Assignment no. 3 Networking and servers

Question 1:

Points: 20

Deploy a website on localhost using either apache2 or Nginx. Create a DNS name for this website as 'awesomeweb'. You can use any web template you want or can write your own simple HTML code. Write detailed documentation with the steps involved.

Ans:-

Step1:- Install Apache2 server

Sudo apt install apache2

Step2:- Start and check the status of apache2 server

Sudo systemctl start apache2

Sudo systemctl status apache 2

Step3:- Create a DNS name for this website as 'awesomeweb'

- cd /var/www/html
- create index.html command- "sudo nano index.html"
- add the html/css content in index.html file and check file present in the directory by command "ls"

step4:- Create a new configuration file for "awesomeweb" website

- sudo nano /etc/apache2/sites-available/awesomeweb.conf

```
<VirtualHost *:80>
  ServerName awesomeweb
   DocumentRoot /var/www/html
  <Directory /var/www/html>
     Options Indexes FollowSymLinks MultiViews
   AllowOverride All
  Order allow,deny
  allow from all
 </Directory>
</VirtualHost>
```

step5:- Enable new virtual host

-sudo a2ensite awesomeweb.conf

Step6:- sudo systemctl restart apache2

Step7:- Edit hosts file

-sudo nano /etc/hosts

Add 127.0.0.1 awesomweb to the hosts

Step8:- Test

Open browser and type "awesomweb"

Question 2:

A website can have many subdomains and different services are running on them. Write a Python script to check the status of the subdomains which are up or down. The script should automatically

check the status every minute and should update it in tabular format on the screen. Write a detailed documentation of it.

Ans- for this need to install ‘requests’ library.

Functionality:
The **check_status()** function sends an HTTP request to each subdomain and checks the response status code.
The **display_status()** function prints the status of each subdomain in a tabular format.
The **main()** function continuously checks the status of subdomains every minute and updates the display.

Question 3: Hosting and Scanning a website on Virtual Machine

Points: 10

How to Install VirtualBox
Here's a step-by-step guide to installing Oracle VirtualBox on your Windows, macOS, or Linux computer:

Step 1: Download VirtualBox

1. Go to the official VirtualBox website: https://www.virtualbox.org/

2. Click on the "Downloads" link in the top navigation menu.

Step 2: Choose the Correct Package

1. On the Downloads page, you'll see various packages for different host operating systems. Select the appropriate package for your OS (e.g., Windows, macOS, or Linux).

Step 3: Install VirtualBox

1. For Windows:

- Download the installer for Windows and double-click on the downloaded file to start the installation.
- Follow the on-screen instructions and accept the license agreement.
- Choose the components you want to install and the installation path.
- Complete the installation process.

3. For Linux:

- Download the appropriate package for your Linux distribution (e.g., .deb for Debian/Ubuntu-based systems, .rpm for Red Hat/Fedora-based systems).

- Install VirtualBox using the package manager of your Linux distribution. For example, for Ubuntu, use the following command in the terminal:

  - sudo dpkg -i <VirtualBox_package_name>.deb

- You may need to install additional dependencies if prompted by the package manager.

Step 4: Post-installation Configuration (All Operating Systems)

1. After installation, you might need to add your user account to the "vboxusers" group (Linux) or "VirtualBox Users" group (Windows) to grant permissions to manage VMs.

Step 5: Launch VirtualBox

1. Once the installation is complete, you can launch VirtualBox from your application menu (Windows and Linux) or from the Applications folder (macOS).

Congratulations! You now have Oracle VirtualBox installed on your computer and can start creating and managing virtual machines for various purposes, including development, testing, and exploration of different operating systems. Once the VM has been installed, visit https://www.osboxes.org/ download a Ubuntu 22.04 image, and start it through your VirtualBox.

Now, complete the given tasks.

Task 1: Install Nginx inside the Ubuntu machine and host a website.

Task 2: Come back to your host machine (windows/Linux/mac) and scan the virtual machine using Nmap.

Task 3: Create the documentation of the process and the output of the scan.

Task 4: Observe the ports which are open.

O'Reilly Credential

You can use this to learn self-paced content.

Link to the O'Reilly Library: https://www.oreilly.com/library/view/temporary-access/ Instructions to access the O'Reilly Library content:

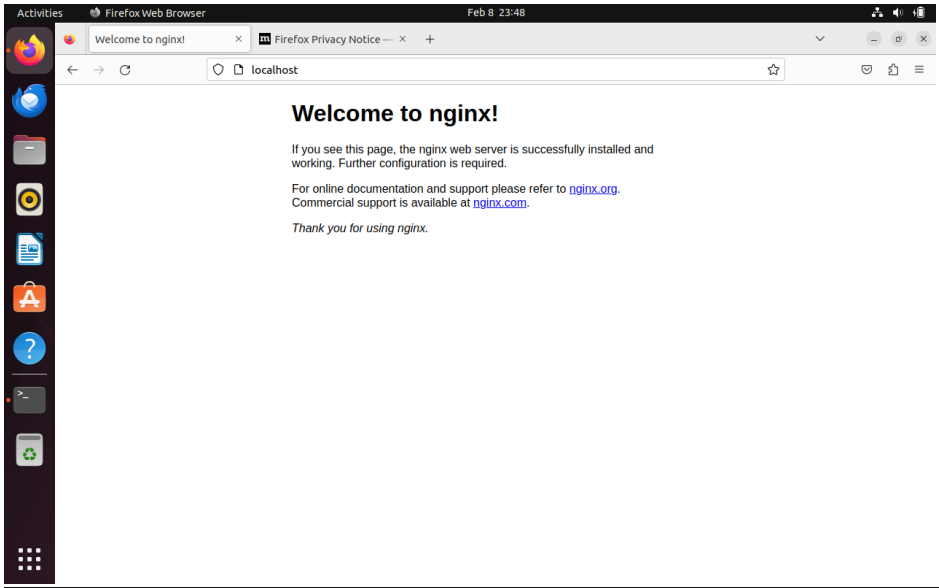
1. Open the link in a browser.

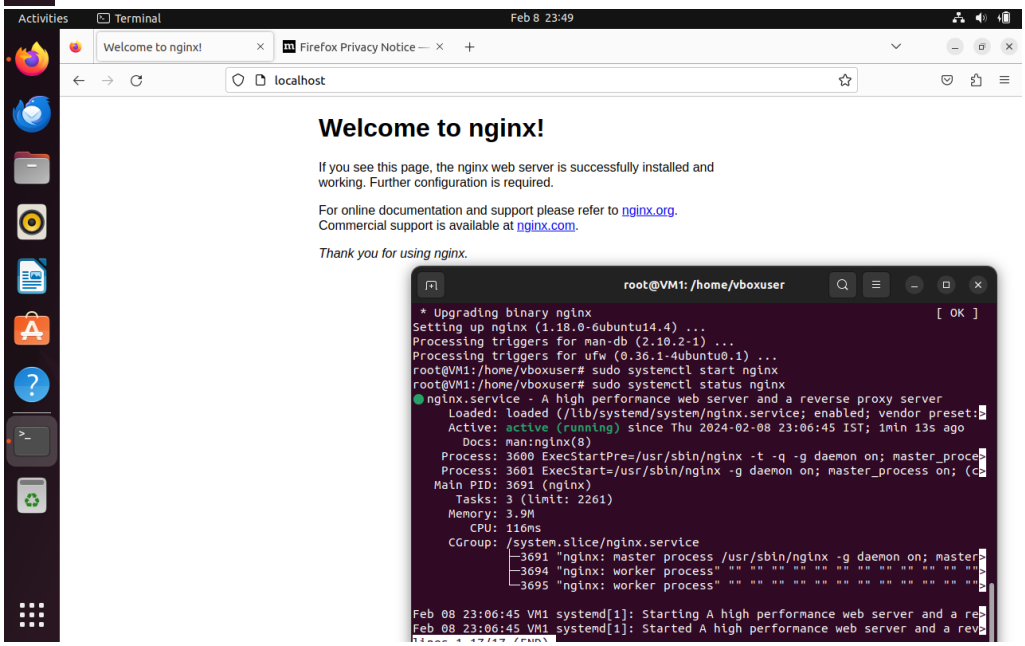
2. Select an Institution not listed.

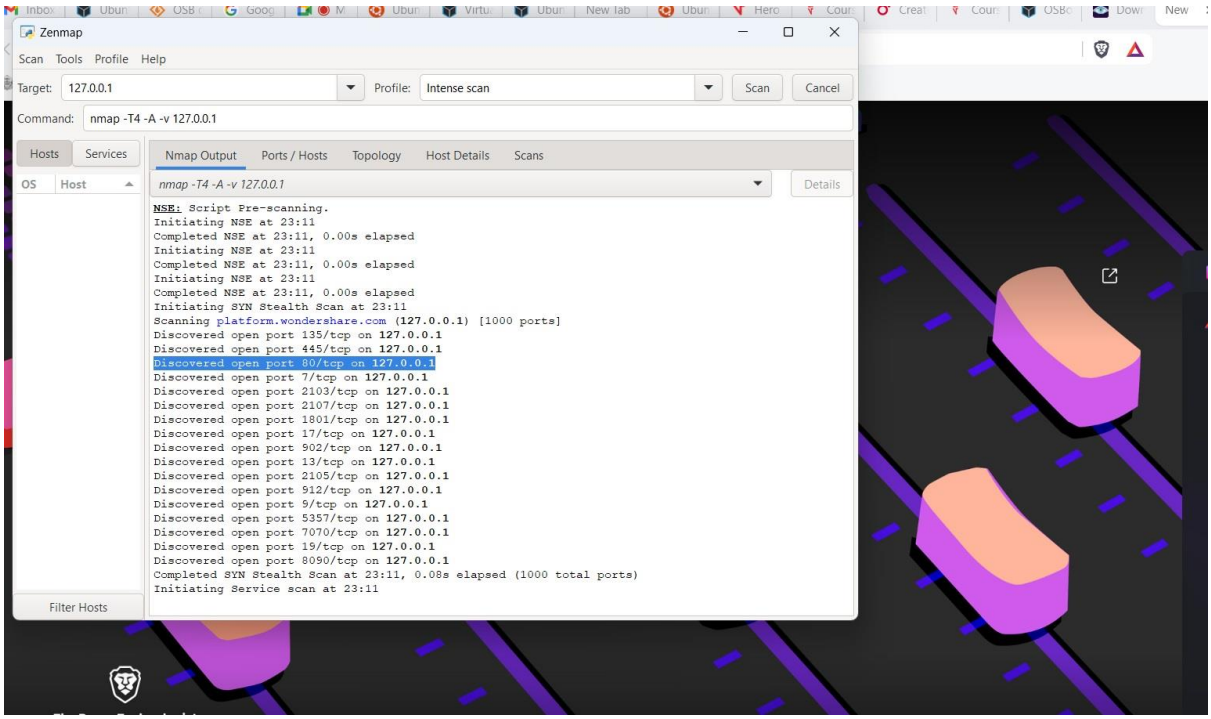
3. Enter your credentials, firstname@hv.oreilly.com (replace ‘firstname’ with your name)

4. Click enter to access the content.

Output
Virtual Box






Zenmap
Scan Tools Profile Help
Target: 127.0.0.1
Profile: Intense scan
Scan
Cancel
Command: nmap -T4 -A -v 127.0.0.1
Hosts
Services
OS
Host
Filter Hosts
Nmap Output
Ports / Hosts
Topology
Host Details
Scans
nmap -T4 -A -v 127.0.0.1
Details
NSE: Script Pre-scanning.
Initiating NSE at 23:11
Completed NSE at 23:11, 0.00s elapsed
Initiating NSE at 23:11
Completed NSE at 23:11, 0.00s elapsed
Initiating NSE at 23:11
Completed NSE at 23:11, 0.00s elapsed
Initiating SYN Stealth Scan at 23:11
Scanning platform.wondershare.com (127.0.0.1) [1000 ports]
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 80/tcp on 127.0.0.1
Discovered open port 7/tcp on 127.0.0.1
Discovered open port 2103/tcp on 127.0.0.1
Discovered open port 2107/tcp on 127.0.0.1
Discovered open port 1801/tcp on 127.0.0.1
Discovered open port 17/tcp on 127.0.0.1
Discovered open port 902/tcp on 127.0.0.1
Discovered open port 13/tcp on 127.0.0.1
Discovered open port 2105/tcp on 127.0.0.1
Discovered open port 912/tcp on 127.0.0.1
Discovered open port 9/tcp on 127.0.0.1
Discovered open port 5357/tcp on 127.0.0.1
Discovered open port 7070/tcp on 127.0.0.1
Discovered open port 19/tcp on 127.0.0.1
Discovered open port 8090/tcp on 127.0.0.1
Completed SYN Stealth Scan at 23:11, 0.08s elapsed (1000 total ports)
Initiating Service scan at 23:11