KIT304 Server Administration and Security Assurance

Tutorial 2

Goal

Today's tutorial will focus on user account creation and group management on Unix operating systems.

Introduction

The basic structure of the practical component of this unit is to cover a set of practical skills, and then conduct an exam to assess your understanding of them. The exercises you'll undertake as part of this require you to complete a set of tasks, and in some cases you will need to read online and/or provided documentation to learn how to use specific tools. The practical exams will then be a set of tasks to complete that will be similar to what you've covered in the exercises, but in a shorter period of time. You won't have time to learn the tools needed during the exams, so you will need to become proficient in the tutorials. If you get stuck or have problem, ask for help.

Activity

Today you are going to be creating, modifying and deleting users and groups on the CentOS system. But rather than use the CentOS GUI, you will be undertaking all of these tasks from the command line on another virtual machine via an SSH connection to the CentOS VM.

Networking

Your first task will be to configure the networking setup for the two Virtual Machines you'll be using in this .

1. Launch the **CentOS8** virtual machine from the VMWare Fusion window, and once it's running, log in with the username **student** and the password **student.**

2. To configure the CentOS IP address:

   - Click on the **Power** icon menu at the upper right of the screen, and then click on the **Ethernet (ens33) Off** entry to expose a submenu. Choose the **Wired Settings** option.
   - In the network settings panel that opens, press the "gear" icon to the right of the **Ethernet (ens33) 1000 MB/s** connection and then click on the **IPv4** tab.

- Change **IPv4 Method** from *Automatic (DHCP)* to *Manual*.
- In the **Addresses** section, set the IP address to `192.168.1.X` (choose your own valid value for X), set the subnet mask to 255.255.255.0, and set the gateway to 0.0.0.0.
- Click **Apply**.
- If the slide switch for the Wired connection is already on, slide it to **Off** (if you're reconfiguring the connection, you need to turn it off, and then on again for the changes to be accepted).
- Slide the slide switch for the Wired connection from **Off** to **On**.
- Close the settings window.

3. Check that the settings are now in use by starting a terminal window, and entering the command `ifconfig ens33` – the settings you entered should be visible in the output.

4. Launch **Kali** from the VMWare Fusion window. Kali is a Linux distribution that you will be using in many of your tutorials, and specifically later in semester during Network Security module.

5. Once Kali has booted up, log in with the username **root** and the password **toor**.

6. To assign an IP address to the Kali VM, open a terminal window (using the third icon from the top of the quick launch item on the left hand side of screen) and type the following

```
ip a add 192.168.1.Y/24 dev eth0
```

Choose your own value for ***Y***, ensuring that it's different to the value of ***X*** that you used for CentOS. Again check that it has been correctly assigned by entering the command `ifconfig -a`, or `ip a`. You may want to read through the `ifconfig` and `ip` manual pages to learn more about these commands. You won't be delving into them much today, but you will be using these commands in future s during the semester.

7. Now that both virtual machines have IP addresses, they should be able to see each other on the virtual network running inside VMWare. Confirm this by using the `ping` command, and then minimise the CentOS window, as you will spend the remainder of the tutorial connecting to it from Kali.

8. In the Kali virtual machine, you are going to make a remote connection to CentOS:

   - From the command line type `ssh student@ipaddress` (replacing *ipaddress* with the IP address of your CentOS host).
   - You will be prompted to confirm the connection by accepting a cryptographic key. Type **yes** to do this and then press enter. From KIT111 or KIT201 you may remember that this is the initial sharing of a key that future connections will trust. However, due to the way the lab is configured, every time you log out of the Macintosh all of the virtual machines

are reset, so you will actually get a new key (and associated prompt) the first time you connect with **ssh** in every tutorial.

- Once the connection is accepted, you'll be prompted to enter the password for the student account. It's also the word **student**.

User Accounts

Accounts on Unix are how we represent users and the files and permissions that relate to them.

In the previous tutorial you saw that each user has entries in certain files in the **/etc** folder that describe their account, and also a folder in the **/home** directory where their files are stored. In this part of the tutorial, you will create some new accounts, which will in turn create folders for those accounts in **/home**, and add entries to the relevant files in **/etc**.

In this section you are going to use the following commands (with various additional options):

- **useradd**
- **userdel**
- **usermod**

You should take a moment to read about these commands first (using **man**, or **info**) and then work your way through the following tasks.

9. Create a user with the most basic version of the **useradd** command, which results in the options being given default values. To do this, enter the command:

```
useradd username
```

(make up a username) and then take a look at what has changed in the **/home** directory, as well as what happened in the **/etc/passwd** and **/etc/shadow** files.

You will get an error on the first attempt. If you can't figure out why, ask your tutor for help. What command did you have to enter to fix this?

____

10. Using the **man** or **info** commands, find out what each column in the **/etc/passwd** file stores, and write down its purpose:

____

____

____

____

11. Looking at the **UID** field you should see that there is a numerical grouping that CentOS is using. For your new user, what is it? (This is commonly 500 in other Unix distributions. What purpose is it serving?)

    ____

12. In the `/etc/shadow` file there is a very significant difference between the account you just created and the **student** account. Use the command:

    ```
    passwd username
    ```

    to rectify this difference and verify the results by examining the `/etc/shadow` file for the change.

13. Open another Terminal window (in Kali) and create another `ssh` connection to the CentOS virtual machine, this time logging in using the new account that you created in step 10. After you've logged in, your session will be defaulted to its home directory in `/home/`*`username`*. What is different about this home directory to that of the **student** account?

    ____

    You will use this `ssh` session later, but you can return to the first `ssh` session you created leaving this one still running.

14. When you create a new account, you are able to specify that a specific directory structure and set of files be replicated automatically inside the new account's home directory. The source (or *template*) directory is referred to as a *skeleton* directory. Using the `man` page for **`useradd`**, determine and then use a variation of the `useradd` command to create a new account, but this time specify that the existing `student` account home directory should be used as the skeleton directory. What is the full command to do this?

    ____

    While the ability to use one directory as a skeleton for another is convenient, it is more common to use the default skeleton directory that already exists in the system. Where is this default skeleton directory?

    ____

15. Anything you put in a skeleton directory is copied to the home directory of new accounts that you create with **useradd** when you specify the option to use that skeleton. Modify the *default* skeleton directory (add some files and/or subdirectories to it), create another user account using the default skeleton directory, and then check that the new account's home directory contains everything in the skeleton.

> ➢ **Checkpoint 1**: Demonstrate to your tutor that you added content to **/etc/skel**, and that this new content is visible in the new account's home directory.

16. It is possible to create an account and not create an associated home directory for it. What is the command-line option to do this?

    ____

    Create another account using this option, and confirm the results in the **/home** directory and the **shadow** and **passwd** files.

17. By this point, you should have a fair amount of confidence when it comes to adding users to the system. What commands would you use to create accounts that have the following characteristics? Make sure you enter these commands to ensure they work.

    - An account with an expiry date:

      ____

    - An account with a comment field that stores extra information about the user:

      ____

18. Now that you know how to add a user and specify an expiry date on their account, you can use the **chage -l** ***username*** command to verify the expiry date. What variant of the **chage** command would you use to force a user to change their password at least every 90 days?

    ____

19. Now that you have created multiple accounts, look again at the contents of the **passwd** file. Everything that is present in this file can be changed through the use of the **usermod** command. How would you use this command to make the following changes:

    - Rename a user ____

- Change the UID of a user ____

- Set two users to have the same home directory

  ____

- Modify the comment field ____

20. From time to time it is necessary to delete accounts. The command for this is `userdel`. Try this command on the account you first created back at step 10 (for which you should still have an open **ssh** session).

    What occurs when you try to delete it?

    ____

    Look up the command `w` (lower-case "W") in the man pages, and then try it in the terminal. What can you see?

    ____

21. Since that user is currently logged in, look at the `userdel` man page and see whether any options enable you to overcome this problem. If so, what is the option?

    ____

    What occurs when you try to delete a user with this option?

    ____

22. Inspect the three files and/or directories that `useradd` modifies or interacts with. Is there anything unexpected?

    ____

    What option could you have used with `userdel` to fix this oddity?

    ____

Groups

In this section you are going to be using the following commands and numerous options on them. You may want to read about the commands first and then work your way through the tasks

- `groupadd`
- `groupdel`
- `groupmod`

23. When you examined the `passwd` file you should have seen the presence of a **GID** – or group ID field. Re-examine the `passwd` file and look at the GID values for the various user accounts on the system. What pattern is present?

    ____

24. In the `/etc` folder there is another file of interest called `group`. Take a look at the contents of this file. What similarity do you see here with the numbers for the accounts that you've created, compared to what you saw earlier for the UID?

    ____

25. There are obviously a set of fields (or columns) in the `group` file. What is the purpose of each column?

    ____

    ____

    ____

26. The `/etc/passwd` file only lists one group for each user – this is known as the user's ***primary*** group. In the `/etc/group` file you can see how users can be members of other, ***secondary*** groups. You can modify a user's group membership with the `usermod` command. You can modify a user's primary group, or you append the user to a list of one or more secondary groups.

    Add one of the users to several secondary groups. What command did you use?

    ____

    The commands `id` and `groups` are both useful for listing the groups that a user is part of. Experiment with them.

➢ **Checkpoint 2**: Have your tutor check that your response above is correct.

27. User accounts are not constrained to the groups that are automatically created when a new user is created – you can also create your own groups. Use the **`groupadd`** command to create a new group and then add some users to it. What command did you use to create the group?

    ____

28. Using the **`groupdel`** command, try to delete a group that is a user's primary group. What happened?

    ____

    What occurs if you try to delete a secondary group in the same way?

    ____

29. The final command that you should try today is the **`groupmod`** tool, which allows you to make changes to the groups that already exist. What command is required to give two groups the same GID?

    ____

    Feel free to experiment further with these group commands until you are confident with them and with options you've explored in this tutorial.

Finishing up

When you're done using a virtual machine, either **suspend** it or you can **power it down**. from VMWare's **Virtual Machine** menu. It doesn't matter which of these you choose.

> ➢ After suspending or powering down any VMs you were running, and before logging out, be sure to reconnect your Macintosh to the campus network. If you do not do this, and try to log out, the system will display an alert message and sound a warning. It is important that machines be on the campus network when not in use so that they can receive important software updates.

After you log out, the Macintosh will reboot, and the kit304 account you were using will be reset. All of the changes you made to the virtual machine will be deleted and reset to the initial state that has been established for this unit.

Conclusion

Today you have had some practical experience creating, modifying and deleting both users and groups. You will continue to build on this next week when you look more closely at *superusers* and look in more depth at *permissions* and *processes*.

As you work through these topics you should try to become self-reliant and be able to look up the information you need using the **`man`** and/or **`info`** tools. There is considerably more depth to the tools you are using that there won't be time to explore in the tutorials, but the important point is that the documentation is there, readily available for you to explore on your own.

Skills to Master

To successfully complete this tutorial, you must have mastered the following skills:

- be able to create user accounts, and modify attributes about them including their comment field and home directory
- be able to set an expiry date on an account
- be able to create accounts that use a skeleton directory for initial home directory content, and be able to modify that skeleton directory content
- be able to create groups, and add accounts to, and remove accounts from them
- understand the meaning of the fields in each of the files **`/etc/passwd`**, **`/etc/shadow`** and **`/etc/group`**
- be able to use the **`man`** command to learn not only about existing commands, but also to learn about the format of configuration files like **`/etc/passwd`**

Anything identified in this skills section could be part of an assessment item in this module.