VSIT | Vidyalankar School of Information Technology
NAAC Accredited College

LAB MANUAL

SUBJECT Linux Administration

YEAR : Third SEMESTER : V

ACADEMIC YEAR : 2019-2020

Practical : 1

1.Title: Graphical User Interface and Command Line Interface and Processes

2. Prior Concepts:

None

3. New Concepts:

GUI: In this activity, you will explore the GNOME graphical desktop interface. You will find where the essential elements of the GNOME desktop are located

CLI: Use of various commands to perform various tasks in your login

Processes: Execute various commands to manage processes.

4. Objectives:

1. Explore the GNOME Desktop Interface.
2. Identify essential elements in GNOME
3. Run various CLI commands
4. Identify and learn the commands to manage processes.

5. Procedure:

GUI:

- Log in to the graphical desktop as user "student."
- Change the password of user student to "password," using the tools available in the graphical desktop.
- Open a terminal window, and type ls to display files in the current directory.
- Use Nautilus to browse to the contents of the /etc directory. Can you open the files in this directory? Can you create new files in this directory?
- Configure your graphical desktop to have four available workspaces.
- Open the NetworkManager application, and find out the current IP address configuration in use on your computer.
- Use the graphical help system, and see what information you can find about changing a user's password.

CLI:

- Use man and man -k to find out how to change the current date on your computer. Set the date to yesterday.
- Create a directory with the name /tempdir. Copy all files from the /etc directory that start with an a, b, or c to this directory.
- Find out which command and which specific options you will need to show a time sorted list of the contents of the directory /etc.
- Create a file in your home directory, and fill it all with errors that are generated if you try to run the command grep -R root * from the /proc directory as an ordinary user. If necessary, refer to the man page of grep to find out how to use the command.
- Find all files on your server that have a size greater than 100 MB.
- Log in as root , and open two console windows in the graphical environment.
- From console window 1, run the following commands: cpuinfo, cat /etc/hosts, and w. From console window 2, use the following commands: ps aux, tail -n 10 /etc/passwd, and mail -s hello root < . Can you run the commands that you've entered in console window 1 from the histor y in console window 2? What do you need to do to update the histor y with the commands that you've used from both environments?

- Make a copy of the file /etc/passwd to your home directory. After copying it, rename the file ~/passwd to ~/users. Use the most efficient method to delete all lines in this file in which the third column has a number less than 500. Next, replace the text /bin/bash all throughout the file with the text /bin/false.

Processes:

- Start the command dd if=/dev/sda of=/dev/zero three times as a background job.
- Find the PID of the three dd processes you just started, and change the nice value of one of the processes to -5.
- Start the command dd if=/dev/zero of=/dev/sda as a foreground job. Next, use the appropriate procedure to put it in the background. Then verify that it indeed runs as a background job.
- Use the most efficient procedure to terminate all of the dd commands

6. Implementation :

GUI:

- In the login screen, click the login name "student" and type the password.
- In the upper-right corner you can see the name of the user who is currently logged in.
- Click this username to get access to different tools, such as the tool that allows you to change the password.
- Right-click the graphical desktop, and select Open in terminal. Next, type ls.
- On the graphical desktop, you'll find an icon representing your home folder. Click it and navigate to the /etc folder. You'll notice that as a normal user, you have limited access to this folder.
- Right-click a workspace icon, and select the number of workspaces you want to be displayed.
- Right-click the Network Manager icon in the upper-right corner of the desktop.
- Next, click Connection Information to display information about the current connection.
- Press F1 to show the help system. Type the keyword you want to search for and browse the results.

CLI:

- For instance, use man -k time | grep 8. You'll find the date command. Use date mmddhhmm to set the date.
- mkdir /tempdir, cp /etc/[abc]* /tempdir
- Use man ls. You'll find the -t option, which allows you to sort ls output on time.
- cd /proc; grep -R root * 2> ~/procerrors.txt
- find / -size +100M
- This doesn't work because the history file gets updated only when the shell is closed.
- cp /etc/passwd ~. mv ~/passwd ~/users

Processes:

- Run dd if=/dev/sda of=/dev/zero three times.
- Use ps aux | grep dd, and write down the PIDs. A useful addition to show just the PIDs and nothing else is found by piping the results of this command through awk '{ print $2}'. Next, use nice -5 $PID (where $PID is replaced by the PIDs you just found).
- To put a foreground job in the background, use the Ctrl+Z key sequence to pause the job. Next, use the bg command, which restarts the job in the background. Then use jobs to show a list of current jobs, including the one you just started.
- Use killall dd.

7. Results:

O/P of the program

8. Application:

Increase familiarity with GUI

9. Questions:

What is the purpose of the Applications Menu?

What is the ‘Places’ menu item?

What is the difference between Applications-> System Tools and System-> Administration?

What is the difference between a CLI and a GUI. Why is CLI used?

What are processes? Why do we have to change process priority?

Practical: 2

1.Title: Storage Devices and Links, Backup and Repository

2. Prior Concepts:

1. Types of storage devices
2. Types of links
3. Types of backup
4. Purpose of a repository

3. New Concepts:

- Creation of a symbolic and a hard link.
- Take backups in various forms.
- Creation of a repository

4. Objectives:

1. Understand creation of links
2. Learn how to take backups
3. Learn how to create a repository

5. Procedure:

Working with Storage Devices and Links

1. First use dmesg to find out the device name of the USB flash drive. Next, assuming that the name of the USB drive is /dev/sdb, use fdisk -cul to show the partitions on this device. It will probably show just one partition with the name /dev/sdb1. Mount it using mount /dev/sdb1 /mnt.

2. The link is ln -s /etc /tmp.

Making a Backup

1. Use tar czvf /tmp.tar /tmp. To verify the archive, use tar tvf /tmp.tar. You’ll see that the archive doesn’t contain the symbolic link.

2. This is the h option. Use tar czhvf /tmp.tar /tmp to create the archive.

3. Add the following to /etc/rsyslog.conf:

authpriv.info root.

Next, use service restart rsyslog to restart the syslog service.

4. Remove the /var/log/messages line from the /etc/logrotate.d/syslog file. Next, create a file with the name /etc/logrotate.d/messages, containing the following contents:

/var/log/messages

{

weekly

rotate 2

minsize 1M

}

Creating Repositories

1. Use mkdir /packages. Next, copy all RPMs from the installation DVD to this directory. Then install createrepo, using rpm -ivh createrepo[Tab] from the directory that contains the packages (assuming that createrepo hasn't yet been installed). If you get messages about dependencies, install them as well. Use createrepo /packages to mark the /packages directory as a repository.

2. Create a file with the name /etc/yum.repos.d/packages.repo, and make sure it has the following contents:

[packages]

name=packages

baseurl=file:///packages

gpgcheck=0

6. Implementation:

Procedure mentioned above implemented by students in CLI or by opening terminal in GUI, in the lab.

7. Results:

Students will observe the inodes for symbolic and hard links. They will see the tar files in their home directory. They will see the repository created in yum. This repository will be used when they use the yum command to install a package.

8. Application:

Real life application in system administration.

9. Questions

What is the difference between symbolic and hard links?

What is the difference between gzip and bzip2 formats?

What is a repository? From where does yum access a repository?

Practical: 3
1.Title: Working with RPMs, Storage and Networking

2. Prior Concepts:

1. Types of storage devices
2. Basic concepts of networking

3. New Concepts:

- Using a RPM
- Change network settings from static to dynamic and vice versa
- Create partitions on a storage device.

4. Objectives:

1. Understand how to use a RPM
2. Learn how to change network settings
3. Learn how to create partitions

5. Procedure:

Using Query Options

1. Use yum provides */winbind. This shows that winbind is in the samba-winbind package. Use yum install samba-winbind to install the package.

2. rpm -qc samba-winbind reveals after installation that the only configuration file is /etc/security/pam_winbind.conf.

Extracting Files from RPMs

1. Copy the samba-winbind-[version].rpm file to /tmp. From there, use rpm2cpio sambawinbind[

tab] | cpio -idmc to extract it. You can now copy it to its target destination.

Configuring and Managing Storage

1. Use dd if=/dev/zero of=/dev/sdb bs=1M count=10.

2. Use fdisk -cu /dev/sdb to create two partitions. The first needs to be of type 83, and the second needs to be type 8e. Use +500M twice when asked for the last cylinder you want to use.

3. Use pvcreate /dev/sdb2.

4. Use vgcreate vgroup /dev/sdb2.

5. Use lvcreate -n logvol1 -L 500M /dev/vgroup.

6. Use mkfs.ext4 /dev/vgroup/logvol1.

7. Use cryptsetup luksFormat /dev/sdb1.

8. Use cryptsetup luksOpen /dev/sdb1 cryptvol.

9. Use mkfs.ext4 /dev/mapper/cryptvol.

10. Add the following line to /etc/crypttab: cryptvol /dev/sdb1.

11. Add the following lines to /etc/fstab:

/dev/mapper/cryptvol /cryptvol ext4 defaults 1 2 and /dev/vgroup.logvol1 /logvol ext4 defaults 1 2

Connecting to the Network

1. Use ip addr show, ip route show, and cat /etc/resolv.conf.

2. Use ip addr add dev <yourdevicehere> 10.0.0.111/24.

3. Change the IPADDR line in /etc/sysconfig/network-scripts/yourinterface. The NetworkManager service picks up the changes automatically.

4. dig www.sandervanvugt.com will give you the answer.

5. Change the HOSTNAME parameter in /etc/sysconfig/network.

6. Modify the contents of /etc/ssh/sshd_config. Make sure these two lines are activated:

PermitRootLogin no and AllowUsers linda.

7. Use ssh-keygen to generate the public/private key pair. Next, copy the public key to the server from the client using ssh-copy-id server.

8. Modify the /etc/sysconfig/ssh_config file to include the line ForwardX11 yes.

9. Install tigervnc-server, and modify the /etc/sysconfig/vncservers file to include the lines VNCSERVERS=”1:linda” and VNCSERVERARGS[1]=”-geometry 800x600 -nolisten tcp -localhost”. Next, use su - linda to become user linda, and as linda use vncpasswd to set the VNC password and start the vncserver using service vncserver start.

10. Use vncviewer -via linda@server localhost:1. Make sure that an entry that defines the IP address for the server is included in /etc/hosts on the client.

6. Implementation:

Procedure mentioned above implemented by students in CLI or by opening terminal in GUI, in the lab.

7. Results:

Students will understand use of RPMs, managing storage, configuring network

8. Application:

Real life application in system administration.

9. Questions

How are files extracted using RPMs?

What is a logical volume?

What is a public/private key pair?

Practical: 4

1.Title: Working with Users, Groups, and Permissions

2. Prior Concepts:

1. Concept of user and group in linux
2. Basic and advanced permissions in linux

3. New Concepts:

- Creation, modification and deletion of users, groups
- Changing user permissions

4. Objectives:

1. Understand how to create, modify, delete users and groups
2. Learn how to change user permissions

5. Procedure:

1. Use useradd Bob Bill Susan Caroline to create the users. Don't forget to set the password for each of these users using the passwd command.

2. Use groupadd {support,sales} to create the groups.

3. Use mkdir -p /data/sales /data/support to create the directories.

4. Use chgrp sales /data/sales and chgrp support /data/support to set group ownership.

5. Use chown Caroline /data/sales and chown Isabelle /data/account to change user ownership.

6. Use chmod 3770 /data/* to set the appropriate permissions.

6. Implementation:

Procedure mentioned above implemented by students in CLI or by opening terminal in GUI, in the lab.

7. Results:

Students will understand use of various commands for user administration

8. Application:

Real life application in system administration.

9. Questions

What are the various advanced permissions for directories?

How can group ownership be changed?

Practical: 5
1.Title: Firewall and Cryptographic Services

2. Prior Concepts:

1. Meaning of firewall
2. Need of cryptographic services

3. New Concepts:

- iptables
- Cryptographic services

4. Objectives:

1. Understand how to modify iptables for setting up a firewall as per requirements
2. Learn how to generate encrypt decrypt files

5. Procedure:

Securing server with iptables

1. On the host computer, type iptables -L -v to display the current confi guration. The purpose of this instruction is to clear any current confi guration. Before doing that, however, it's good to know how your fi rewall is currently configured.

2. Type the following commands:

iptables -P INPUT ACCEPT, iptables -P OUTPUT ACCEPT, and iptables -P FORWARD ACCEPT. Now use iptables -F to flush all other rules.

3. At this point, there should be no firewall on the host computer. Use iptables -L -v to verify that the policy is set to ACCEPT for all three chains in the filter table. If this is the case, use service iptables save to w rite the current configuration to the configuration files. This ensures you'll keep this configuration, even after a reboot.

4. Repeat steps 1 to 3 on the vir tual machine.

5. Af ter clearing the fi rewall on the vir tual machine, you must test which services are offered from the virtual machine. Use ping to test whether you can still reach the virtual machine (for example, ping 192.168.100.176).

6. Next use yum install -y nmap on the host to install the nmap network scanner.

7. After installing it, use nmap, followed by the IP address of the virtual machine to scan available services on the virtual machine (for example, nmap 192.168.100.176). You should see that some services are offered.

8. At this point, it is time to star t configuring the firewall. Remember, everything you do from this moment on must be done on the virtual machine. The first thing to do is to set a policy for the three chains. To do this, type the following:

iptables -P INPUT DROP

iptables -P OUTPUT DROP

iptables -P FORWARD DROP

9. At this point, all traffic is blocked, so it's time to open your firewall and allow the traffic that you want to permit. Given that not even a ping to localhost (ping localhost) is going to work at this time, open the loopback interface first. Use the following code to accomplish this:

iptables -A INPUT -i lo -j ACCEPT

iptables -A OUTPUT -o lo -j ACCEPT

10. Now that localhost is working again, it's time to open the SSH port. To do this, enter the following command:

iptables -A INPUT -p tcp --dport 22 -j ACCEPT

Now try to open an SSH session from the host computer. You will see that it doesn't work. This is because your virtual machine is now confi gured to accept incoming SSH sessions, but it is not confi gured to send a reply to the originator of the SSH request. To open your virtual machine to also send a reply, use the following command:

iptables -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

11. Now that SSH is open, you'll still need to open the HTTP por t. To do this, use the following command:

iptables -A INPUT -p tcp --dport 80 -j ACCEPT

By using this command, you should now be able to reach the web server on the virtual host. No additional action is required because you've already configured a rule that allows all answers to be returned to the originator of the request.

12. Now is a nice moment to check the current configuration. To do this, type iptables -L -v

Ensure that the OUTPUT chain is set to send packets to DNS, HTTP, and SSH. These lines do that for you:

iptables -A OUTPUT -p tcp --dport 22 -j ACCEPT

iptables -A OUTPUT -p tcp --dport 53 -j ACCEPT

iptables -A OUTPUT -p tcp --dport 80 -j ACCEPT

iptables -A OUTPUT -p tcp --dport 21 -j ACCEPT

Just opening these ports in the output chain is not enough, however. You need to make sure that answers can also get back. To do this, use the following command:

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT

Now save the configuration to make it persistent.

service iptables restart

Setting Up Cryptographic Services

1. You can easily perform this exercise by using the genkey command. Just be sure you indicate the amount of days you want the certificate to be valid (the default value is set to one month only), and include the FQDN of the server for which you are creating the certificate.

2. Start by using the gpg --gen-key command for both users. Next, have both users export their key using gpg --export > mykey. Then have both users import each other's keys by using gpg --import < mykey. Use gpg --list-keys to verify that the keys are visible.

3. You can now create the encrypted fi le using gpg -e secret.txt. Type the name of the other user to whom you want to send the encrypted fi le. As the other user, use gpg -d secret.txt to decrypt the fi le.

6. Implementation:

Procedure mentioned above implemented by students in CLI or by opening terminal in GUI, in the lab.

7. Results:

Students will understand use of modifying iptables for firewall configuration and encryption and decryption of files between users.

8. Application:

Real life application in system administration.

9. Questions

What are iptables?

What are the different chains and policies in firewall configuration?

How can one user decrypt a file that has been encrypted by another?

Practical: 6

1.Title: Configuring Server for File Sharing

2. Prior Concepts:

1. Meaning of NFS, SMB, FTP
2. SMB emulation using Samba

3. New Concepts:

- Exporting a share
- Sharing of files using FTP
- Use of Samba for file sharing between Linux and Windows

4. Objectives:

1. Understand how to export and mount a share in NFS
2. Learn how to share files using FTP
3. Learn how to share files between Linux server and Windows client using Samba

5. Procedure:

Sharing using NFS

1. Make sure the directory you want to create exists in the file system, and copy some random files to it. Next, create the file /etc/exports, and put in the following line:

/nfsfiles 192.168.1.70(rw)

Use service nfs start to start the NFS server, and use chkconfig nfs on to enable it.

Use showmount -e localhost to verify that it is available.

2. On the host, edit /etc/auto.master and make sure it includes the following line:

/mnt/nfs /etc/auto.nfs

Create the file /etc/auto.nfs, and give it the following contents:

* -rw 192.168.1.70/nfsfiles

Access the directory /mnt/nfs, and type ls to verify that it works.

Sharing using FTP

1. Install vsftpd. Create a directory /var/ftp/upload, and make sure the user and group owners are set to ftp.ftp. Set the permission mode on this directory to 730. Use semanage to label this directory with public_content_rw_t, and use setsebool -P allow_ftpd_anon_write on. Next, include the following parameters in /etc/vsftpd/vsftpd.conf:

anon_upload_enable = YES

chown_uploads = YES

chown_username = daemon

To get your traffi c through the firewall, edit the /etc/sysconfig/iptables_config file to include the following line:

IPTABLES_MODULES=”nf_conntrack_ftp nf_nat_ftp”

Add the following lines to the fi rewall confi guration, and after adding these lines, use service iptables save to make the new rules persistent:

iptables -A INPUT -p tcp --dport 21 -j ALLOW

iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ALLOW

Sharing using Samba

1. Use mkdir /data to create the data directory, and put some files in there. Make a Linux group sambausers, make this group owner of the directory /data, and give it rwx permissions. Install the samba and samba-common packages and edit the /etc/ samba/smb.conf file to include the following minimal share configuration:

[sambadata]

path = /data

writable = yes

Set the SELinux context type to public_content_t on the /data directory, and then use smbpasswd -a to create Samba users linda and lisa. They can now access the Samba server.

6. Implementation:

Procedure mentioned above implemented by students in CLI or by opening terminal in GUI, in the lab.

7. Results:

Students will understand file sharing between linux server and client and a linux server and windows client.

8. Application:

Real life application in system administration.

9. Questions

What is the difference between NFS and Samba?

What is anonymous user in FTP?

Practical: 7
1.Title: DNS, DHCP, Mail Server

2. Prior Concepts:

1. Name Resolution
2. Dynamic allocation of IP addresses
3. Working of email

3. New Concepts:

- Configuration of Primary DNS and zone
- Configuration of DHCP
- Configuration of Mail Server

4. Objectives:

1. Understand configuration of Primary DNS
2. Learn how to assign IP addresses dynamically using DHCP
3. Configuration of Mail server

5. Procedure:

DNS, DHCP

1. In /etc/named.rfc1912.zones, create a zone declaration. It should appear as follows

on the master server:

zone "example.com" IN {

type master;

file "example.com";

notify yes;

allow-update { IP-OF-YOUR-SLAVE };

};

On the slave server, also create a zone declaration in /etc/named.rfc19212.zones that

looks like the following:

zone "example.com" IN {

type slave;

masters {

192.168.1.220;

};

file "example.com.slave";

};

2. Use ifconfig to find out the MAC address in use on your second virtual machine. Configure a DHCP server that assigns the IP address 192.168.100.2 to this second virtual machine. Run this DHCP server on the first virtual machine. You can modify the configuration of your current DHCP server to accomplish this task.

3. The example assumes that there is an entry in DNS for the host that can be used to assign the IP address.

host yourhost {

hardware ethernet aa:bb:cc:00:11:22;

fixed-address yourhost.example.com;

}

Mail Server

1. Edit /etc/resolv.conf on both your host and your virtual machines. Set the domain and search parameters to the appropriate domains and, in the nameserver field, put the IP address of the host computer.

2. On the host computer, create a DNS configuration that identifies the host and the virtual machine as the mail exchange for their domains.

3. On both hosts, edit /etc/postfix/main.cf. First make sure that inet_interfaces is set to all. Next change the myorigin parameter to the local domain name.

4. Install Dovecot on both servers, and edit the protocols line so that only POP3 is offered. Run /usr/libexec/dovecot/mkcert.sh to create self-signed certificates, and install them to the appropriate locations.

5. In Mutt, press m to compose a mail message. On the other server, use c to change the mailbox to which you want to connect. Enter the URL pop://testvm.example.local to access POP on the testvm computer, and verify that the message has been received.

6. In addition, make sure that the firewall, if activated, has been adjusted. Ports 143, 993, 110, and 995 need to be open for POP and IMAP to work.

7. To identify the mail server for your domain, you'll also need to set up DNS. Create a zone file containing the following to do this:

[root@rhev named]# cat example.com

$TTL 86400

$ORIGIN example.com.

@ 1D IN SOA rhev.example.com. hostmaster.example.

com. (

20120822

3H ; refresh

15 ; retry

1W ; expire

3h ; minimum

)

IN NS rhev.example.com.

rhev IN A 192.168.1.220

rhevh IN A 192.168.1.151

rhevh1 IN A 192.168.1.221

blah IN A 192.168.1.1

router IN CNAME blah

IN MX 10 blah.example.com.

IN MX 20 blah.provider.com.

6. Implementation:

Procedure mentioned above implemented by students in CLI or by opening terminal in GUI, in the lab.

7. Results:

Students will understand how to configure DNS, DHCP, and Mail Server

8. Application:

Real life application in system administration.

9. Questions

What is DNS? What are DNS records in zone file?

What is a DHCP conversation?

Practical: 8
1.Title: Web Server

2. Prior Concepts:

4. What is a web server?

3. New Concepts:

- Virtual hosts using Apache
- Shell script to monitor Apache activity
- Using select command

4. Objectives:

4. Understand how create virtual hosts in Apache
5. Learn how to write script to monitor Apache activity

5. Procedure:

Configure Apache

Make sure to perform the following tasks:

1. After creating the directories, use semanage fcontext -a -t httpd_sys_content_t "/web(/.*)" followed by restorecon -r /web. This ensures that SELinux allows access to the nondefault document roots.

2. Use an editor to create a file index.html in the appropriate document roots.

3. In /etc/httpd/conf.d, create a configuration file for each of the virtual hosts. Make sure that at least the following directives are used in these files:

<VirtualHost *:80>

ServerAdmin webmaster@server1.example.com

DocumentRoot /www/docs/server1.example.com

ServerName server1.example.com

ErrorLog logs/server1/example.com-error_log

CustomLog logs/server1.example.com-access_log common

</VirtualHost>

4. Put the following lines in the virtual host configuration for the accounting server:

order deny,allow

allow from 192.168

deny from all

5. Use htpasswd -cm /etc/httpd/.htpasswd leo and htpasswd -m /etc/httpd/.

htpasswd linda to create the user accounts. Next, include the following code block in the sales virtual server configuration file:

<Directory />

AuthName Authorized Use Only

AuthType basic

AuthUserFile /etc/httpd/.htpasswd

Require valid-user

</Directory>

Writing a Script to Monitor Activity on the Apache Web Server

#!/bin/bash

#

Monitoring process httpd

```
#
COUNTER=0
while ps aux | grep httpd | grep -v grep > /dev/null
do
COUNTER=$((COUNTER+1))
sleep 1
echo COUNTER is $COUNTER
done
logger HTTPMONITOR: httpd stopped at `date`
/etc/init.d/apache2 start
mail -s Apache server just stopped root < .
```

Using the select Command

```
#!/bin/bash
#
# RPM research: query the RPM database
echo ‘Enter the name of an RPM or file’
read RPM
echo ‘select a task from the menu’
select TASK in ‘Check from which RPM this file comes’ ‘Check if
this RPM is installed’ ‘Install this RPM’ ‘Remove this RPM’
do
case $REPLY in
1) TASK=”rpm -qf $RPM”;;
2) TASK=”rpm -qa | grep $RPM”;;
3) TASK=”rpm -ivh $RPM”;;
4) TASK=”rpm -e $RPM;;
*) echo error && exit 1;;
esac
if [ -n "TASK" ]
```

then

clear

echo you have selected TASK

$TASK

break

else

echo invalid choice

fi

done

6. Implementation:

Procedure mentioned above implemented by students in CLI or by opening terminal in GUI, in the lab.

7. Results:

Students will understand how to create virtual hosts and write script to monitor Apache

8. Application:

Real life application in system administration.

9. Questions

What are virtual hosts? Name the corresponding files

What is a shell script? How does a shell script help the system administrator?