**A Personal Web Server Using**

**Nginx on Rocky Linux.**

**Objective :**

**To configure a personal web server using Nginx on Rocky Linux.**

**System Requirements :**

* **Rocky Linux**
* **Internet access**
* **Basic HTML editor (e.g., nano, vi)**

**Tools Used :**

* **Nginx web server**
* **Systemd (systemclt)**
* **DNF package manager**
* **SCP for remote file transfer(WinSCP)**

**Implementation Steps :**

1. **Install Nginx  
   sudo dnf install nginx -y**
2. **Start and enable Nginx**

**sudo systemctl start nginx**

**sudo systemctl enable nginx**

**(If NGINX is not enabling or start, then port 80 or 443 is already in use , so we Resolve Port Conflicts by sudo systemctl stop httpd or sudo fuser -k 80/tcp to kill the process.)**

1. **Verify service  
   Access http://localhost/ or http://<your-IP>/**

**(If Step-3 Verify service shows ERROR, then Enter Step-7 SELinux & Step-8 Configure firewall to add http service and after that check the Step-3 again.)**

1. **Create custom HTML page**

**sudo nano /usr/share/nginx/html/index.html**

**( Add your own HTML code into the Nano-Editor)**

1. **Set file permissions**

**sudo chown nginx:nginx /usr/share/nginx/html/index.html**

**(User):(Group)**

**sudo chmod 644 /usr/share/nginx/html/index.html**

**(User: READ[4]&WRITE[2] , Group: READ[4] , Other: READ[4])**

1. **Restart Nginx  
   sudo systemctl restart nginx**

**( To apply changes and ensure the Nginx web server is running with the latest configuration )**

1. **SELinux**

**getenforce**

**( If Nginx fails to serve files or access directories, SELinux might be denying access.**

**🡪getenforce helps to confirm whether SELinux is enforcing policies that could be causing the issue and Block Unauthorized actions. )**

1. **Configure firewall for HTTP**

**sudo firewall-cmd --permanent --add-service=http**

**(It allows HTTP traffic (port 80) through the firewall permanently.)**

**sudo firewall-cmd –reload**

**(It applies the permanent firewall changes immediately.)**

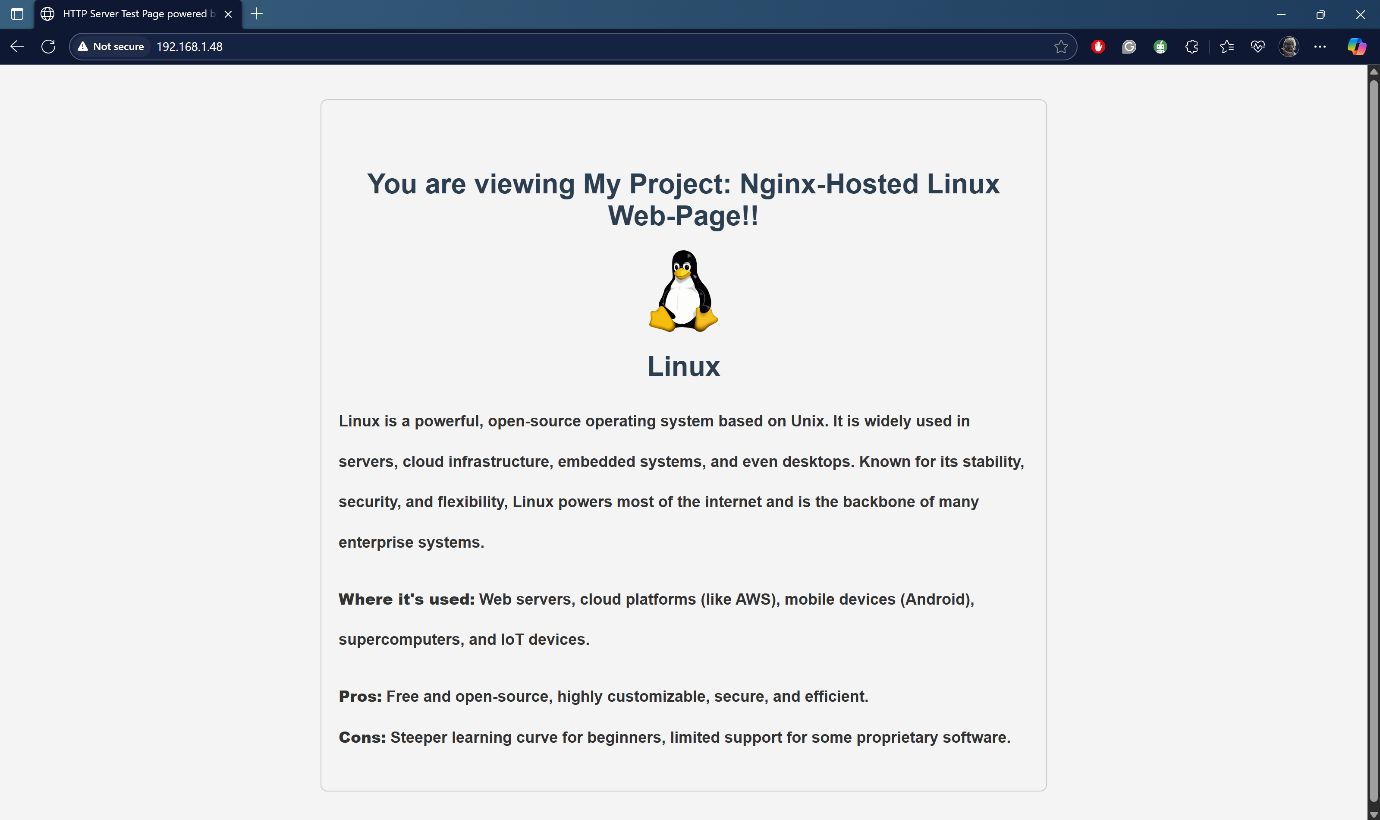
1. **Access from LAN**

**ip a or hostname -I --**🡪 **to find IP like http://192.168.1.48/**

**Results :**

* **Successfully served a custom HTML page via Nginx**
* **Verified access from local and LAN devices**
* **Ensured secure file permissions and firewall configuration**

**Output :**

****