DT149G — Administration of UNIX-like systems
Laboratory Assignment:
System Administration II

Lennart Franked[*]

October 25, 2024

Contents

1 Introduction **1**

2 Aim **2**

3 Reading instructions **2**

4 Tasks **2**

4.1 Bootprocess . . . 2

4.1.1 Runlevels . . . 2

4.2 The file system . . . 2

4.2.1 File-types and Links . . . 3

4.3 Users, groups and permissions . . . 4

4.3.1 User and groups . . . 4

4.3.2 Permissions . . . 4

4.4 Backup and file copy . . . 5

4.5 Sharing files . . . 5

4.5.1 File Transfer Protocol . . . 5

4.5.2 Network File System . . . 5

4.5.3 Samba — A Windows SMB/CIFS file server for UNIX . . 5

4.6 Setting up the firewall . . . 6

5 Examination **7**

1 Introduction

In this laboratory assignment you will work with basic system administration such as startup scripts, user account management, creating new file systems and examining different tools to create backups of your filesystem.

[*] E-post: lennart.franked@miun.se.

2 Aim

After completion of this assignment you will have:

- Become familiar with upstart, init and boot scripts.
- Know how to administrate user accounts.
- Knowledge how to partition and format new harddrives for your system.
- Be able to set up storage backup on your system.
- Have the knowledge of setting up an IPTables firewall.

3 Reading instructions

Before starting this assignment you should have read Nemeth et al., 2017, chapters 2, 3, 5, 8, 21, 22, 27.8. During the lab you will also need to consult the follwing documents Bhushan, 1971, Postel and Reynolds, 1985

4 Tasks

Perform the following tasks and document all the steps taken to complete the tasks.

4.1 Bootprocess

4.1.1 Runlevels

1. Even though Ubuntu no longer uses the System V runlevel system, it still uses runlevels to place the system in different states (off, singeluser, multiuser and restart). Before starting these tasks, see `telinit (8)` and `runlevel (8)`.
    - which runlevel is your system currently in?
    - Place your system in another runlevel.

To answer in your report *Explain how the links in `/etc/rc?.d` relates to the scripts in `/etc/init.d`. See `runlevel (7)` for a detailed explanation.*

4.2 The file system

Before you start this assignment, create a new disk volume in your hypervisor, and link this to your virtual machine. Once you have done this, you should familiarize yourself with `df (1)` and `du (1)` `fdisk (8)`, and the /dev folder. With the help of these commands, find the following information.

1. Identify your disk partitions and how much free space you have on them.
2. Find the flag to `df (1)` to show the results in powers of 1024.
3. How much disk space does your `Desktop` folder take?

4. Create a new partition that spans all the unpartitioned space on your newly created disk volume.

5. Create a new ext4 file system on the new partition, see `mkfs (8)`,

6. check that the file system is ok, see `fsck (8)`,

7. create a new mountpoint in your system e.g. /dump,

8. mount your newly created and formatted partition to your mount point,

9. configure your system to automatically mount your new partition at boot, see `fstab (5)`.

To answer in your report

- *Which partitions did you have, and how much free space did they have in MB or GB?*
- *How large was your Desktop-folder in MB or GB?*
- *Take screenshots of what you did to create a new partition and then formatting this partition using ext4.*
- *Include a screenshot of your fstab after you have added your newly formatted partition*
- *Explain the configuration line that you added to fstab.*

4.2.1 File-types and Links

Read the man-page for `stat (1)` and `ln (1)`, then perform the following tasks.

1. Run `stat (1)` on a file in /dev, a folder, a file in /etc/init.d/ and on the /etc/passwd file. Note the difference between the different files.

2. Create a symbolic link within a file system, and then create a symbolic link to a file located on another file system.

3. Create a hard link within a file system, and then create a hard link to a file located on another file system.

To answer in your report

- *What information can be found in an inode?*
- *What where the difference between the different files you were running stat(1) on?*
- *From a theoretical point, what is the difference between a hard link and a symbolic (soft) link? Make sure your answers include a discussion about inodes.*
- *Based on your observation from the laboratory task above, what practical difference is there between a hard and a soft link?*
- *Reflect upon different usage scenarios for the two types of links*

4.3 Users, groups and permissions

4.3.1 User and groups

Before starting with the next assignment, make sure to get aquainted with `passwd (5), shadow (5)` and `group (5)`, followed by `adduser (8)`, `addgroup (8)` and `adduser.conf (5)`. Make sure to read about the purpose of `/etc/skel`.

1. Make the appropriate changes so that a `.ssh` folder is created in the home folder for every new user that is added to the system.
2. Add the users *donald* and *mickey* to your system with the help of the `adduser (8)` command.
3. Create the group *disney* and add your newly created users to that group.

To answer in your report

- *Explain* UID *and* GID *and how it relates to users in the system*
- *What did you have to do, so that every time you create a new user a* `.ssh` *folder will be present in that users home folder?*
- Briefly explain the process of adding a new user and group to your system.
- Include a screenshot that shows that you now have created two more accounts. (Note that showing home-folders will not be enough to show this)

4.3.2 Permissions

The next part can be solved using the `ls (1), chmod (1), chown (1)` and `chgrp (1)` commands.

1. check the permissions for the home folders of the newly created users,
2. change the permissions on the home folder so that the owner and the group of the home folder is the only one able to access it.
3. create a new folder in e.g. `/dump` that only the users in the disney group can access.

To answer in your report

- Take a screenshot, that shows before and after you have changed the permission of the newly created folder in /dump.
- explain as much as you can about the file listed below

```
-rw-r--r-- 1 lennart lennart 5496 nov 10 17:40
    lab_assgn2.tex
```

4.4 Backup and file copy

For this part, you need to get familiar with the following programs: `cp (1)`, `tar (1)`, `cpio (1)` and `rsync (1)`.

1. Create a backup script for each of the programs listed above. The backup script will must take a backup of your home folder and place it in your newly created partition.
2. With the help of `dd (1)` create a copy of your `/etc/passwd` file where the contents of the file has been converted to upper case letters *NOTE: READ THE MAN-PAGE CAREFULLY BEFORE DOING THIS, IF PERFORMED WRONGLY YOU WILL BREAK YOUR SYSTEM.*

To answer in your report

- *Include all your four scripts in the report, along with a short explanation of how it works.*
- Take a screenshot of your modified passwd-file.

4.5 Sharing files

There are numerous ways of sharing files over the network, in this section we are going to test three popular methods of sharing files. The first method covered in this lab is also one of the earliest method, the File Transfer Protocol (FTP). The first RFC about FTP was published April 16th 1971 Bhushan, 1971 and an updated version of FTP was published in rfc959 Postel and Reynolds, 1985.

4.5.1 File Transfer Protocol

1. Find and install an FTP-server of your own choosing, for example `ftpd (8)`.
2. Using file and folder permissions, configure your system so that each users home folder is not accessible to anyone else. Show all the steps taken to achieve this.
3. Give access to the /dump folder to all the members in the Disney group.

4.5.2 Network File System

1. Install NFS on your system and configure it in the same way as you did with the FTP-server, that is, make sure that each user can access their home-directory and that only users that belong to the Disney group can access your partition that you created in the second laboratory assignment.

4.5.3 Samba — A Windows SMB/CIFS file server for UNIX

1. Finally install and configure SAMBA the same way as for FTP and NFS

To answer in your report

- Give a short description of the installation and configuration process for FTP, NFS and Samba
- Reflect upon the different ways in FTP, NFS and SAMBA to handle permissions and users.
- Include screenshots that shows that you have a working FTP, NFS and SAMBA server.

4.6 Setting up the firewall

Linux use the Netfilter framework to filter packages, enable NAT or PAT and perform other forms of packet mangling, see netfilter.org, 2023 for more information about netfilter. In this section we are going to work with IPTables, which is a text based front-end for Netfilter.

In this section, you will setup IPTables so that you will allow your computer to run as usual, and open up the ports for FTP, NFS and Samba.

With this in mind we need to configure our firewall for the following policy:

- Drop all incoming packets by default.
- Allow all traffic to and from the local networks.
- Allow all incoming packets using transport protocol TCP and port 137-139, 445 (SAMBA/CIFS).
- Allow all incoming packets using transport protocol TCP and port 20,21 (FTP).
- Allow all incoming packets using transport protocol ICMP of type echo-request.
- Allow all incoming packets using transport protocol ICMP of type echo-reply.
- Allow all outbound packets.
- Enable stateful packet inspection

You will in the upcoming assignments update this policy.

Since the rules for IPTables are added with the help of the `iptables(8)` command, the best way to set up your firewall is by adding the commands in a shell script. Therefore create a file named `iptables.sh` and add the following at the beginning of the file:

```
#!/bin/sh
#
#IPTABLES SCRIPT
#<COURSE NAME> <COURSE CODE> - ASSIGNMENT 6
#<YOUR NAME>
```

```
#
#Creating a macro that specifies the location of iptables.
IPTABLES=/sbin/iptables

echo ‘‘Flushing existing tables’’
$IPTABLES -F
echo ‘‘Setting default policies’’
$IPTABLES -P INPUT DROP
#Make sure that you replace iptables with $IPTABLES, this
#way you will use the macro defined above.
echo "Setting up INPUT chains"
#Add your input and output chains below
```

Replace everything that is written within <>, then add your iptables commands after ‘Add your input and output chains below’.

To answer in your report For this task, present the following in your report:

- Include a screenshot of your IPTables-script
- Run `iptables --list` and include a screenshot of that output
- Explain what the purpose of enabling stateful packet inspection is.

5 Examination

Hand in a report containing all your solutions to the questions in Section 4 *Remember that you must include references to the given reading instructions, alternatively to the laboratory work you have done*

References

Bhushan, A. (1971). *File Transfer Protocol* (rfc No. 114). IETF. http://tools.ietf.org/rfc/rfc0114.txt

Nemeth, E., Snyder, G., Hein, T. R., Whaley, B., & Mackin, D. (2017). *Unix and linux system administration handbook* (Fifth edition.). Addison-Wesley/Pearson.

netfilter.org. (2023). Netfilter [Accessed: 2023-12-08]. http://www.netfilter.org

Postel, J., & Reynolds, J. (1985). *File Transfer Protocol* (rfc No. 959). IETF. http://tools.ietf.org/rfc/rfc0959.txt