info: username, password, user id, group id, full name of user, home directory, login shell
  - In the **/etc/passwd** file,
    - Amber:x:1000:100:Amber Dawn:/home/amber:/bin/bash
  - Check after adding

User Management (cont.)

- Involved files
  - **/etc/passwd**, **/etc/group**, **/etc/shadow**
  - In **/etc/shadow**,
  - Chloe:$2a$05$wa7xVOqOH4lVOrh.qa9ivSX0G0QUCFqbk11YV6:14743:0:99999:7:::
  - Username:encrypted password:last password change:minimum:expiration:warning:disabled:diabled date:reserved
- User login environment
  - **.bash_profile, .bashrc, /etc/profile**
  - Place global files such as **profile** under **/etc**
    - Other scripts can be referred in it
  - Use **env**/**set** to check/set your environment
    - Paths and prompts
  - Keep a copy of your shell scripts (initial setups) in order to survive them from upgrade of OS/software
- For more detailed info, **man bash**

User Management (cont.)

- Password
  - Very important for security
  - Should not be names of persons, books, places, your computer, nor your phone number, birthday, car registration plate, login name, words in dictionaries, keyboard sequence
  - Should be composed of letters (lower and upper cases), digits, and special characters like $,@
  - Refer to http://en.wikipedia.org/wiki/Password_strength
  - **passwd** imposes similar rules to make passwords secure.
  - Change frequently
- User id and group id
  - Users should be divided into groups for security reasons, e.g. students, staff, admin
  - Special users/groups: nobody, mail, ftp
- **addgroup**
  - In **/etc/group**,
  - video:x:33:hzy,paul,kai
  - Group name:password:group id;list of members

User Management (cont.)

- Remove a user: **deluser**
  - The relevant lines from **/etc/passwd**, **/etc/group**, and **/etc/shadow** will be removed.
  - It is a good idea to first disable the account before you start removing stuff
- Disable a user temporarily
  - A better way when you are not sure if a user will come back
  - Way 1: Put an * in the password field of **/etc/passwd** or **/etc/shadow**
  - Way 2: use **passwd -{llu} username**
  - Way 3: Change the login shell to a script file

User Account

- How to manage user accounts on different computers?
  - Share home directory using NFS
  - Share passwords using NIS (Network Information System) or LDAP (lightweight directory access protocol)
  - Allocate an Email server
  - Directory services like LDAP
- How to remember different passwords for different accounts on different computers?

User Account (cont.)

- Control user resources
  - Disk space
    - Separate disk partition for problem users
  - Use **df** command to monitor space
  - Quotas and limits
    - Better not to put them on users until necessary
    - Check **limits.conf** under **/etc/security**
  - Killing old processes: **kill**
    - Don't do it unless you are absolutely sure
- Account policy
  - Who shouldn't have a user code?
  - How to deal with weak passwords?

User Support

- User support services
  - cshelp
- User training and well-being
- How to treat the users?
  - Your adversaries?
  - Your friends?
  - Your co-operators?
  - …

Keeping Time

- Time zone
- Showing and setting time
  - **date**
  - **date -u**: showing the universal time
  - Get a time stamp: **date +%y%m%d%H%M%S**
- Hardware and software clocks
  - Use **date** to update software clock
  - Then use **hwclock -w** to set hardware clock

Keeping Time (cont.)

- Time server
  - Use some time server with accurate time
  - **netdate udp hostname** will set the time of the current machine to that of **hostname** (It seems netdate is not available now)
  - Can automatically adjust time by putting the command in cron table.
  - Can also use NTP for more accuracy
- Network Time Protocol (NTP)
  - Used to synchronize the time of a computer to another time server or reference time source.
    - **ntpdate**
  - Accuracy: 1 ms to dozens of milliseconds
  - Cryptography for security
  - How does it work? For more details, please refer to http://www.ntp.org/

Host Management

- Shutting down a host
  - Turn off the power?
  - Should use command **shutdown**
  - **shutdown -h time** halt the system. **time** can be **now**.
  - **shutdown -r time** reboot the system
- Log files and audits
  - **syslogd**: a daemon for logging messages. Its configuration file is **/etc/syslog.conf**
  - **dmesg**: check kernel messages
  - **lastlog:** check the last login time of every user
  - **syslog** under **/var/log**: the log file of the system
  - They should be rotated regularly

Software Installation

- GNU software structure
  - lib, bin, sbin, etc, src
- GNU software installation
  - **./configure**
  - **make**
  - **make -n install:** before real installation.
  - **make install**
- Package management
  - **apt**, **rpm, yum, dpkg (the basic mechanism of apt)**

Summary

- Which files are involved in user management?
- Different roles in a network community
- What should a strong password look like?
- How to support users? Like cshelp, user training, friendly attitude.