CST8177 – Linux II

System Administration

Todd Kelley
kelleyt@algonquincollege.com

Today's Topics

- logging into CLS from off campus on Port 443
- mail command on CLS
- system administration
- user and group management

Port 443 to connect to CLS

- If you are off campus and you cannot access the CLS, it could be because Port 22 (the SSH port) is blocked.
- The CLS also listens for SSH connections on Port 443, the HTTPS port, which is less likely to be blocked
- Try adding a -p 443 option to your SSH command:
  - `ssh -p 443 kelleyt@cst8177.idallen.ca`

mail

- use the mail command to send outgoing and read incoming email on the CLS
- Sending outgoing (user types what's in bold):

```
$ mail username@example.com
Cc:
Subject: First Message from CLS
This is a test message.
^D
$
```

System Administration

- http://www.gnu.org/fun/jokes/know.your.sysadmin.html
- The system administrator role in a nutshell is to keep the system healthy and the users as productive as possible
- OK, what's a system? Examples:
  - multi-user Linux machine like our CLS, 245 users
  - multiple Linux workstations (lab in T127)
  - individual Linux workstations (primary user is a sysadmin too, they come to you for help)
  - Web Servers, Mail Servers, Document Servers...
- OK, what does it mean for a system to be healthy?

Healthy Multi-User System

- an account has been created for everyone who should have one (the users)
- every user is authorized to read, write, and execute exactly what they should be able to
  - not more
  - not less
- every user can access the resources they need
  - disk space
  - software applications/libraries
  - processes, memory, CPU time
  - resource hogs don't affect the work of other users

Healthy Multi-User System (cont'd)

- Accessible to its users
  - accessible remotely if applicable (ssh)
  - good uptime with reasonable maintenance windows
- Secure from attack
  - inaccessible to unauthorized users (external attack)
  - no unauthorized or stolen access to user accounts
  - resistant to internal attacks
    - users cannot elevate their privileges
    - users don't bring system down without trying
  - prevent cross-user attacks
    - ensure users cannot interfere with each other's
      - confidentiality of files
      - integrity of files
      - availability of files

Regular Maintenance

- backups
- security patches
- monitor and manage disk space
  - find and educate and control "space hogs"
  - add new disk space
  - replace failed disk space
- software installation
- software updates
- system upgrades (preferably not often)
- monitor the system logs for issues

Three types of account

- Root account
  - having a root password is not necessary
  - not having a root password means one less password to manage, one less vulnerability
  - root access is gained by system administrators
- System Administrator
  - configured in sudoers file
  - gain root privileges with `sudo -s`
- Regular User
  - often named according to a pattern
  - this is the kind of account you have on the CLS

Setting up root

- common model is to put sysadmins in sudoers file
- as root, do `visudo`
- put the following line in
  - `youradminname ALL=(ALL) ALL`
  - youradminname: the username you use for admin
  - ALL: from any host
  - (ALL): run commands as any user
  - ALL: run any command
- test that you can become root with `sudo -s`
- put * in root password field in /etc/shadow

sudo refresher

- `sudo -s` gives you a shell as root
- this is not a login shell, it retains your old environment
- after sudo -s, you can simulate login with

`su -`

- the dash means "simulate a full login"
- a full login will leave you with root's path
- root's path will contain /sbin, /usr/sbin, etc, which are directories not normally needed in a regular user's path

User Management

- Create, Modify, and Remove User Accounts
- Create, Populate, Modify, and Remove Groups
- Password Policy
  - strength of passwords
  - how often passwords must be/can be changed
  - how often passwords can be reused (or based on an old password)
- Set and Administer File Permissions
- http://teaching.idallen.com/cst8207/12f/notes/600_users_and_groups.html

passwd command

- man passwd
- passwd –l : lock an account
- passwd –u: unlock an account
- passwd –n: min password lifetime in days
- passwd –x: max password lifetime in days
- passwd –w: number of days warning
- passwd –i: number of days after expiry to disable
- passwd –S: print a summary