Setting Up a Secure Nginx Web Server with User Authentication and Logging

This guide demonstrates how to install and configure Nginx on Ubuntu, create a welcome page, implement user authentication, and configure logging for access attempts.

1. Install Nginx:

Update package lists and install Nginx.

```
sudo apt-get update
sudo apt-get install nginx
```

2. Create a Welcome Page:

Create an HTML file named 'index.html' in the document root.

```
echo "<h1>Welcome to Operating Systems Lab</h1>" > /var/www/html/index.html (or other HTML names)
```

3. Implement User Authentication:

3.1 Install htpasswd Utility:

```
Install the 'apache2-utils' package to access the 'htpasswd' tool.
sudo apt-get install apache2-utils
```

3.2 Create Password File:

Create a password file named '.htpasswd' in the '/etc/nginx' directory. Replace 'user' with your desired username and enter a secure password.

```
sudo htpasswd -c /etc/nginx/.htpasswd user
```

3.3 Configure Nginx for Authentication:

Open the Nginx configuration file (usually '/etc/nginx/sites-available/default'). Add the following lines within the 'location' block to enable authentication and specify the password file.

```
auth_basic "Restricted Content";
auth_basic_user_file /etc/nginx/.htpasswd;
```

3.4 Restart Nginx:

Apply the changes by restarting Nginx.

```
sudo systemctl restart nginx
```

4. Configure Logging:

Nginx logs access attempts to '/var/log/nginx/access.log'. View the last few lines:

```
tail /var/log/nginx/access.log
```

4.1 For continuous monitoring, use the '-f' option:

```
tail -f /var/log/nginx/access.log
```