Assignment Name: DNS, DHCP, Web Servers & MySQL

Duration : 2 weeks (Starting from July 20th , 2021 to 03-08-2021)

Operation system: Ubuntu

Note: Completed assignments should be submitted via http://school.wso2.com.

Assignment answer file must be named as Linux_LT-2021.pdf

- Register a freenom.com domain with your student id (You will receive your Student ID within this week). The TLD must be .ml. Do not change the nameservers, It must be Freenom's default name servers.
  - Ex; LT-2021-001.ml - Domain Registering

    https://www.freenom.com/en/index.html
- Add DNS A records to point to your GCP instance. (You will be hosting your website on this instance) - DNS Records

- You need to use an email forwarding service, (I tested with https://improvmx.com/). The goal is to receive emails sent to admin@lt-2021-001.ml (Replace with your Domain) to your personal email. If needed, think about the email security hardening steps as well. - DNS Records

- I (kalana@wso2.com) will send an email to this newly created email address with a unique string. Ie: "student1111"

- You need to save that string and configure your web browser to achieve the following end results.
  - When we head over to http://lt-2021-001.ml it must be redirected to https version of the site.
    - There are free SSL Certificate issuers. (ie: letsencrypt) - HTTPS with TSL
  - http://lt-2021-001.ml should host a Simple Python file server with dummy files which is running on port 8081. (We should be able to access the file server by

typing both http://lt-2021-001.ml and http://lt-2021-001.ml:8081) - Reverse Proxy Configuration

- There must be a path with the unique string you received and in that path there should be your student ID in plain text. (Path Ie: https://lt-2021-001.ml/student1111.)- - Web server Configuration

(I have added several simple examples on the slide No 37)

- There must be a path /secret and it must be password protected using HTTP Basic Authentication. Both the user name and the password should be “wso2”. - Nginx Modules

Deliverables:

1. **A PDF containing below data. Ie: Linux_LT-2021.pdf**
    a. **A Screenshot of the DNS records.**
    b. **The Public key used to enable HTTPS on the website.**
    c. **Edited Nginx Host configuration files. (You can use a public Github repo add the link to the Document)**
2. **An HTTPS enabled working site with the unique DNS name with all the aforementioned paths and conditions.**
3. **A screenshot of the result generated by https://www.ssllabs.com/ssltest/ after completing all the steps.**

- You can do your own research and do web server security hardening if you like.
- N:B- No step should cost you any money or even Trials with credit cards.