RANCID exercises
AfNOG 11, Kigali

RANCID and CVSWeb are already installed on your stations - on a clean Ubuntu you can install them with:
```
sudo apt-get install rancid-core rancid-util expect cvsweb
```
(you need a webserver installed like apache2)

Choose your assigned router:
PC1-10: 196.200.218.249
PC11-20: 196.200.218.250
PC21-28: 196.200.218.251
PC29-36: 196.200.218.252
PC37-44: 196.200.218.253
You will monitor all routers, but only make changes in your group for the assigned router

1. RANCID will run as the rancid user on the local workstation. So will this exercise
   ◦ Login as root first: `su` (use password on the board)
   ◦ Login as user rancid: `su -s /bin/bash rancid`
   ◦ Change to the home directory of rancid: `cd ~`
   ◦ Check: `pwd` - you should be in `/var/lib/rancid`
2. First you need to configure clogin so it can login to the routers
   ◦ Login to your assigned router via telnet, enter configuration mode and add a user rancid. :
     ```
     ssh inst@x.x.x.x (use your assigned router ip - enter
     the password)
     ```

   ◦ Enter the following commands on the router command line:
     ```
     conf t
     username rancid password rancid
     end
     wr
     exit
     ```
   ◦ `vi .cloginrc` (or use your favourite editor). Enter the following file:
     ```
     add user * rancid
     add password * {rancid} {afnog}
     ```
     (This tells rancid it can login to all routers via telnet with username rancid, password rancid and enable password AfNOG - if you want usernames/passwords per router, just put the IP address instead of * and use one line per router)
   ◦ Protect the file from other users: `chmod 600 .cloginrc`

- Try it with your assigned router: `bin/clogin x.x.x.x` --- you should be automatically logged in. exit the router (if it doesn't work try again - there can only by 5 at the same time)

3. You need to define the groups of devices - we will only have one called cisco (you could have one for each Cisco,HP,Juniper, one per city, per workgroup, whatever):
   - Open a new terminal window, you need to be root. Do `sudo vi /etc/rancid/rancid.conf` (use vi or your favourite editor, but you must be root)
   - search for the line `LIST_OF_GROUPS`, uncomment it and set only one group "all". It should look like this:
     `LIST_OF_GROUPS="all"`
   - Save and exit the editor
   - Before you continue, make sure you are user rancid again (run `whoami` to confirm). Run `su -s /bin/bash rancid` if you are not.
   - Let rancid create necessary files. Run `/var/lib/rancid/bin/rancid-cvs`. You should see output like this:
     ```
     No conflicts created by this import

     cvs checkout: Updating all
     Directory /var/lib/rancid/CVS/all/configs added to
     the repository
     cvs commit: Examining configs
     cvs add: scheduling file `router.db' for addition
     cvs add: use `cvs commit' to add this file
     permanently
     /var/lib/rancid/CVS/all/router.db,v  <--  router.db
     initial revision: 1.1
     ```
4. Now add the monitored routers to the router.db file of the group.
   - Edit `/var/lib/rancid/all/router.db`
   - Add one line like this for every router in the classroom (monitor all of them, not only your assigned one):
     ```
     196.200.218.249:cisco:up
     196.200.218.250:cisco:up
     196.200.218.251:cisco:up
     196.200.218.252:cisco:up
     196.200.218.253:cisco:up
     ```
   - Save the file and exit
5. Check that someone in each row has at least completed Step 2, so your rancid will be able to login to all routers in the classroom
6. Run rancid the first time
   - `/var/lib/rancid/bin/rancid-run`
   - Check the logs: `more /var/lib/rancid/logs/*`

- ◦ If it looks ok you should be able to see all router configuration files with ls cisco/configs - check one:
  `more /var/lib/rancid/all/configs/x.x.x.x`
7. Now change something on your assigned router:
   - ◦ `bin/clogin x.x.x.x` (this should still work)
   - ◦ `conf t`
   - ◦ Change something on the router which has no effect according to the following schema:
     - ▪ PC 1,11,21,29,37: `snmp-server location <YOUR HOMETOWN and Country>`
     - ▪ PC 2,12,22,30,38: `snmp-server contact <Name of someone in class>`
     - ▪ PC 3,13,23,31,39,: `banner motd ^ AfNOG is cool!!! ^`
     - ▪ PC 4,14,24,32,40: `access-list 1337 permit any`
     - ▪ PC 5,15,25,33,41: `interface Loopback 0 description My home is my castle`
     - ▪ PC 6,16,26,34,42: `line vty 0 4 logout-warning 60`
     - ▪ PC 7,17,27,35,43: `line vty 0 4 motd-banner`
     - ▪ PC 8,18,28,36,44: `no ip httpd server`
     - ▪ PC 9,19: `service nagle`
     - ▪ PC 10,20: `autonomous-system 65432`
   - ◦ `end`
   - ◦ `wr`
   - ◦ `exit`
8. Run rancid again
   - ◦ `/var/lib/rancid/bin/rancid-run`
   - ◦ Check `/var/lib/rancid/all/configs/x.x.x.x` - can you spot your change?
   - ◦ Look at other files, did they change? How can you tell?
   - ◦ `cd /var/lib/rancid/all/configs`
   - ◦ try `cvs log x.x.x.x` for files you suspect changed to see revisions, then `cvs diff -r1.3 -r1.2 x.x.x.x` (or similar) to compare revisions (or `cvs annotate x.x.x.x`)
   - ◦ feel free to run rancid again to catch other people's changes.
9. Now add the switches from the network diagram:
   - ◦ Edit `/var/lib/rancid/all/router.db`
   - ◦ Add one line like this for every Cisco switch in the classroom (2 are Cisco, 3 are HP):
     `196.200.218.29:cisco:up`
     `196.200.218.61:cisco:up`

- Run `bin/rancid-run` again and look at the changes
10. Look at your configs via Web Interface
    - Edit (as root) `/etc/cvsweb/cvsweb.conf`
    - search for `/var/lib/cvs` and change to `/var/lib/rancid/CVS`, save and exit
    - make a link to cvsweb: `sudo ln -s /usr/share/cvsweb /var/www/cvsweb`
    - Open in your browser: http://localhost/cgi-bin/cvsweb - and navigate there
      Obviously, if you choose to use this "at home", secure that web server
11. Bonus exercise if you're done early: Add mail capabilites to RANCID:
    - Edit /etc/aliases as root and insert the following:
      `rancid-all: net@noc.mgmt.ws.afnog.org`
      `rancid-admin-all: net@noc.mgmt.ws.afnog.org`
    - Then run 'newaliases'This will forward all rancid emails to the RT on the NOC maching
    - Change the snmp location to something else (see step 7)
    - Run `/var/lib/rancid/bin/rancid-run` again
    - You should have mail in RT showing the changes