

Assignment 1 Configure and enable Nginx to use TLS and generate certificate

1. Run the command :

```
Command Prompt - ssh rahu X + v
Microsoft Windows [Version 10.0.22621.2215]
(c) Microsoft Corporation. All rights reserved.

C:\Users\rahu>ssh rahu@192.168.56.101
rahu@192.168.56.101's password:
Last login: Sun Sep  3 10:08:41 2023 from 192.168.56.1
~sh-4.2$ openssl req -x509 -newkey rsa:2048 -nodes -keyout mm.pem -out mmcert.pem -sha256 -days 365
Generating a 2048 bit RSA private key
.....+++
...+++
writing new private key to 'mm.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [XX]:IN
State or Province Name (full name) []:Telangana
Locality Name (eg, city) [Default City]:Hyderabad
Organization Name (eg, company) [Default Company Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:
Email Address []:
~sh-4.2$
```

2. Modify Nginx configuration

```
Command Prompt - ssh rahu X + v
http {
    log_format main '$remote_addr - $remote_user [$time_local] "$request" '
        '$status $body_bytes_sent "$http_referer" '
        '"$http_user_agent" "$http_x_forwarded_for"';

    access_log /var/log/nginx/access.log main;

    sendfile        on;
    tcp_nopush      on;
    tcp_nodelay      on;
    keepalive_timeout 65;
    types_hash_max_size 4096;

    include /etc/nginx/mime.types;
    default_type application/octet-stream;

    # Load modular configuration files from the /etc/nginx/conf.d directory.
    # See http://nginx.org/en/docs/nginx_core_module.html#include
    # for more information.
    include /etc/nginx/conf.d/*.conf;

    server {
        listen      80;
        listen 443 ssl;
        listen      [::]:8080;
        server_name localhost;
        ssl_certificate /home/rahu/mmcert.pem;
        ssl_certificate_key /home/rahu/mm.pem;
        root /usr/share/nginx/html;

        # Load configuration files for the default server block.
        -- INSERT --
    }
}
```

3. Restart the nginx server
4. Launch the server from your browser

Assignment 2 Configure Firewall rules to prevent remote access

1. Sudo yum install -y ufw

```
Command Prompt - ssh rahu x + v
-sh-4.2$ sudo yum install -y epel-release
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
epel/x86_64/metalink | 7.4 kB 00:00
* base: centos.excellmedia.net
* epel: epel.excellmedia.net
* extras: centos.excellmedia.net
* updates: centos.excellmedia.net
base | 3.6 kB 00:00
extras | 2.9 kB 00:00
mysql-connectors-community | 2.6 kB 00:00
mysql-tools-community | 2.6 kB 00:00
mysql80-community | 2.6 kB 00:00
nginx | 2.9 kB 00:00
updates | 2.9 kB 00:00
Package epel-release-7-14.noarch already installed and latest version
Nothing to do
-sh-4.2$ sudo yum install -y ufw
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
* base: centos.excellmedia.net
* epel: epel.excellmedia.net
* extras: centos.excellmedia.net
* updates: centos.excellmedia.net
Resolving Dependencies
--> Running transaction check
--> Package ufw.noarch 0:0.35-9.el7 will be installed
--> Finished Dependency Resolution

Dependencies Resolved


=====
=====
```

2. Check the status of ufw using “sudo ufw status”

```
Parent stopped and disabled on system startup
-sh-4.2$ sudo ufw status
Status: inactive
-sh-4.2$
```

3. Enable the ufw using the command “sudo ufw enable”

```
-sh-4.2$ sudo ufw status
Status: inactive
-sh-4.2$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
-sh-4.2$
```



4. Check the status of ufw using “sudo ufw status”

```
-sh-4.2$ sudo ufw status
Status: inactive
-sh-4.2$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
-sh-4.2$ sudo ufw status
Status: active

To Action From
--
SSH ALLOW Anywhere
224.0.0.251 mDNS ALLOW Anywhere
SSH (v6) ALLOW Anywhere (v6)
ff02::fb mDNS ALLOW Anywhere (v6)

-sh-4.2$
```

5. Try to access your server from the machine where the ip address is blocked the site cant be reached error should display.

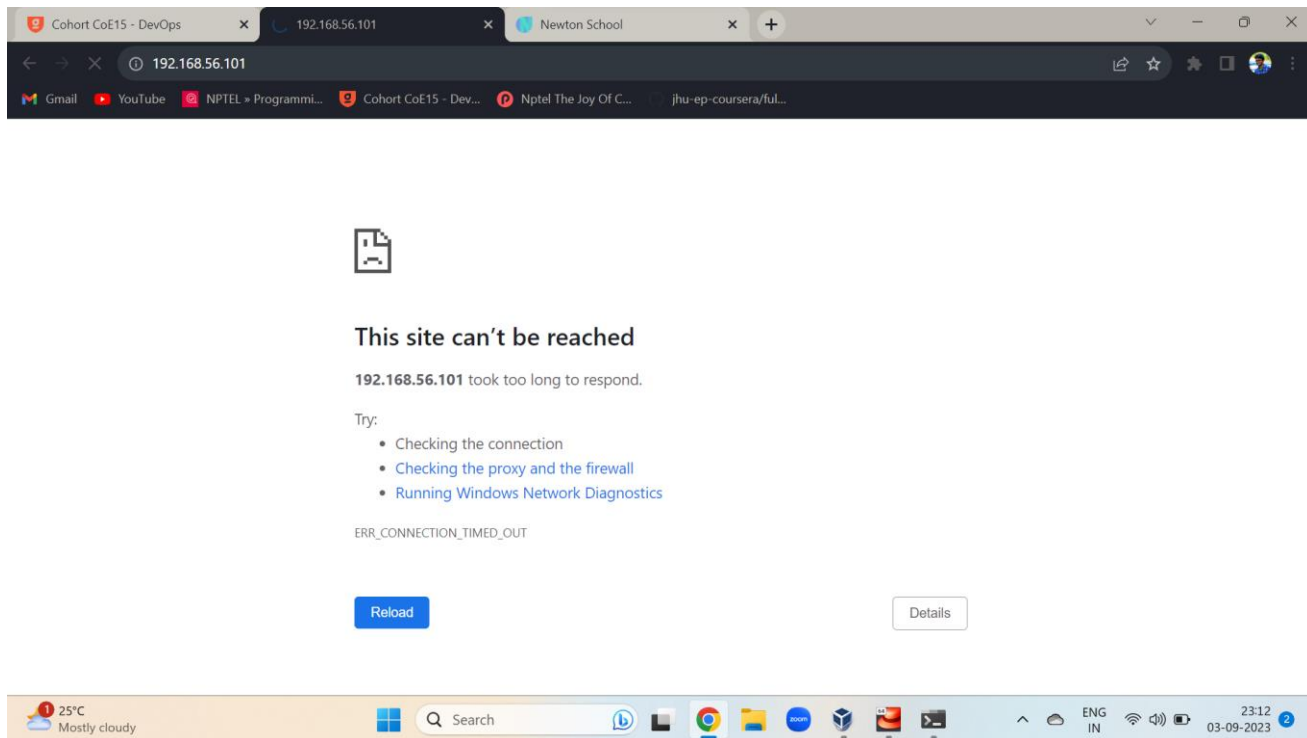
```
Transaction test succeeded
Running transaction
  Installing : ufw-0.35-9.el7.noarch 1/1
  Verifying : ufw-0.35-9.el7.noarch 1/1

Installed:
  ufw.noarch 0:0.35-9.el7

Complete!
-sh-4.2$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
-sh-4.2$ sudo ufw disable
Firewall stopped and disabled on system startup
-sh-4.2$ sudo ufw status
Status: inactive
-sh-4.2$ sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
-sh-4.2$ sudo ufw status
Status: active

To Action From
--
SSH ALLOW Anywhere
224.0.0.251 mDNS ALLOW Anywhere
SSH (v6) ALLOW Anywhere (v6)
ff02::fb mDNS ALLOW Anywhere (v6)

-sh-4.2$ sudo ufw deny from 192.168.56.101
Rule added
-sh-4.2$
```



6. Now if you try to access the server it should allow
7. Deny a port number using command “ sudo ufw deny portnumber “