

## SECTION 11      Manage Network Services: NIS, Mail, xinetd

In this section of the workbook, you learn how to do the following:

- “Enable Network Information Service (NIS) on Your Network” on 11-1
- “Send Mail to root” on 11-9
- “Configure the Internet Daemon (xinetd) and TCP Wrapper” on 11-10

### ***Exercise 11-1      Enable Network Information Service (NIS) on Your Network***

Within a network of any size it is not possible to keep the user accounts locally. This is just not manageable, as it means one has to add and delete users on every single workstation.

NIS is a solution for this that exists already for some time. While it is still workable, it should be replaced by LDAP where possible to avoid certain security issues inherent in NIS.

The purpose of this exercise is to walk you through the steps necessary to set up NIS.

In this exercise, you do the following:

- [Part I: Configure an NIS Server with YaST](#)
- [Part II: Create an NIS User](#)
- [Part III: Update the NIS Maps](#)
- [Part IV: Verify a Local NIS Configuration](#)

You need to complete this exercise to complete the rest of the exercises in this course.

## SECTION 11      Manage Network Services: NIS, Mail, xinetd

In this section of the workbook, you learn how to do the following:

- “Enable Network Information Service (NIS) on Your Network” on 11-1
- “Send Mail to root” on 11-9
- “Configure the Internet Daemon (xinetd) and TCP Wrapper” on 11-10

### ***Exercise 11-1      Enable Network Information Service (NIS) on Your Network***

Within a network of any size it is not possible to keep the user accounts locally. This is just not manageable, as it means one has to add and delete users on every single workstation.

NIS is a solution for this that exists already for some time. While it is still workable, it should be replaced by LDAP where possible to avoid certain security issues inherent in NIS.

The purpose of this exercise is to walk you through the steps necessary to set up NIS.

In this exercise, you do the following:

- [Part I: Configure an NIS Server with YaST](#)
- [Part II: Create an NIS User](#)
- [Part III: Update the NIS Maps](#)
- [Part IV: Verify a Local NIS Configuration](#)

You need to complete this exercise to complete the rest of the exercises in this course.

You can configure the NIS Server on the da10 and the client on the da1 VMWare machine.

- [Part V: Prepare for NIS Network Users](#)
- [Part VI: Configure the NIS Client Using YaST](#)

In this exercise, you work with a partner with one of your computers acting as the NIS server and the other as the NIS client.



---

For this exercise to work properly, all the steps need to be done in sequence. For example, in Part V complete the steps on the NFS server computer before completing the steps on the NFS client computer.

---

### Part I: Configure an NIS Server with YaST

From the NIS server computer, do the following:

1. From the KDE desktop, select the **YaST** icon; then enter a password of **novell** and select **OK**.  
The YaST Control Center appears.
2. Select **Network Services > NIS Server**.  
The Network Information Service (NIS) Server Setup dialog appears.
3. Select **Create NIS Master Server**; then continue by selecting **Next**.  
The Master Server Setup dialog appears.
4. In the NIS Domain Name field enter **NIS-DAxx** (where **xx** is the host number of your server).  
For example, if your server hostname is DA50, you would enter **NIS-DA50**.
5. Select the following options:
  - This Host Is Also a NIS Client**
  - Fast Map Distribution (rpc.ypxfrd)**
  - Allow Changes to Passwords**

You can configure the NIS Server on the da10 and the client on the da1 VMWare machine.

- [Part V: Prepare for NIS Network Users](#)
- [Part VI: Configure the NIS Client Using YaST](#)

In this exercise, you work with a partner with one of your computers acting as the NIS server and the other as the NIS client.



---

For this exercise to work properly, all the steps need to be done in sequence. For example, in Part V complete the steps on the NFS server computer before completing the steps on the NFS client computer.

---

### Part I: Configure an NIS Server with YaST

From the NIS server computer, do the following:

1. From the KDE desktop, select the **YaST** icon; then enter a password of **novell** and select **OK**.  
The YaST Control Center appears.
2. Select **Network Services > NIS Server**.  
The Network Information Service (NIS) Server Setup dialog appears.
3. Select **Create NIS Master Server**; then continue by selecting **Next**.  
The Master Server Setup dialog appears.
4. In the NIS Domain Name field enter **NIS-DAxx** (where **xx** is the host number of your server).  
For example, if your server hostname is DA50, you would enter **NIS-DA50**.
5. Select the following options:
  - This Host Is Also a NIS Client**
  - Fast Map Distribution (rpc.ypxfrd)**
  - Allow Changes to Passwords**

- ❑ **Allow Changes to GECOS Field**
  - ❑ **Allow Changes to Login Shell**
6. Continue by selecting **Next**.  
An NIS Server Maps Setup dialog appears.
  7. From the list of server maps, deselect **netid**; then make sure that **group**, **passwd**, **rpc**, and **services** are selected.
  8. Continue by selecting **Next**.  
The NIS Server Query Hosts Setup dialog appears.
  9. Accept the default settings and complete the NIS server setup by selecting **Finish**.

## Part II: Create an NIS User

Before testing the NIS configuration, you need to create an NIS user on the computer where the NIS server is configured.

From the NIS server computer, do the following:

1. From a terminal window, su to root (**su -**) with a password of **novell**.
2. Create the directory `/export/nis-xx/home` for NIS network users by entering the following:  
**mkdir -p /export/nis-xx/home**  
(where **xx** is the host number of your server)
3. From the YaST Control Center, select **Security and Users > Edit and create users**.  
The User and Group Administration dialog appears.
4. Select **Set Filter**; then select **NIS Users**.

Notice that when you create new users they are added as NIS users by default.

- ❑ **Allow Changes to GECOS Field**
  - ❑ **Allow Changes to Login Shell**
6. Continue by selecting **Next**.  
An NIS Server Maps Setup dialog appears.
  7. From the list of server maps, deselect **netid**; then make sure that **group**, **passwd**, **rpc**, and **services** are selected.
  8. Continue by selecting **Next**.  
The NIS Server Query Hosts Setup dialog appears.
  9. Accept the default settings and complete the NIS server setup by selecting **Finish**.

## Part II: Create an NIS User

Before testing the NIS configuration, you need to create an NIS user on the computer where the NIS server is configured.

From the NIS server computer, do the following:

1. From a terminal window, su to root (**su -**) with a password of **novell**.
2. Create the directory `/export/nis-xx/home` for NIS network users by entering the following:  
**mkdir -p /export/nis-xx/home**  
(where **xx** is the host number of your server)
3. From the YaST Control Center, select **Security and Users > Edit and create users**.  
The User and Group Administration dialog appears.
4. Select **Set Filter**; then select **NIS Users**.

Notice that when you create new users they are added as NIS users by default.

5. Select **Set Filter**; then select **Local Users**.
6. Create a new user by selecting **Add**.  
The Add a New Local User dialog appears.
7. Enter the following (where **xx** is the host number of your server):
  - ❑ Full User Name: **dbaxx**
  - ❑ User Login: **dbaxx**
  - ❑ Password: **N0v3ll**
  - ❑ Verify password: **N0v3ll**
8. Select **Details**.  
A Details dialog appears.
9. In the Home Directory field, enter  
**/export/nis-xx/home/dbaxx**  
Then select **Next**.
10. Continue by selecting **Create**.  
Notice that the user **dbaxx** is listed with the other users.
11. Select **Set Filter**; then select **NIS Users**.  
The maps have not been updated, so the user **dbaxx** is not listed as an NIS user.
12. Save the changes by selecting **Finish**.
13. From the terminal window, enter  
**ls -l /export/nis-xx/home/**  
Check to make sure that the owner of the directory **dbaxx** is the user **dbaxx**.
14. (Conditional) If **dbaxx** is not the owner, then enter  
**chown -R dbaxx.users /export/nis-xx/home/dbaxx**

5. Select **Set Filter**; then select **Local Users**.
6. Create a new user by selecting **Add**.  
The Add a New Local User dialog appears.
7. Enter the following (where **xx** is the host number of your server):
  - Full User Name: **dbaxx**
  - User Login: **dbaxx**
  - Password: **N0v3ll**
  - Verify password: **N0v3ll**
8. Select **Details**.  
A Details dialog appears.
9. In the Home Directory field, enter  
**/export/nis-xx/home/dbaxx**  
Then select **Next**.
10. Continue by selecting **Create**.  
Notice that the user **dbaxx** is listed with the other users.
11. Select **Set Filter**; then select **NIS Users**.  
The maps have not been updated, so the user **dbaxx** is not listed as an NIS user.
12. Save the changes by selecting **Finish**.
13. From the terminal window, enter  
**ls -l /export/nis-xx/home/**  
Check to make sure that the owner of the directory **dbaxx** is the user **dbaxx**.
14. (Conditional) If **dbaxx** is not the owner, then enter  
**chown -R dbaxx.users /export/nis-xx/home/dbaxx**

### Part III: Update the NIS Maps

From the NIS server computer, update the NIS maps by doing the following:

1. From the terminal window, make sure that the yp services are running by entering  
**rcypserv restart**
2. Change to the directory /var/yp by entering **cd /var/yp**.
3. Update the NIS maps by entering **make**.

### Part IV: Verify a Local NIS Configuration

From the NIS server computer, do the following:

1. Switch to a virtual console by entering **Ctrl + Alt + F2**.
2. Log in as **dbarx** with a password of **N0v3ll**.  
You are now ready to test the configuration.
3. Check the NIS domain by entering **domainname**.  
You see NIS-DAxx listed.
4. Change the GECOS field by entering **chfn**; then enter a password of **N0v3ll**.
5. Enter the following values:
  - Room Number: **Classroom**
  - Work Phone: **555-1212**
  - Home Phone: **444-1212**
6. Su to root (**su -**) with a password of **novell**.
7. Update the NIS maps by changing to the directory /var/yp (**cd /var/yp**) and entering **make**.
8. Verify that the NIS map was updated by entering

If your VMWare host is a Linux machine, press Ctrl + Alt and hold them. Then press Space, and then, while still holding Ctrl + Alt down, press F2. Otherwise your host will switch to console 2, not the guest.

### Part III: Update the NIS Maps

From the NIS server computer, update the NIS maps by doing the following:

1. From the terminal window, make sure that the yp services are running by entering  
**rcypserv restart**
2. Change to the directory /var/yp by entering **cd /var/yp**.
3. Update the NIS maps by entering **make**.

### Part IV: Verify a Local NIS Configuration

From the NIS server computer, do the following:

1. Switch to a virtual console by entering **Ctrl + Alt + F2**.
2. Log in as **dbarx** with a password of **N0v3ll**.  
You are now ready to test the configuration.
3. Check the NIS domain by entering **domainname**.  
You see NIS-DAxx listed.
4. Change the GECOS field by entering **chfn**; then enter a password of **N0v3ll**.
5. Enter the following values:
  - Room Number: **Classroom**
  - Work Phone: **555-1212**
  - Home Phone: **444-1212**
6. Su to root (**su -**) with a password of **novell**.
7. Update the NIS maps by changing to the directory /var/yp (**cd /var/yp**) and entering **make**.
8. Verify that the NIS map was updated by entering

If your VMWare host is a Linux machine, press Ctrl + Alt and hold them. Then press Space, and then, while still holding Ctrl + Alt down, press F2. Otherwise your host will switch to console 2, not the guest.

### **ypcat passwd**

9. Return to the KDE desktop by pressing **Ctrl + Alt + F7**.

## **Part V: Prepare for NIS Network Users**

An NIS user needs a home directory on the NIS client computer.

In this part of the exercise, you work with a partner to create an NFS export of the NIS home directory path and then mount this exported file system on the NIS client computer.

On the NIS server computer, do the following:

1. Configure the directory `/export/nis-xx` as an NFS export:
  - a. From the YaST Control Center, configure the NFS server by selecting **Network Services > NFS Server**.  
A Configuration of the NFS server dialog appears.
  - b. Make sure **Start NFS Server** is selected; then continue by selecting **Next**.  
A Directories to export to the others dialog appears.
  - c. Select **Add Directory**.  
A dialog appears requesting the directory to export.
  - d. Browse to and select or enter `/export/nis-xx/`; then select **OK**.  
A dialog appears with fields for entering a wildcard and options.
  - e. Enter the following:
    - Hosts wildcard: **\***
    - Options: **rw,no\_root\_squash,sync**Make sure you replace the “ro” with “rw” or you will not be able to log in remotely to the KDE desktop as `dbaxx`.
  - f. Continue by selecting **OK**.

### **ypcat passwd**

9. Return to the KDE desktop by pressing **Ctrl + Alt + F7**.

## **Part V: Prepare for NIS Network Users**

An NIS user needs a home directory on the NIS client computer.

In this part of the exercise, you work with a partner to create an NFS export of the NIS home directory path and then mount this exported file system on the NIS client computer.

On the NIS server computer, do the following:

1. Configure the directory `/export/nis-xx` as an NFS export:
  - a. From the YaST Control Center, configure the NFS server by selecting **Network Services > NFS Server**.  
A Configuration of the NFS server dialog appears.
  - b. Make sure **Start NFS Server** is selected; then continue by selecting **Next**.  
A Directories to export to the others dialog appears.
  - c. Select **Add Directory**.  
A dialog appears requesting the directory to export.
  - d. Browse to and select or enter `/export/nis-xx/`; then select **OK**.  
A dialog appears with fields for entering a wildcard and options.
  - e. Enter the following:
    - Hosts wildcard: **\***
    - Options: **rw,no\_root\_squash,sync**Make sure you replace the “ro” with “rw” or you will not be able to log in remotely to the KDE desktop as `dbaxx`.
  - f. Continue by selecting **OK**.

The directory is added to the list.

- g. Save the changes to the system by selecting **Finish**.
  - h. From the terminal window, verify that the file system was exported by entering  
**showmount -e localhost**
  - i. View the entry made by YaST to the file `/etc/exports` by entering **cat /etc/exports**.
2. On the NIS client computer, do the following:
- a. From a terminal window, su to root (**su -**) with a password of **novell**.
  - b. Create a directory `/export/nis-xx` (where *xx* is the host number of the NIS server computer) by entering  
**mkdir -p /export/nis-xx**  
For example if your NIS server is DA50, you would enter  
**mkdir -p /export/nis-50**
  - c. From the KDE desktop, select the **YaST** icon; then enter a password of **novell** and select **OK**.  
The YaST Control Center appears.
  - d. From the YaST Control Center, select  
**Network Services > NFS Client**  
The Configuration of the NFS client dialog appears.
  - e. Mount a remote file system by selecting **Add**.  
A dialog appears for adding the remote file system.
  - f. Enter the following:
    - Host name of the NFS Server: **10.0.0.rr** (where *rr* is the host number of the NIS server computer)
    - Remote filesystem: **/export/nis-xx**
    - Mountpoint (local): **/export/nis-xx/** (where *rr* is the host number of the remote NFS server)
    - Options field: **defaults,rsize=8192,wsz=8192,soft**

The directory is added to the list.

- g. Save the changes to the system by selecting **Finish**.
  - h. From the terminal window, verify that the file system was exported by entering  
**showmount -e localhost**
  - i. View the entry made by YaST to the file `/etc/exports` by entering **cat /etc/exports**.
2. On the NIS client computer, do the following:
- a. From a terminal window, su to root (**su -**) with a password of **novell**.
  - b. Create a directory `/export/nis-xx` (where *xx* is the host number of the NIS server computer) by entering  
**mkdir -p /export/nis-xx**  
For example if your NIS server is DA50, you would enter  
**mkdir -p /export/nis-50**
  - c. From the KDE desktop, select the **YaST** icon; then enter a password of **novell** and select **OK**.  
The YaST Control Center appears.
  - d. From the YaST Control Center, select  
**Network Services > NFS Client**  
The Configuration of the NFS client dialog appears.
  - e. Mount a remote file system by selecting **Add**.  
A dialog appears for adding the remote file system.
  - f. Enter the following:
    - Host name of the NFS Server: **10.0.0.rr** (where *rr* is the host number of the NIS server computer)
    - Remote filesystem: **/export/nis-xx**
    - Mountpoint (local): **/export/nis-xx/** (where *rr* is the host number of the remote NFS server)
    - Options field: **defaults,rsize=8192,wsz=8192,soft**

- g. Save the configuration by selecting **OK**.  
You are returned to the Configuration of the NFS client dialog where the remote file system is listed.
- h. Save the changes to the system by selecting **Finish**.
- i. From the terminal window, verify that the file system is mounted by entering **mount**.
- j. Verify that an entry exists in /etc/fstab by entering  
**cat /etc/fstab**

## Part VI: Configure the NIS Client Using YaST

From the NIS client computer, do the following:

1. From the YaST Control Center, select  
**Network Services > NIS Client**  
The Configuration of NIS Client dialog appears.
2. Make sure **Use NIS** is selected.
3. In the NIS domain field, enter **NIS-D $rr$**  (where  **$rr$**  is the host number of your NIS server computer).
4. In the Addresses of NIS servers field, enter **10.0.0. $rr$**  (where  **$rr$**  is the host number of your NIS server computer).
5. Save the changes to the system by selecting **Finish**.
6. Test the NIS remote access:
  - a. Log out of the KDE desktop by selecting  
**KDE Menu > Logout > Logout**  
The GUI login screen appears.  
Scroll through the list of users and notice that the **db $axx$**  user appears, even though it is not a local user account.
  - b. Log in as the user **db $axx$**  with a password of **N0v3ll**.

If you are experiencing problems logging in to the KDE desktop, make sure that /export/nis- $xx$  is set to rw instead of ro, and that db $axx$  is the owner of the home directory.

- g. Save the configuration by selecting **OK**.  
You are returned to the Configuration of the NFS client dialog where the remote file system is listed.
- h. Save the changes to the system by selecting **Finish**.
- i. From the terminal window, verify that the file system is mounted by entering **mount**.
- j. Verify that an entry exists in /etc/fstab by entering  
**cat /etc/fstab**

## Part VI: Configure the NIS Client Using YaST

From the NIS client computer, do the following:

1. From the YaST Control Center, select  
**Network Services > NIS Client**  
The Configuration of NIS Client dialog appears.
2. Make sure **Use NIS** is selected.
3. In the NIS domain field, enter **NIS-D $rr$**  (where  **$rr$**  is the host number of your NIS server computer).
4. In the Addresses of NIS servers field, enter **10.0.0. $rr$**  (where  **$rr$**  is the host number of your NIS server computer).
5. Save the changes to the system by selecting **Finish**.
6. Test the NIS remote access:
  - a. Log out of the KDE desktop by selecting  
**KDE Menu > Logout > Logout**  
The GUI login screen appears.  
Scroll through the list of users and notice that the **db $axx$**  user appears, even though it is not a local user account.
  - b. Log in as the user **db $axx$**  with a password of **N0v3ll**.

If you are experiencing problems logging in to the KDE desktop, make sure that /export/nis- $xx$  is set to rw instead of ro, and that db $axx$  is the owner of the home directory.

- c. When you finish, log out as **dbaxx**; then log back in as **geeko**.

*(End of Exercise)*

### **Exercise 11-2 Send Mail to root**

Sometimes a very simple mail client is all you need. The purpose of this exercise is to introduce you to the program mail for this purpose.

To send mail to root, do the following:

1. Open a terminal window.
2. Enter **mail root**.
3. Enter the subject **My first e-mail with mail**.
4. Enter the following three lines of text (press **Enter** after each line):

**I have just installed SLES 9  
on my computer and I'm ready  
for administration training.**

5. To finish, enter a single dot in a new line and press **Enter**.
6. Su to root by entering **su -**; then enter a password of **novell**.
7. Enter **mail**.

In the last line of the list you should find the mail message you just sent to root.

8. To read the message, enter the **number** in the second column of the table and press **Enter**.
9. Delete the message by entering **d** and the **number** of the message (such as **d 4**).
10. Quit mail by entering **q**.

- c. When you finish, log out as **dbarr**; then log back in as **geeko**.

*(End of Exercise)*

### **Exercise 11-2 Send Mail to root**

Sometimes a very simple mail client is all you need. The purpose of this exercise is to introduce you to the program mail for this purpose.

To send mail to root, do the following:

1. Open a terminal window.
2. Enter **mail root**.
3. Enter the subject **My first e-mail with mail**.
4. Enter the following three lines of text (press **Enter** after each line):

**I have just installed SLES 9  
on my computer and I'm ready  
for administration training.**

5. To finish, enter a single dot in a new line and press **Enter**.
6. Su to root by entering **su -**; then enter a password of **novell**.
7. Enter **mail**.

In the last line of the list you should find the mail message you just sent to root.

8. To read the message, enter the **number** in the second column of the table and press **Enter**.
9. Delete the message by entering **d** and the **number** of the message (such as **d 4**).
10. Quit mail by entering **q**.

11. Verify that the message was deleted by entering **mail**; then exit mail by entering **q**.
12. Log out as root by entering **exit**.
13. Close the terminal window.

*(End of Exercise)*

### **Exercise 11-3    Configure the Internet Daemon (xinetd) and TCP Wrapper**

Various services can be offered via inetd/xinetd. In both cases additional fine tuning of access restrictions is possible using the TCP wrapper and the files `/etc/hosts.allow` and `/etc/hosts.deny`.

The purpose of this exercise is to show you the basic configuration steps necessary to offer services using xinetd.

In this exercise, you do the following:

- [Part I: Enable xinetd Services with YaST](#)
- [Part II: Enable xinetd Services Manually](#)
- [Part III: Configure TCP Wrapper](#)

#### **Part I: Enable xinetd Services with YaST**

Do the following:

1. From your KDE desktop, select the **YaST** icon; then enter a password of **novell** and select **OK**.  
The YaST Control Center appears.
2. Select **Network Services > Network Services (inetd)**.  
The Network Services Configuration (xinetd) dialog appears.
3. Select **Enable**.

11. Verify that the message was deleted by entering **mail**; then exit mail by entering **q**.
12. Log out as root by entering **exit**.
13. Close the terminal window.

*(End of Exercise)*

### **Exercise 11-3    Configure the Internet Daemon (xinetd) and TCP Wrapper**

Various services can be offered via inetd/xinetd. In both cases additional fine tuning of access restrictions is possible using the TCP wrapper and the files `/etc/hosts.allow` and `/etc/hosts.deny`.

The purpose of this exercise is to show you the basic configuration steps necessary to offer services using xinetd.

In this exercise, you do the following:

- [Part I: Enable xinetd Services with YaST](#)
- [Part II: Enable xinetd Services Manually](#)
- [Part III: Configure TCP Wrapper](#)

#### **Part I: Enable xinetd Services with YaST**

Do the following:

1. From your KDE desktop, select the **YaST** icon; then enter a password of **novell** and select **OK**.  
The YaST Control Center appears.
2. Select **Network Services > Network Services (inetd)**.  
The Network Services Configuration (xinetd) dialog appears.
3. Select **Enable**.

A list of currently available services becomes active.

4. Scroll down and select the service **Telnet**; then set the service to On by selecting **Toggle Status (On or Off)**.
5. Save the configuration to the system by selecting **Finish**.
6. Test the configuration:
  - a. Open a terminal window and su to root (**su -**) with a password of **novell**.
  - b. Telnet to localhost by entering **telnet localhost**.
  - c. Log in as **geeko** with a password of **N0v3ll**.
  - d. Log out by entering **exit**.
  - e. Log in to a partner's server as geeko by entering **telnet partner\_server\_IP\_address**  
You'll need to wait until the neighbor completes enabling inetd and Telnet.
  - f. Log out by entering **exit**.

To do step e., you will have to configure xinetd as given in this exercise on the VMWare machine da1.

## Part II: Enable xinetd Services Manually

Enable the FTP server by doing the following:

1. From the terminal window, edit the file `/etc/xinetd.d/vsftpd` by entering  
**vim /etc/xinetd.d/vsftpd**
2. At the bottom of the file, change the `disable = yes` setting to the following:  
`disable = no`
3. Exit vi and save the changes by entering **:wq**.
4. Restart the service xinetd by entering **rcxinetd restart**.
5. Test the FTP service by doing the following:

A list of currently available services becomes active.

4. Scroll down and select the service **Telnet**; then set the service to On by selecting **Toggle Status (On or Off)**.
5. Save the configuration to the system by selecting **Finish**.
6. Test the configuration:
  - a. Open a terminal window and su to root (**su -**) with a password of **novell**.
  - b. Telnet to localhost by entering **telnet localhost**.
  - c. Log in as **geeko** with a password of **N0v3ll**.
  - d. Log out by entering **exit**.
  - e. Log in to a partner's server as geeko by entering **telnet partner\_server\_IP\_address**  
You'll need to wait until the neighbor completes enabling inetd and Telnet.
  - f. Log out by entering **exit**.

To do step e., you will have to configure xinetd as given in this exercise on the VMWare machine da1.

## Part II: Enable xinetd Services Manually

Enable the FTP server by doing the following:

1. From the terminal window, edit the file `/etc/xinetd.d/vsftpd` by entering  
**vim /etc/xinetd.d/vsftpd**
2. At the bottom of the file, change the `disable = yes` setting to the following:  
`disable = no`
3. Exit vi and save the changes by entering **:wq**.
4. Restart the service xinetd by entering **rcxinetd restart**.
5. Test the FTP service by doing the following:

To do step d., you will have to configure vsftpd as given in this exercise on the VMWare machine da1.

- a. Enter **ftp localhost**.
- b. Log in anonymously by entering the following:
  - Name: **ftp**
  - Password: **your email address**
- c. Exit FTP by entering **exit**.
- d. Log in to a partner's server anonymously by entering **ftp partner\_server\_IP\_address**
- e. Log out by entering **exit**.

### Part III: Configure TCP Wrapper

Do the following:

1. Secure the Telnet service so that everyone in the classroom except your partner can Telnet to your system:
  - a. Edit the file /etc/hosts.deny by entering **vim /etc/hosts.deny**
  - b. Add the following to the end of the file:  
**in.telnetd : partner\_server\_IP\_address**  
Make sure there is an empty line at the end of the file or the configuration will not work.
  - c. Exit vi and save the file by entering **:wq**.
  - d. Have the partner attempt to Telnet to your host; then have another student in the classroom attempt to Telnet to your host.  
The connection for your partner is closed. However, others can Telnet to your server.



---

If the results are not what you expect, check the file /var/log/messages by entering **tail -f /var/log/messages**.

---

To do step d., you will have to configure vsftpd as given in this exercise on the VMWare machine da1.

- a. Enter **ftp localhost**.
- b. Log in anonymously by entering the following:
  - Name: **ftp**
  - Password: **your email address**
- c. Exit FTP by entering **exit**.
- d. Log in to a partner's server anonymously by entering **ftp partner\_server\_IP\_address**
- e. Log out by entering **exit**.

### Part III: Configure TCP Wrapper

Do the following:

1. Secure the Telnet service so that everyone in the classroom except your partner can Telnet to your system:
  - a. Edit the file /etc/hosts.deny by entering **vim /etc/hosts.deny**
  - b. Add the following to the end of the file:  
**in.telnetd : partner\_server\_IP\_address**  
Make sure there is an empty line at the end of the file or the configuration will not work.
  - c. Exit vi and save the file by entering **:wq**.
  - d. Have the partner attempt to Telnet to your host; then have another student in the classroom attempt to Telnet to your host.  
The connection for your partner is closed. However, others can Telnet to your server.



---

If the results are not what you expect, check the file /var/log/messages by entering **tail -f /var/log/messages**.

---

- e. Edit the file `/etc/hosts.deny` again by entering  
**vim /etc/hosts.deny**
  - f. Place a comment character (**#**) in front of the line you just added to the file `/etc/hosts.deny`; then add the following line.  
**ALL : ALL**
  - g. Exit vi and save the file by entering **:wq**.  
Apply the same security restriction by editing the file `/etc/hosts.allow`.
  - h. Edit the file `/etc/hosts.allow` by entering  
**vim /etc/hosts.allow**
  - i. Add the following to the end of the file:  
**in.telnetd : ALL EXCEPT partner\_server\_IP\_address**
  - j. Exit vi and save the file by entering **:wq**.
  - k. Have your partner attempt to Telnet to the system; then have another student in the classroom attempt to Telnet to your host.  
The results are the same as with the file `hosts.deny`.
2. Perform a twist by editing `ALL : ALL` in the file `/etc/hosts.deny`:
    - a. Edit the file `/etc/hosts.deny` by entering  
**vim /etc/hosts.deny**
    - b. Edit the `ALL:ALL` line to reflect the following (in one line):  
**ALL: ALL: twist echo "This service is not accessible from %a!"**
    - c. Exit vi and save the file by entering **:wq**.
    - d. Have your partner attempt to Telnet to the system to verify that the message is sent.
    - e. When you finish testing the twist, edit the file `/etc/hosts.deny` by entering  
**vim /etc/hosts.deny**
    - f. Comment out (**#**) the `ALL: ALL: ...` line.

- e. Edit the file `/etc/hosts.deny` again by entering  
**vim /etc/hosts.deny**
  - f. Place a comment character (**#**) in front of the line you just added to the file `/etc/hosts.deny`; then add the following line.  
**ALL : ALL**
  - g. Exit vi and save the file by entering **:wq**.  
Apply the same security restriction by editing the file `/etc/hosts.allow`.
  - h. Edit the file `/etc/hosts.allow` by entering  
**vim /etc/hosts.allow**
  - i. Add the following to the end of the file:  
**in.telnetd : ALL EXCEPT partner\_server\_IP\_address**
  - j. Exit vi and save the file by entering **:wq**.
  - k. Have your partner attempt to Telnet to the system; then have another student in the classroom attempt to Telnet to your host.  
The results are the same as with the file `hosts.deny`.
2. Perform a twist by editing `ALL : ALL` in the file `/etc/hosts.deny`:
    - a. Edit the file `/etc/hosts.deny` by entering  
**vim /etc/hosts.deny**
    - b. Edit the `ALL:ALL` line to reflect the following (in one line):  
**ALL: ALL: twist echo "This service is not accessible from %a!"**
    - c. Exit vi and save the file by entering **:wq**.
    - d. Have your partner attempt to Telnet to the system to verify that the message is sent.
    - e. When you finish testing the twist, edit the file `/etc/hosts.deny` by entering  
**vim /etc/hosts.deny**
    - f. Comment out (**#**) the `ALL: ALL: ...` line.



