COMP3066 – Week 04 - 05 Assignment

- **This is an individual assignment.**
- **The completed work has to be uploaded to the drop box on D2L.**
  1. **Email submissions will not be accepted.**
- **Reminder:**
  1. **The screenshot taking guidelines must be followed (these can be found in our course on D2L under the "Course Content"**
  2. **User account: Your lastname and then the first letter of the first name. For example: my name is Nikolai (first) Ivanov (last), so my user name is ivanovn**
  3. **Host name of your Linux VM: Your full last name, the dash character, and the two letters of the first name. For example: my name is Nikolai (first) Ivanov (last), so my host name is ivanov-ni**
  4. **Screenshots that do not show the properly configured user account and host name will not be accepted**

Objective: To configure the network services manually on Open SUSE Linux.

Marks breakdown:

Total assignment marks: 10 marks

4 marks: Task 1: DNS Server configuration
- Forward Lookup Zone – 2 marks
- Reverse Lookup Zone – 2 marks

4 marks: Task 2: Apache Server configuration
- Virtual Host – 2 marks
- User Authentication – 1 mark
- SSL – 2 marks

2 marks: Task 3: Samba Server configuration

Note: there are no partial marks: the configuration must be completed successfully to receive the marks

Lab Activity

IMPORTANT:

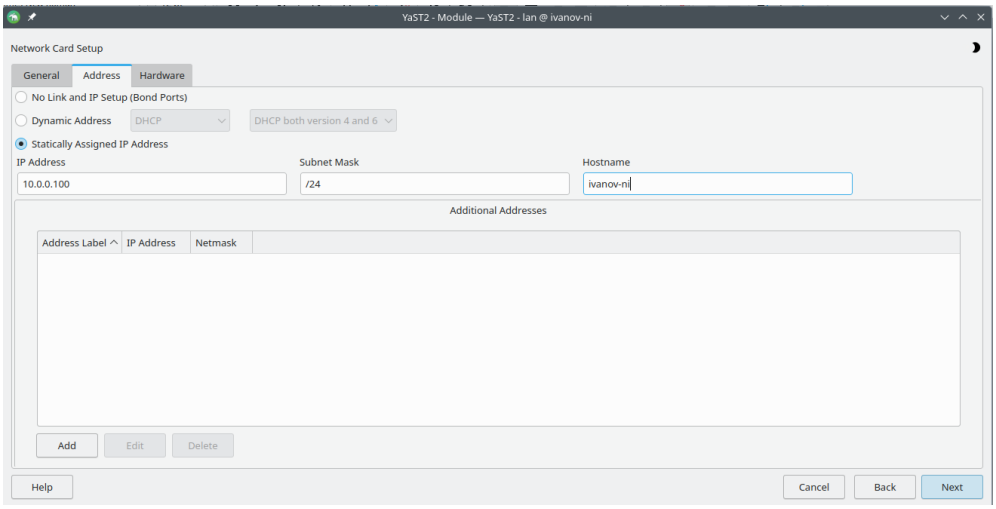
Add a new Host-Only or NAT Network card to your Linux VM. For that you need to shut down Linux (do not suspend, shut it down) and then open the Virtual Machine Settings for your Linux VM. Once in the settings, click the Add button to add new hardware component to the current configuration. Select to add the Network Adapter from the list and make it a Host-Only or NAT adapter. Click OK to close the VM Settings dialog and start your Linux.

Login to Linux and open YaST.

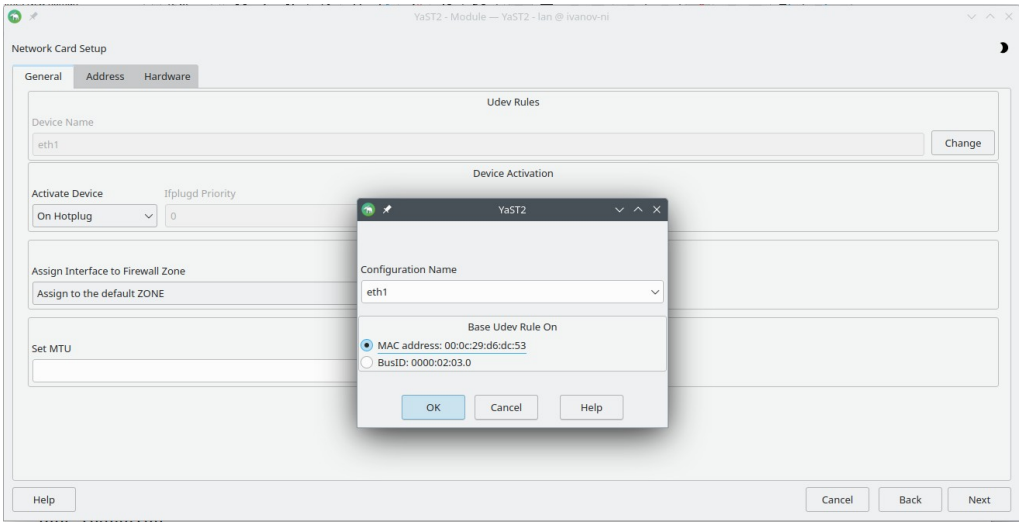
Open System>Network Settings, select the new network card and click the Edit button.

Set the following configuration for the new network card:

Name: eth1
IP Address assignment: Static
IP Address: 10.0.0.100
Subnet mask: /24
Hostname: your last name then a dash “-” and the two letters of the first name. For example, my host name is ivanov-ni (last name: ivanov, first name: nikolai)



NOTE: you can also change the name of the network adapter by opening the “General” tab and clicking the “Change” button next to the “Device Name” text box:



Once you made all the changes, then click Next and then OK to save the above configuration and exit from the “Network Settings” app.

NOTE: adding a new network card removed your configuration from the /etc/sysconfig/network/routes file. Please re-add the default gateway, save the file, and reboot your Linux VM or restart the network service.

Test the new configuration using the following command(s):

ping -c 1 YOUR_HOST_NAME
ping -c 1 10.0.0.100
ping -c 1 www.georgebrown.ca

NOTE: The above ping commands must be successful.

SUBMISSION: Run the following commands: (a) ip address show dev eth0, (b) ip address show dev eth1, (c) ping -c 1 10.0.0.100 | head -n 2, (d) ping -c 1 YOUR_HOST_NAME | head -n 2, and (e) ping -c 1 www.georgebrown.ca | head -n 2. Take the screenshot of the output of these commands and replace the sample screenshot below with your screenshot:

SCREENSHOT

```
loore@loor-ed:~> ip address show dev eth0
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:a6:68:b5 brd ff:ff:ff:ff:ff:ff
    altname enp2s1
    altname ens33
    inet 192.168.132.128/24 brd 192.168.132.255 scope global eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fea6:68b5/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
loore@loor-ed:~> ip address show dev eth1
3: eth1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:a6:68:bf brd ff:ff:ff:ff:ff:ff
    altname enp2s5
    altname ens37
    inet 10.0.0.100/32 scope global eth1
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fea6:68bf/64 scope link proto kernel_ll
       valid_lft forever preferred_lft forever
loore@loor-ed:~> ping -c 1 10.0.0.100 | head -n 2
PING 10.0.0.100 (10.0.0.100) 56(84) bytes of data.
64 bytes from 10.0.0.100: icmp_seq=1 ttl=64 time=0.115 ms
loore@loor-ed:~> ping -c 1 loor-ed | head -n 2
PING loor-ed (127.0.0.1) 56(84) bytes of data.
64 bytes from localhost (127.0.0.1): icmp_seq=1 ttl=64 time=0.083 ms
loore@loor-ed:~> ping -c 1 www.georgebrown.ca | head -n 2
PING a1206.b.akamai.net (23.223.17.201) 56(84) bytes of data.
64 bytes from a23-223-17-201.deploy.static.akamaitechnologies.com (23.223.17.201): icmp_seq=1 ttl=128 time=1.52
ms
loore@loor-ed:~>
```

Task 1 - Configure a DNS server Exercise

- Part I: Install BIND
- Part II: Configure a DNS Master Server

Part I: Install BIND

1. Use either **zypper** or **YaST Software > Software Management** to install the following packages:

   bind

Part II: Configure a DNS Master Server

1. Open a terminal window and su to **root**.
2. Open the file **/etc/named.conf** in a text editor.
3. Configure the forwarders line to match the following:

forwarders { YOUR_GATEWAY_IP_ADDRESS; };

forwarders { 192.168.132.2; };

Make sure that you delete the comment character from the beginning of the forwarders line.

4. Add the following 2 zone statements after the existing zone statements:

```
zone "digitalairlines.com" in {
   type master;
   file "master/digitalairlines.com.zone";
};
zone "0.0.10.in-addr.arpa" in {
   type master;
   file "master/10.0.0.zone";
};
```

5. Save and close the file.
6. Create a new file **digitalairlines.com.zone** in the directory **/var/lib/named/master/**.
7. Enter the following zone configuration in the file:

```
$TTL 172800
@ IN SOA YOURHOSTNAME.digitalairlines.com. root.digitalairlines.com. (
2023092101
1D
2H
1W
3H
)
digitalairlines.com. IN NS YOURHOSTNAME.digitalairlines.com.
YOURHOSTNAME IN A 10.0.0.100
accounting IN A 10.0.0.100
```

```
$TTL 172800
@ IN SOA loor-ed.digitalairlines.com. root.digitalairlines.com. (
2024092301
1D
2H
1W
3H
)
digitalairlines.com. IN NS loor-ed.digitalairlines.com.
loor-ed IN A 10.0.0.100
accounting IN A 10.0.0.100
```

NOTE: replace the **YOURHOSTNAME** with the host name of your Linux VM.

The SOA record (including root.digitalairlines.com) *must be* on a single line. Make sure you enter your Linux HOSTHAME in the SOA and NS records. Use the current date and "01" as the serial number (such as **2023092101**).

8. Save and close the file.

9. Create a new file **10.0.0.zone** in the directory **/var/lib/named/master/**.

10. Enter the following zone configuration in the file:

```
$TTL 172800
@ IN SOA YOURHOSTNAME.digitalairlines.com. root.digitalairlines.com. (
2023092101
1D
2H
1W
3H
)
    IN NS YOURHOSTNAME.digitalairlines.com.
100 IN PTR YOURHOSTNAME.digitalairlines.com.
100 IN PTR accounting.digitalairlines.com.
```

```
$TTL 172800
@ IN SOA loor-ed.digitalairlines.com. root.digitalairlines.com. (
2024092301
1D
2H
1W
3H
)
    IN NS loor-ed.digitalairlines.com.
100 IN PTR loor-ed.digitalairlines.com.
100 IN PTR accounting.digitalairlines.com.
```

NOTE: replace the **YOURHOSTNAME** with the host name of your Linux VM.

The SOA record (including root.digitalairlines.com) *must be* on a single line. Make sure you enter your HOSTNAME in the SOA and NS records. Use the current date and "01" as the serial number (such as **2023092101**).

11. Save and close the file.

12. Open a second terminal window and **su** to root.

13. Enter the following command:

tail -f /var/log/messages

NOTE: if the above command results in the */var/log/messages file not found, then you need to a) install the **rsyslog** package using either YaST software manager or a zypper command and b) restart the rsyslog service by issuing the following command: **service rsyslog restart***

14. Switch to the first terminal window and start bind with the following command:

rcnamed restart

or

systemctl restart named

NOTE: If there are errors in the file /etc/named, they are noted in the output (with specific references and line numbers). The named daemon will not start until these errors are fixed.

15. From the second terminal window, watch the log output of bind for any messages related to two zones that you created.

16. **All errors related to your zones must be fixed before you can continue**.

17. From the first terminal window, start bind automatically when the system is booted by entering the following:

chkconfig named on

18. Open the file **/etc/resolv.conf** in a text editor.

19. **D**o not remove the existing **nameserver** entries by placing.

20. Add the following entry **to be the first entry** in the list of nameservers:

nameserver *10.0.0.100*

21. Save and close the file.

22. Verify that your DNS server works by running the following commands:

host YOURHOSTNAME.digitalairlines.com
host accounting.digitalairlines.com
host 10.0.0.100
dig @10.0.0.100 YOURHOSTNAME.digitalairlines.com

host loor-ed.digitalairlines.com
host accounting.digitalairlines.com
host 10.0.0.100
dig @10.0.0.100 loor-ed.digitalairlines.com

SUBMISSION: Run all the commands listed in step 22. Take the screenshot of the output and replace the sample screenshot below with your screenshot:

SCREENSHOT

```
loore@loor-ed:~> host loor-ed.digitalairlines.com
loor-ed.digitalairlines.com has address 10.0.0.100
loore@loor-ed:~> host accounting.digitalairlines.com
accounting.digitalairlines.com has address 10.0.0.100
loore@loor-ed:~> host 10.0.0.100
100.0.0.10.in-addr.arpa domain name pointer accounting.digitalairlines.com.
100.0.0.10.in-addr.arpa domain name pointer loor-ed.digitalairlines.com.
loore@loor-ed:~> dig @10.0.0.100 loor-ed.digitalairlines.com

; <<>> DiG 9.18.28 <<>> @10.0.0.100 loor-ed.digitalairlines.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 43958
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 3df36f6f0e3b79110100000066f1dbe23b19a93aaa3ef396 (good)
;; QUESTION SECTION:
;loor-ed.digitalairlines.com.   IN      A

;; ANSWER SECTION:
loor-ed.digitalairlines.com. 172800 IN  A       10.0.0.100

;; Query time: 0 msec
;; SERVER: 10.0.0.100#53(10.0.0.100) (UDP)
;; WHEN: Mon Sep 23 17:21:38 EDT 2024
;; MSG SIZE  rcvd: 100

loore@loor-ed:~>
```

IMPORTANT: the DNS configuration must be successful to complete the rest of this lab.

Task 2 Configure an Apache Web Server Exercise

- Part I: Install Apache
- Part II: Test the Installation
- Part III: Configure a Virtual Host for the Accounting Department
- Part IV: Configure User Authentication
- Part V: Configure SSL

Part I: Install Apache

1. Use either **zypper** or **YaST Software > Software Management** to install the following packages:
   apache2
   apache2-prefork
2. Open a terminal window and su to **root**.
3. To start Apache at ***boot time***, enter the following:
   chkconfig apache2 on
4. To start the Apache daemon, enter the following:

rcapache2 restart

or

service apache2 restart

or

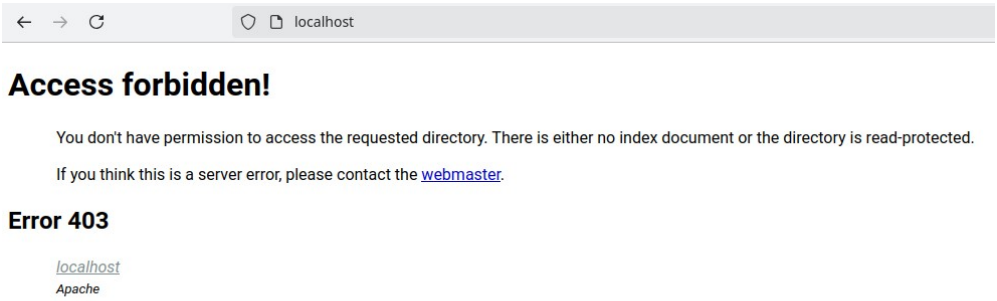
systemctl restart apache2

Part II: Test the Installation

1. Start the **Web Browser**.
2. In the address bar of the web browser, enter the following:

   http://localhost

The apache web server runs but there is no default configured web application and the web browser will display the “Access Fobidden; Error 403” as shown in the following screenshot:



Part III: Configure a Virtual Host for the Accounting Department

1. From the terminal window (as root), create a directory for the virtual host by entering the following:

mkdir /srv/www/accounting

2. Adjust the file system permissions by entering the following:

chown wwwrun /srv/www/accounting/

3. In the new directory, create a file **index.html** with the following content (do not forget to replace YOURHOSTNAME with your actuall host name):

<html><head><title>Accounting Intranet Server</title></head><body>

<h1>Accounting Intranet: completed by YOURHOSTNAME</h1></body></html>

<html><head><title>Accounting Intranet Server</title></head><body>

<h1>Accounting Intranet: completed by loor-ed</h1></body></html>

4. Adjust the file system permissions of the file by entering the following:

chown wwwrun index.html

5. Change to the directory /etc/apache2/vhosts.d/ by entering the following:

cd /etc/apache2/vhosts.d/

6. Move the existing virtual host template files to your home directory by entering the following:

mv vhost* ~

7. Create a new text file in the */etc/apache2/vhosts.d/ folder* and name it **accounting.conf** Then, open this file in a text editor and make the following changes:

```
<VirtualHost accounting.digitalairlines.com:80>
ServerName accounting.digitalairlines.com
DocumentRoot /srv/www/accounting
ErrorLog /var/log/apache2/accounting.digitalairlines.com-error_log
CustomLog /var/log/apache2/accounting.digitalairlines.com-access_log combined
UseCanonicalName On
<Directory "/srv/www/accounting/">
AllowOverride None
Options Indexes FollowSymLinks
Order allow,deny
Allow from all
</Directory>
</VirtualHost>
```

8. Test the syntax of your configuration file by entering the following:

apache2ctl configtest

Note 1: the above command will fail if the apache mode_access_compat is not enabled. Run the following command to enable the module:

a2enmod mod_access_compat

and restart the apache service by issing the following command:

rcapache2 restart

or

service apache2 restart

or

systemctl restart apache2

repeat the **apache2ctl configtest** command after you enabled the mod_access_compat

Note 2: to fix the "AH00558: httpd-prefork: Could not reliably determine the server's fully qualified domain name..." warning, open the apache2 config file (/etc/apache2/httpd.conf) in nano and add the following line to the end of the file:

ServerName YOURHOSTNAME.digitalairlines.com

ServerName loor-ed.digitalairlines.com

9. Restart Apache by entering the following:

rcapache2 restart

or

service apache2 restart

or

systemctl restart apache2

and test the configuration by entering:

apache2ctl configtest

This time the above command must display the "Syntax OK" message.

```
loore@loor-ed:~> sudo apache2ctl configtest
[sudo] password for root:
Syntax OK
loore@loor-ed:~>
```

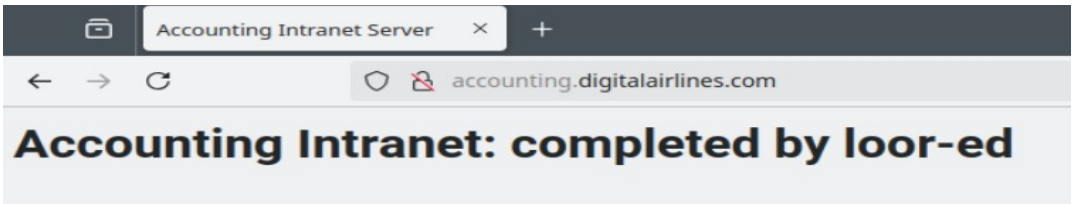
10. From the Web browser, access the virtual host by entering the following:

http://accounting.digitalairlines.com

The accounting intranet index page is displayed.

11. Close the Web browser.

SUBMISSION: the screenshot of the web browser window in Step 10. Make sure to include the URL bar of the Web Browser in your screenshot. Repalce the sample screenshot below with your screenshot:



Part IV: Configure User Authentication

1. Use YaST Security and Users->User and Group Management to create a new user. Use **geeko** as user name and set **novell** to be the password for the geeko user

2. From the terminal window (as root), create the file **htpasswd** and add the user **geeko** to it by entering the following:

htpasswd2 -c /etc/apache2/htpasswd geeko

2. When prompted for a password, enter **novell** (you will be asked to confirm the password).

3. Open the virtual host configuration file **/etc/apache2/vhosts.d/accounting.conf** in a text editor.

4. Find the following directory directive:

<Directory "/srv/www/accounting/">

5. Right after this directory block opening element, add the following lines:

```
AuthType Basic
AuthName "Accounting Intranet: Completed by YOURHOSTNAME"
AuthUserFile /etc/apache2/htpasswd
Require user geeko
```

```
AuthType Basic
AuthName "Accounting Intranet: Completed by loor-ed"
AuthUserFile /etc/apache2/htpasswd
Require user geeko
```

6. Check the syntax of the configuration file by entering the following command:

apache2ctl configtest

you must get the “Syntax OK” message as a result of the syntax check.

7. Restart the Apache server by entering the following:

rcapache2 restart

or

service apache2 restart

or

systemctl restart apache2

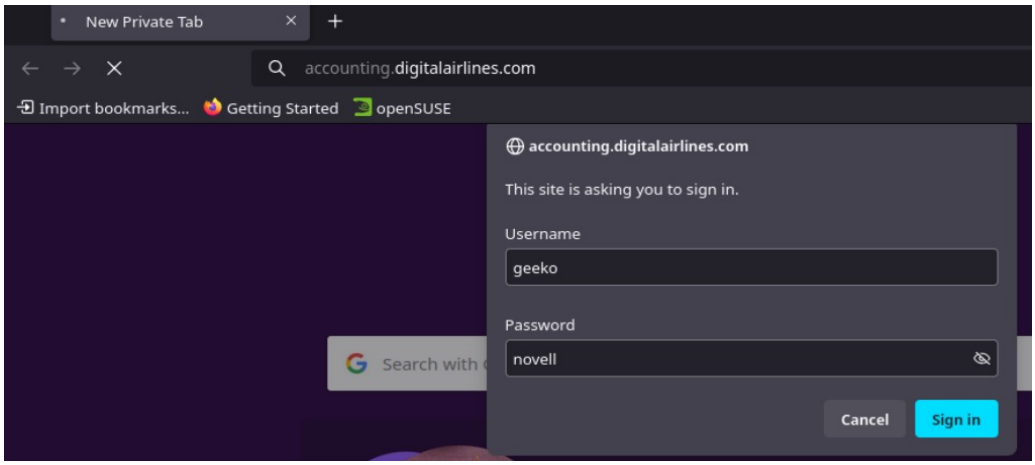
8. Open the Web browser; then enter the following:

http://accounting.digitalairlines.com

A password dialog appears.

9. Enter a user name of **geeko** and a password of **novell**.

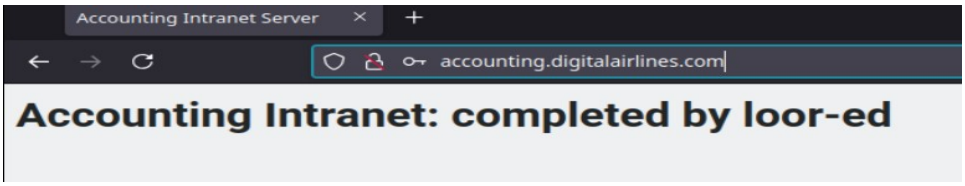
SUBMISSION: take a screenshot of the web browser window in steps 8 and 9 (make sure that the password dialog box is in the screen shot and that the Web Browser URL bar is visible in the screenshot). Repalce the sample screenshot below with your screenshot:



Note: the entered user name and password are saved in the web browser cache; the cache has to be cleared in the web browser settings to see the prompt to log in again.

10. Access the protected web site by selecting **OK**.

SUBMISSOIN: take a screenshot of the web browser window in step 10 (make sure that the Web Browser URL bar is visible in the screenshot). Repalce the sample screenshot below with your screenshot:



Part V: Configure SSL

1. Move to the **/etc/apache2** directory. All commands must be run as root.
2. Enter the following command to generate the private key and the certificate:

openssl req -x509 -sha256 -nodes -days 365 -newkey rsa:2048 -keyout server.key -out server.crt

3. Enter the following information:

Option	**Value**
Country Name	CA
State or Province Name	Ontario
Locality Name	Toronto
Organization Name	Digital Airlines
Organization Unit Name	**YOUR FULL NAME** (first name and last name)
Common Name	accounting.digitalairlines.com.
Email Address	**YOURHOSTNAME**@digitalairlines.com

Option	**Value**
Country Name	CA
State or Province Name	Ontario
Locality Name	Toronto
Organization Name	Digital Airlines
Organization Unit Name	**Eduardo Loor** (first name and last name)
Common Name	accounting.digitalairlines.com.
Email Address	**loor-ed**@digitalairlines.com

When **(if)** prompted for password, enter Novell.

Terminate the openssl command prompt by typing exit and hitting the enter key (you can also use the CTRL+C to do the same).

4. Move the generated key and certificate files by entering the following commands:

mv /etc/apache2/server.key /etc/apache2/ssl.key/

mv /etc/apache2/server.crt /etc/apache2/ssl.crt/

5. Copy the **/etc/apache2/vhosts.d/accounting.conf** file to **/etc/apache2/vhosts.d/accounting-ssl.conf** and open the **/etc/apache2/vhosts.d/accounting-ssl.conf** in a text editor. Change the following lines:

<VirtualHost accounting.digitalairlines.com:80>

to

<VirtualHost accounting.digitalairlines.com:443>

and

ServerName accounting.digitalairlines.com

to
ServerName accounting.digitalairlines.com:443

6. Add the following lines after the **ServerName** directive:

```
SSLEngine on
SSLCertificateFile /etc/apache2/ssl.crt/server.crt
SSLCertificateKeyFile /etc/apache2/ssl.key/server.key
```

7. Save and close the file.

8. Open the file **/etc/sysconfig/apache2** in a text editor, and change the following lines:

```
APACHE_SERVER_FLAGS="SSL"

APACHE_START_TIMEOUT="10"
```

Note: the above lines might already be present. If they are not present, you will have to add them to the configuration file.

9. Save and close the file.

10. Copy mod_socache_shmcb.so to /srv/www/modules directory. For this, first you need to create modules directory /srv/www/

mkdir /srv/www/modules

copy shmcb file to modules directory

cp /usr/lib64/apache2-prefork/mod_socache_shmcb.so /srv/www/modules/

and then, edit **/etc/apache2/httpd.conf** and add these lines to the end of the httpd.conf file:

#Load module shmcb

LoadModule socache_shmcb_module modules/mod_socache_shmcb.so

#Load module shmcb

LoadModule socache_shmcb_module /srv/www/modules/mod_socache_shmcb.so

11. From the terminal window, check the syntax of the configuration file by entering the following:

apache2ctl configtest

Note: You must get the “Syntax OK” message. If you get a message stating that the module_socache_shmcb is already loaded, then open the httpd.conf file and comment out the LoadModule line you added in step 16 by placing the # character in front of the line and test the configuration again.

12. Restart Apache by entering the following:

rcapache2 restart

alternatively, you can use the following command: **systemctl restart apache2.service**

13. From the WEB browser, enter the following:

https://accounting.digitalairlines.com/

As the certificate used in this exercises is self-signed, the browser displays a warning - “Your Connection is NOT Secure”.

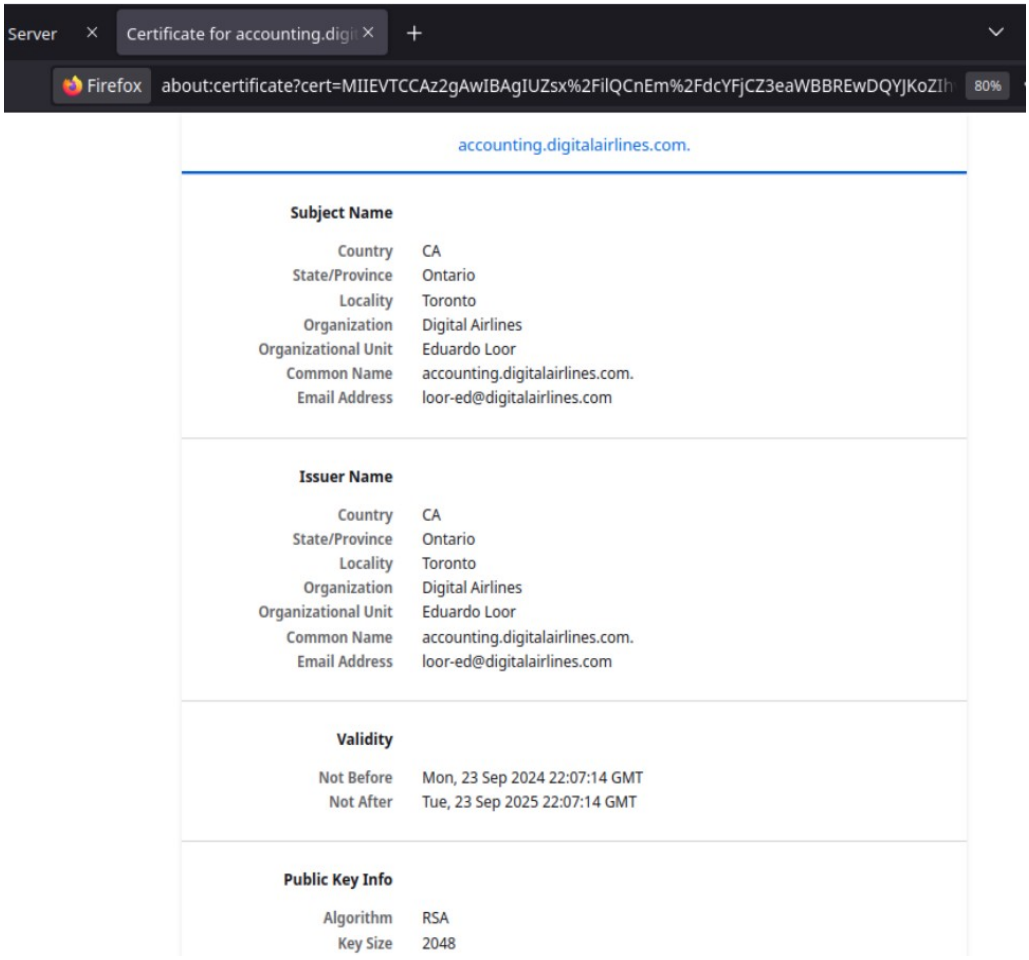
14. Click the “Advanced” button and add click the “View Certificate” link to review the certificate information.

15. Close the view certificate window and add a security exception to proceed by clicking the “Accept the Risk and Continue” button.. In the login dialog, enter **geeko** as the username and **novell** as the password.

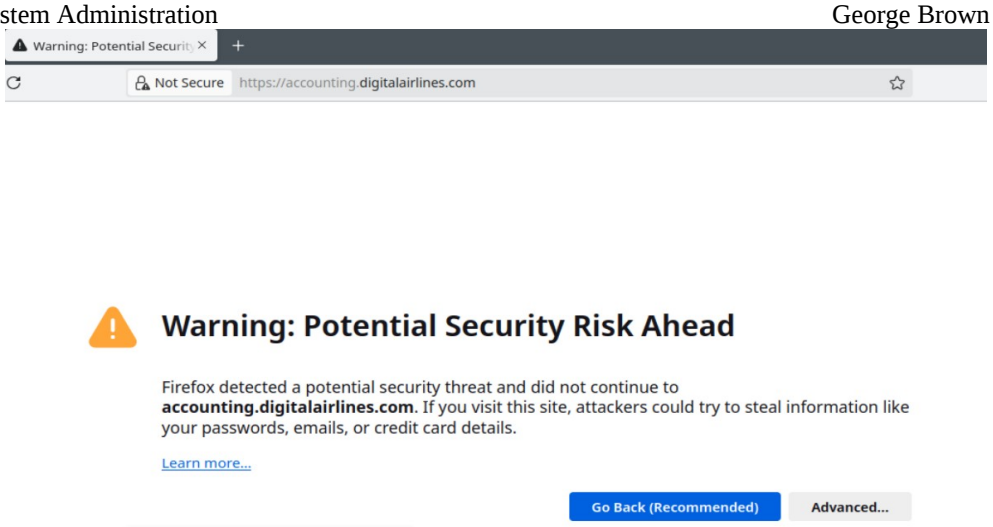
16. Click the OK button to login.

SUBMISSION: Repalce the sample screenshots below with your screenshot:

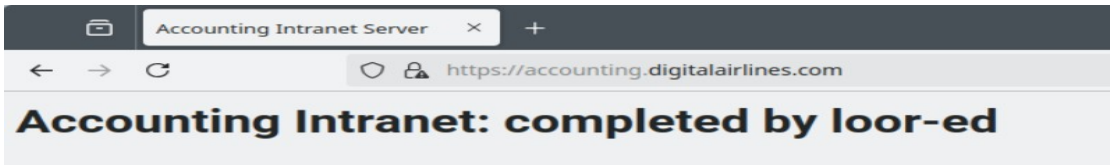
Screenshot of the generated certificate:



Screenshot of the certificate warning when accessing https://accounting.digitalairlines.com (must say https in the URL):



Screenshot of the loaded https://accounting.digitalairlines.com page (must say https in the URL):



Task 3 Configure a File Server With Samba.

Exercise

IMPORTANT:

Disable AppArmor. To disable AppArmor, start YaST, open Security and Users->AppArmor Configuration panel and then launch Settings. Uncheck the “Enable AppArmor” check box and click the Done button.

Part I: Install Samba

Part II: Configure a Share for the User Geeko

Part III: Access the Share of the User Geeko With smbclient

Part IV: Mount Geeko's Share

Part I: Install Samba

1. Use either **zypper** or **YaST Software > Software Management** to install the following packages:
   samba (if not already installed)
   samba-client (if not already installed)

Part II: Configure a Share for the User Geeko

1. From a terminal window, su to **root**.
2. Change to the directory **/etc/samba**.
3. Save the default Samba configuration file by entering the following:

mv smb.conf smb.save

4. Create the file **smb.conf** with a text editor.
5. Add the following lines to the configuration file (do not forget to replace YOURHOSTNAME with your host name):

```
[global]
workgroup = Accounting
netbios name = YOURHOSTNAME
security = user
[geeko-dir]
comment = Geeko Directory
path = /srv/samba/geeko
valid users = geeko
read only = no
```

```
[global]
workgroup = Accounting
netbios name = loor-ed
security = user
[geeko-dir]
comment = Geeko Directory
path = /srv/samba/geeko
valid users = geeko
read only = no
```

6. Save and close the file.

7. Create the directory to export by entering the following commands:

mkdir -p /srv/samba/geeko

8. Create a test file in the directory by entering the following:

touch /srv/samba/geeko/my_file

9. Adjust the directory permissions by entering the following commands:

chown -R geeko /srv/samba/geeko

10. Add geeko to the file smbpasswd file by entering the following:

smbpasswd -a geeko

11. When prompted for a password, enter **novell** (twice).

12. Check the syntax of the configuration file by entering the following:

testparm

13. Start the Samba servers by entering the following commands:

rcnmb restart
rcsmb restart

or

systemctl restart nmb
systemctl restart smb

SUBMISSION: the screen shot of the window after completing steps 12 and 13. Repalce the sample screenshot below with your screenshot:

```
loor-ed:/etc/samba # testparm
Load smb config files from /etc/samba/smb.conf
Loaded services file OK.
Weak crypto is allowed by GnuTLS (e.g. NTLM as a compatibility fallback)

Server role: ROLE_STANDALONE

Press enter to see a dump of your service definitions

# Global parameters
[global]
        security = USER
        workgroup = ACCOUNTING
        idmap config * : backend = tdb


[geeko-dir]
        comment = Geeko Directory
        path = /srv/samba/geeko
        read only = No
        valid users = geeko
loor-ed:/etc/samba # rcnmb restart
loor-ed:/etc/samba # rcsmb restart
loor-ed:/etc/samba #
```

Part III: Access the Share of the User Geeko With smbclient

1. Open another terminal window as a regular (not root) user.

2. Access Geeko's share by entering the following:

smbclient -U geeko //localhost/geeko-dir

3. When prompted for a password, enter **novell**.

4. Display all available commands of smbclient by entering the following:

help

5. List the content of the share by entering the following:

ls

6. Copy the file my_file to the current directory by entering the following:

get my_file

7. Exit smbclient by pressing **Ctrl+D** or typing **exit** and pressing the Enter key.

8. Verify that the file my_file has been copied to the current directory by entering **ls -l my_file**.

SUBMISSION: the screen shot of the window after completing steps 2, 5, 6, and 8. Repalce the sample screenshots below with your screenshot:

Screenshot for Steps 2, 5, 6, and 8: