ITB721/ITN721 Unix Network Administration

Practical 4

Ensure that you browse the man pages for all relevant commands immediately before using them.

Exercise 1: Process Management

1. Using appropriate options, display the process table for each of the following situations:
    a. A full listing of processes running under your normal user account
    b. A full listing of processes running as the "root" user
    c. A long format listing for all entries in the process table for the "sendmail" process
    d. A full listing for all processes on the system
    e. A full listing of all processes on the system sorted by UID
    f. A listing of only the PIDs for all "bash" processes
2. Using your command line from 1(d) above, record the entries for the "init" process and the "bash" process/es. Explain the meaning of the UID, PID, PPID and CMD fields in these particular entries.
3. Using your command line from 1(d) above, identify two processes that have a parent-child relationship. How did you determine this relationship?
4. Display the most processor intensive processes on the system in a form that continuously updates the information. What command did you use? Which is the most CPU intensive process? How did you determine that?
5. Which process on your system is the most "not nice" process? (There could be more than one.) Which process is the "nicest" process? (There could be more than one.) How did you determine these? What does it mean if a process is "not nice"?
6. Using an appropriate command line, find the process ID of the "cupsd" process owned by root. Kill this process only.
7. From your terminal window, run the command "xclock&" three times. Display the process table and check that these entries exist. Now, using a single command line, kill all the instances of "xclock".

Exercise 2: Using SSH

You wish to establish a secure remote shell connection from the "vmuser" account on virtpc1 (the client) to their "vmuser" account on virtpc2 (the server). You will be using SSH for this.

1. Start up virtpc1 and virtpc2.
2. Configure and activate eth0 on virtpc1 with the IP address 192.168.20.1, netmask 255.255.255.0 and broadcast 192.168.20.255.
3. Configure and activate eth0 on virtpc2 with the IP address 192.168.20.2, netmask 255.255.255.0 and broadcast 192.168.20.255.
4. Check the connectivity between virtpc1 and virtpc2.
5. Perform all necessary tasks in order to use the SSH service. (**In addition, be sure to stop the ssh**

service on virtpc1.)

6. From the "vmuser" account on virtpc1, use the "ssh" command to securely connect to their "vmuser" account on virtpc2. Use the "hostname" command to verify that you are actually logged on to virtpc2. Close the SSH connection by typing "exit".

Exercise 3: Using SCP

You now wish to securely copy files from virtpc1 (the client) to virtpc2 (the server). You will be using SCP for this (which requires the SSH service).

1. On virtpc1, perform all necessary tasks to create a new account for Mr W Brown to use.
2. On virtpc2, perform all necessary tasks to also create a new account for Mr W Brown to use.
3. Ensure that all necessary tasks have been performed in order to be able to access the SSH service on virtpc2.
4. As the user "wbrown" on virtpc1, use a text editor to create the file "testing" in his home directory on virtpc1.
5. As the user "wbrown" on virtpc2, use a text editor to create the file "results" in his home directory on virtpc2.
6. From the "wbrown" account on virtpc1, use the "scp" command to securely copy the file "testing" to his account on virtpc2.
7. As the user "wbrown" on virtpc2, verify that the file was copied successfully.
8. From the "wbrown" account on virtpc1, use the "scp" command to securely copy the file "results" from his account on virtpc2.
9. As the user "wbrown" on virtpc1, verify that the file was copied successfully.

Exercise 4: Setting up SSH Public Key Authentication

This exercise is additionally required to be done by ITN721 students (but is optional for ITB721 students).

1. Following on from Exercise 3, you are required to set up SSH public key authentication between virtpc1 (client) and virtpc2 (server). As the user "wbrown" on the client, create a pair of SSH cryptographic keys (ensuring that you enter a passphrase). Locate the two files that your new private key and public key have been stored in and view their contents.
2. In Mr Brown's home directory on the server, ensure that a directory called ".ssh" exists, and if not, create it and ensure that this directory has appropriate permissions. Use an appropriate "scp" command line to copy your public key from the client machine to that ".ssh" directory on the server. Rename this file appropriately on the server and ensure that this file has appropriate permissions.
3. Restart the service on the appropriate machine.
4. Test the SSH public key authentication. As the user "wbrown" on the client, use the "ssh" command to securely connect to his account on the server. What difference did you observe between this SSH connection/login and the vmuser connection/login in Exercise 2? Use the "hostname" command to verify that you are logged on to the server. Close the SSH connection.

Exercise 5: Configuring the Telnet Service

(Note: Telnet is used in this unit for teaching purposes only.)

```
                      NETWORK 192.168.20.0/24
                +-------------------+-----------------+
                |192.168.20.1       |192.168.20.2     |192.168.20.3
                | eth0              | eth0            | eth0
           +--------+          +--------+        +--------+
           |virtpc1 |          |virtpc2 |        |virtpc3 |
           +--------+          +--------+        +--------+
             | eth1
             |192.168.74.1
             |
  NETWORK    |
192.168.74.0 |          +------+
    /24      +----------|parent|
                   veth1+------+
              192.168.74.100
```

1. Ensure that the three Xen virtual machines, virtpc1, virtpc2 and virtpc3, have been started up.
2. If required, configure eth0 on virtpc1 with IP address 192.168.20.1, eth0 on virtpc2 with IP address 192.168.20.2 and eth0 on virtpc3 with IP address 192.168.20.3. The netmask for this network is 255.255.255.0, and the broadcast is 192.168.20.255. Activate all relevant interfaces.
3. Test the connectivity to ensure that communication is possible between all three virtual machines.
4. Edit the /etc/hosts file on virtpc1 to include the following entries:

```
192.168.20.2   virtpc2.virtnet   virtpc2
192.168.20.3   virtpc3.virtnet   virtpc3
```

5. Configure and activate eth1 on virtpc1 with IP address 192.168.74.1, netmask 255.255.255.0 and broadcast 192.168.74.255.
6. The parent machine also needs to be configured to be on the same network as virtpc1. To do this, download the "configure-parent" script from Blackboard, and execute it as the root user. This script will configure the relevant interface on the parent with the IP address 192.168.74.100. **(Note that, although this task is essential to this whole exercise, students are not required to understand this ie the means by which the parent is connected to the virtual machines. Thus, this is the only question in this exercise which is not examinable. All other questions in this exercise are examinable.)**
7. Test the connectivity between the parent and virtpc1.
8. Complete the following steps to install the telnet server on virtpc1:
   a. On the parent, download the "telnet-server" and "xinetd" RPMs from http://athena.fit.qut.edu.au/721/fc6/RPMs.
   b. Perform all necessary tasks in order to be able to use SCP. Using SCP, copy the two RPMs from the parent to the home directory of vmuser on virtpc1.
   c. As the root user on virtpc1, install the "xinetd" RPM and then the "telnet-server" RPM.
9. Perform all necessary tasks in order to use the telnet service.
10. On virtpc2 and virtpc3 as clients, try to telnet to virtpc1. Verify that both virtpc2 and virtpc3 can successfully telnet to virtpc1. Then, exit from these telnet sessions.
11. On virtpc1 (the telnet server), restrict general access to the telnet service to permit only virtpc2 to telnet

to virtpc1 (the telnet server). (Hint: you will need to browse the man page for "xinetd.conf".)

12. Configure the telnet server to log the IP address of all source connection attempts (whether successful or not) to a log file called "/var/log/logfile-telnet".
13. Perform all necessary tasks in order to use the telnet service with this new configuration change.
14. On virtpc2 and virtpc3 as clients, try to telnet to virtpc1. Verify that only virtpc2 can telnet to virtpc1. Examine the /var/log/logfile-telnet log file on the telnet server and identify the entries that relate to both the successful and unsuccessful connection attempts.
15. Poweroff virtpc1, virtpc2 and virtpc3.

Exercise 6: Instant Messaging using Gaim and Jabber

Note: This exercise should be done using two different computers, each with an Internet connection. You may wish to do this exercise with a friend.

As an Administrator, you may be asked by your users to provide support for instant messaging (if instant messaging is permitted by management). This is particularly common in the case of help desk and client service job positions, as customers often wish to communicate with the help desk via instant messaging.

To gain some familiarity with server established instant messaging, set up instant messaging using the Jabber system.

1. Go to "http://www.jabber.org.au/register" and perform all necessary tasks in order to obtain a Jabber account. (Once you complete registration LEAVE YOUR BROWSER OPEN, but log out of the Jabber Australia Forum.)
2. As a normal user, run gaim by typing "gaim&" and add a new account by using the Jabber protocol, specifying your Jabber username as the Screen Name, jabber.org.au as the server, and entering your password.
3. Sign on to the system.
4. Ask a friend to also do the above steps on their computer. Exchange Jabber account details.
5. Click on "IM" and carry out a brief instant messaging conversation.