

Karthik Pradeep Hegadi

2KE20CS032

Assignment 19

Understood. To follow the provided instructions and create the files/directory using the same name and case as provided in the task steps, please provide me with the specific names and case instructions for the files/directory you want to create.

Network Security

Assignment 1: Networking Security - Assignment 1 - Configure and enable Nginx to Use TLS and generate a certificate.

```
$~ openssl req -x509 -newkey rsa:2048 -nodes -keyout mm.pem -out mmcrt.pem -sha256 -days 365
```

Options

req: Certificate Signing Request

X509: Certificate to be x509 format

newkey rsa:2048 : New certificate request and private key. RSA key size in bits

nodes: No DES(Data Encryption Standard). Generated private key will not be encrypted

keyout: Private key file name

out: Output file name. In this case, it is certificate

Step 1: Generate the certificate

Step 2: Verify it

```
lusy@localhost.localdomain /etc/nginx (0.021s)
cd certificates/ 

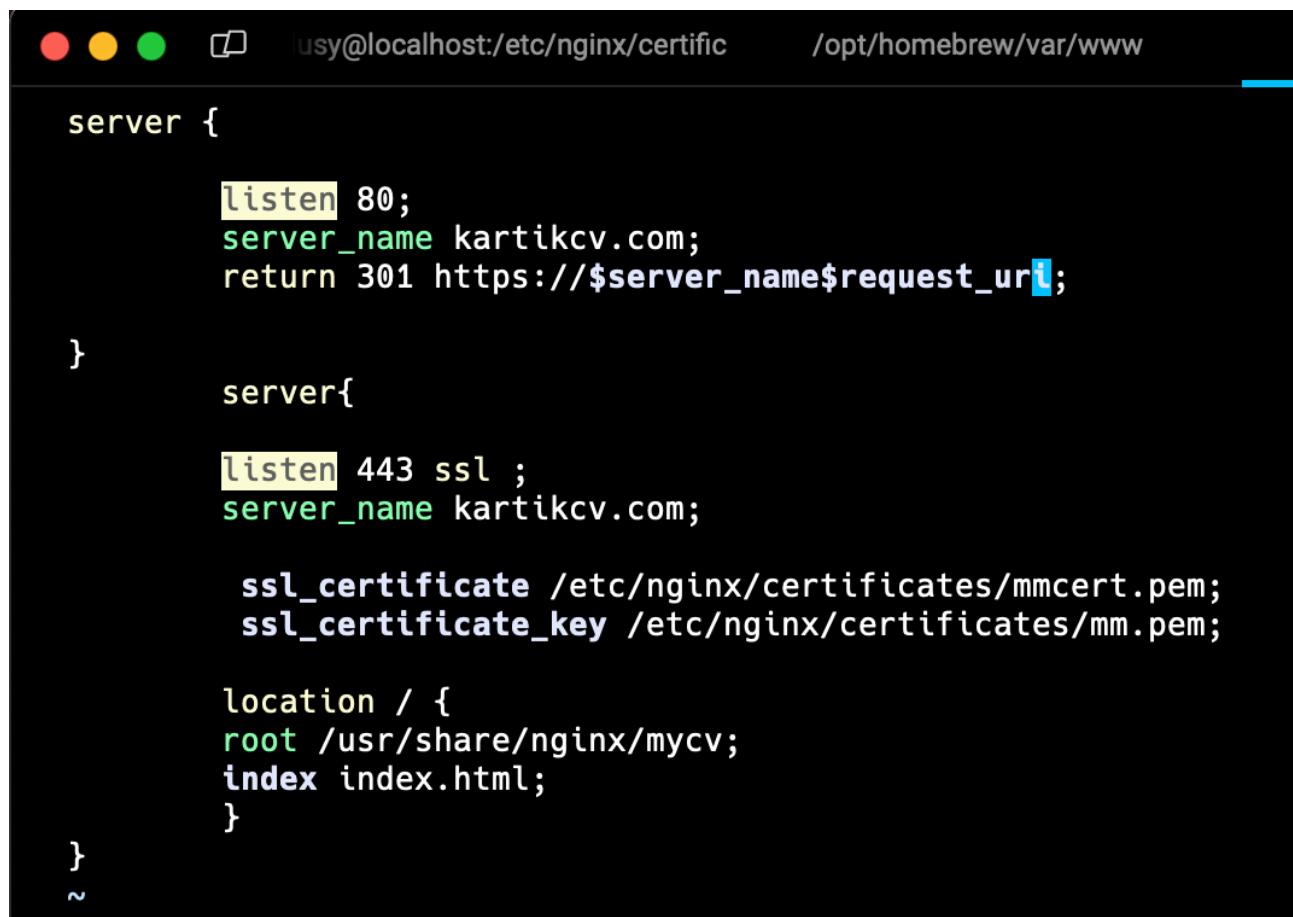
lusy@localhost.localdomain /etc/nginx/certificates (0.022s)
tree
.
└── mmcrt.pem
    └── mm.pem

0 directories, 2 files
```

Step 3: Give permission to the directory to access the folder by master process

```
lusy@localhost.localdomain /etc/nginx (0.057s)
sudo chmod 777 /etc/nginx/certificates/
```

Step 4: Make changes in config files



The screenshot shows a terminal window with a dark background and light-colored text. At the top, there are three colored icons (red, yellow, green) followed by the user information: usy@localhost:/etc/nginx/certific and the path /opt/homebrew/var/www. Below this, the terminal displays the Nginx configuration file. The configuration includes a server block for port 80 and another for SSL port 443. The SSL block specifies the certificate and key files located in the certificates directory.

```
server {
    listen 80;
    server_name kartikcv.com;
    return 301 https://$server_name$request_uri;
}

server{
    listen 443 ssl ;
    server_name kartikcv.com;

    ssl_certificate /etc/nginx/certificates/mmcrt.pem;
    ssl_certificate_key /etc/nginx/certificates/mm.pem;

    location / {
        root /usr/share/nginx/mycv;
        index index.html;
    }
}
```

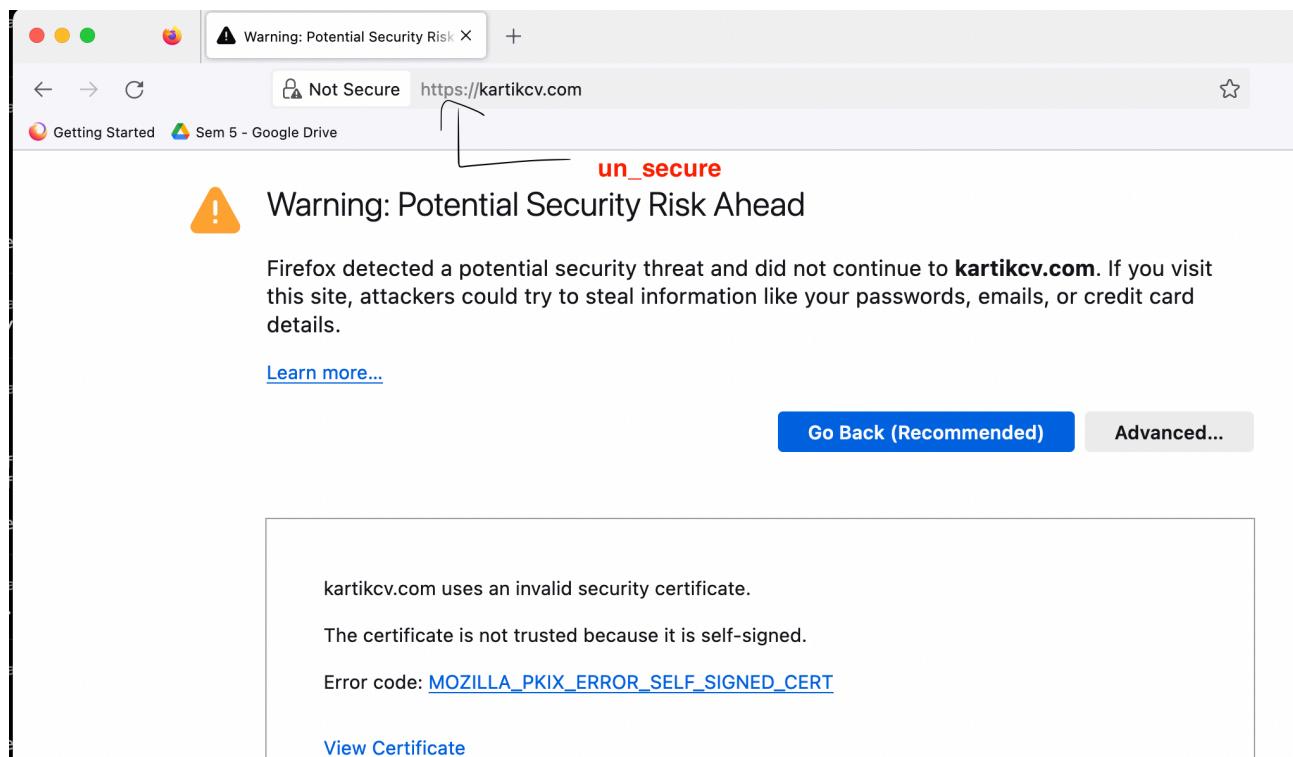
Step 5: Verify using the curl

```
lusy@localhost.localdomain /etc/nginx/conf.d (0.034s)
curl kartikcv.com

<html>
<head><title>301 Moved Permanently</title></head>
<body>
<center><h1>301 Moved Permanently</h1></center>
<hr><center>nginx/1.22.1</center>
</body>
</html>
```

```
lusy@localhost.localdomain /etc/nginx/conf.d
```

Step 6 Thus we can see her “The s is added to HTTP” which shows that the connection is secure



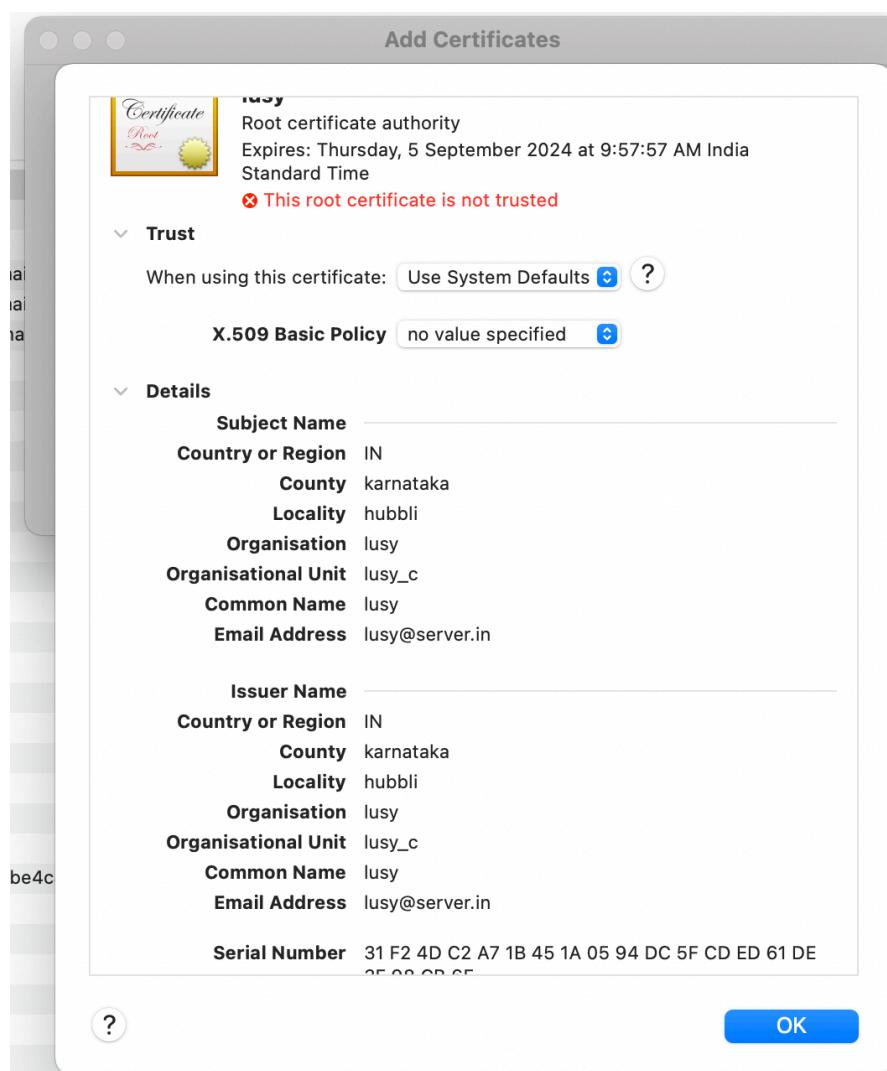
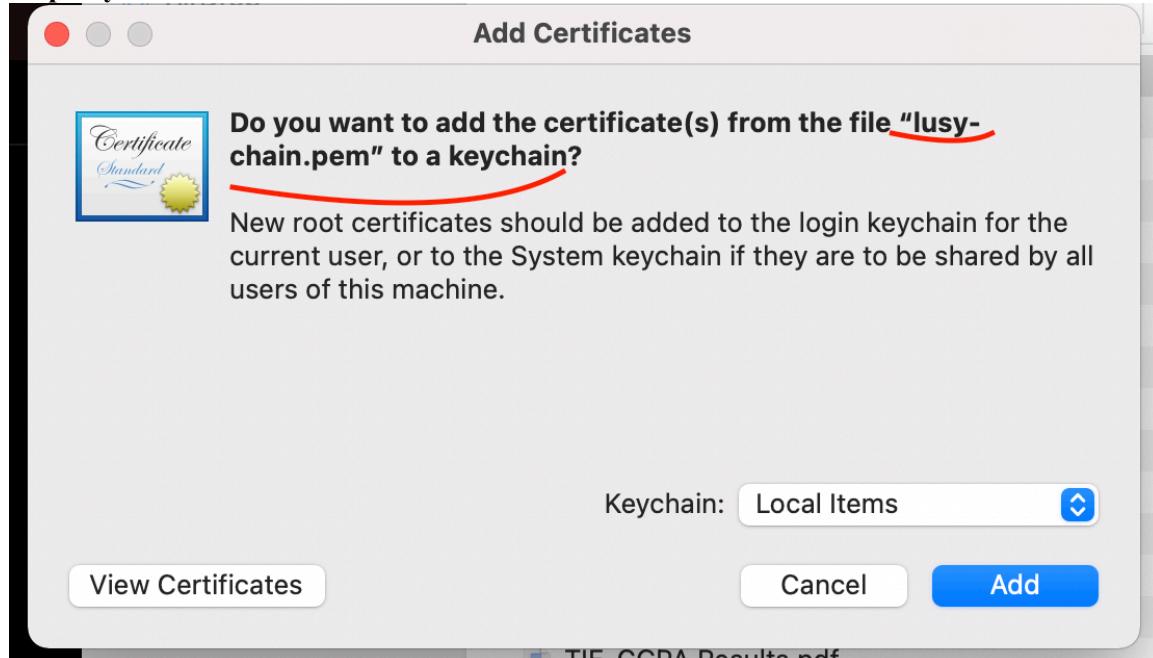
Step 7: Just click on advance and view the generated certification.

Certificate

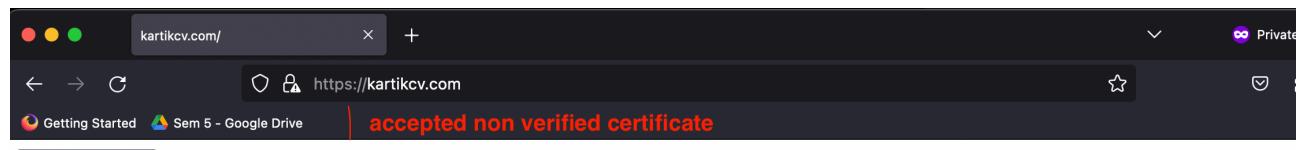
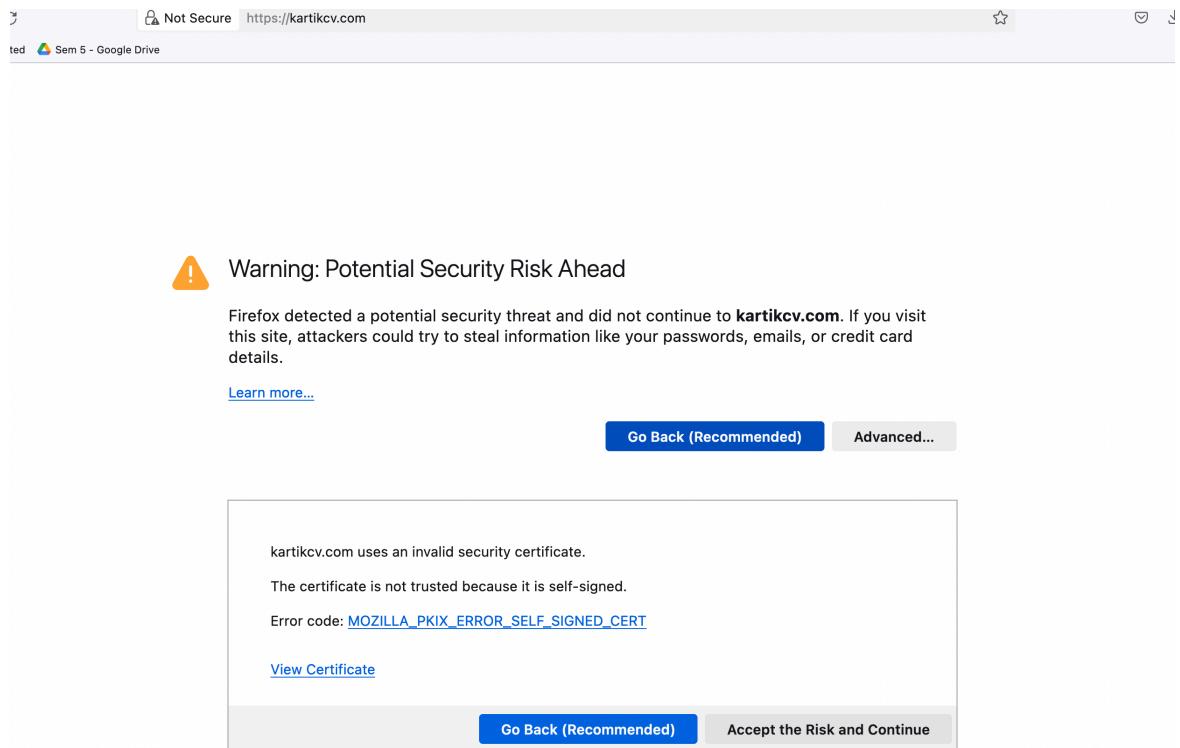
lusy	
Subject Name	
Country IN	
State/Province karnataka	
Locality hubbli	
Organization lusy	
Organizational Unit lusy_c	
Common Name lusy	
Email Address lusy@server.in	
Issuer Name	
Country IN	
State/Province karnataka	
Locality hubbli	
Organization lusy	
Organizational Unit lusy_c	
Common Name lusy	
Email Address lusy@server.in	
Validity	
Not Before	Wed, 06 Sep 2023 04:27:57 GMT
Not After	Thu, 05 Sep 2024 04:27:57 GMT
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	CE:33:A0:3A:C9:14:E0:27:54:DB:65:B9:41:75:B0:13:48:C3:73:D9:40:75:...

Not Before	Wed, 06 Sep 2023 04:27:57 GMT
Not After	Thu, 05 Sep 2024 04:27:57 GMT
Public Key Info	
Algorithm	RSA
Key Size	2048
Exponent	65537
Modulus	CE:33:A0:3A:C9:14:E0:27:54:DB:65:B9:41:75:B0:13:48:C3:73:D9:40:75:...
Miscellaneous	
Serial Number	31:F2:4D:C2:A7:1B:45:1A:05:94:DC:5F:CD:ED:61:DE:3F:98:CB:6F
Signature Algorithm	SHA-256 with RSA Encryption
Version	3
Download	PEM (cert) PEM (chain)
Fingerprints	
SHA-256	7D:16:A6:20:3C:4E:81:C4:D3:F9:D8:BF:C4:55:CB:E7:F7:40:C3:F1:AB:5B...
SHA-1	A8:06:DE:49:A7:1F:D4:5D:55:BB:E3:A3:B9:69:33:43:11:F8:66:A4
Basic Constraints	
Certificate Authority	Yes
Subject Key ID	
Key ID	A3:54:AD:4B:2C:21:92:05:91:3F:8C:08:60:84:86:70:29:71:1C:03
Authority Key ID	
Key ID	A3:54:AD:4B:2C:21:92:05:91:3F:8C:08:60:84:86:70:29:71:1C:03

Step 8: you can Download the certificate to view it.



Step 9: accept and continue then you can see your page.



Hello, I'm Anthony Anaedu.

Software Developer, Technology enthusiast, EE Engineer.

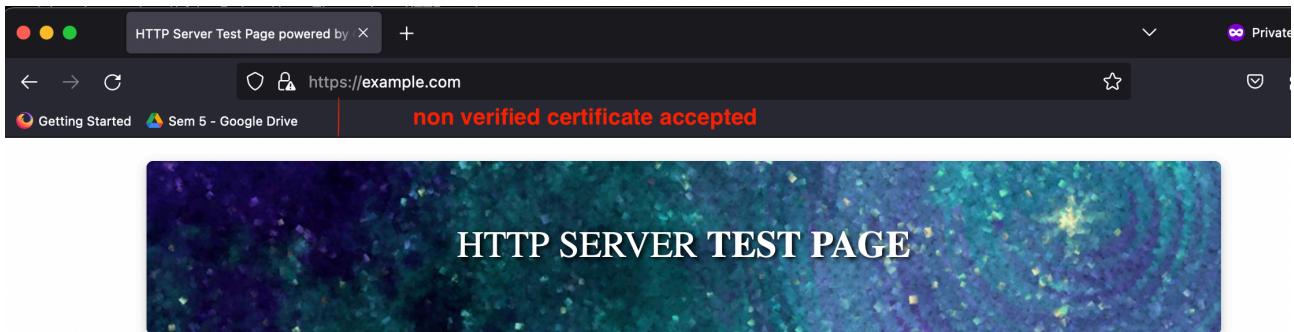
[Twitter](#) [FreeCodeCamp](#) [Github](#)

ABOUT



—TRY

(I have used another test page) just for check it.



This page is used to test the proper operation of the HTTP server after it has been installed. If you can read this page it means that this site is working properly. This server is powered by [CentOS](#).

If you are a member of the general public:

The website you just visited is either experiencing problems or is undergoing routine maintenance.

If you would like to let the administrators of this website know that you've seen this page instead of the page you expected, you should send them e-mail. In general, mail sent to the name "webmaster" and directed to the website's domain should reach the appropriate person.

Assignment 2 : Configure Firewall rules to prevent remote access.

1: Install the firewall into your terminal, run these commands in your terminal sudo yum install -y epel-release

```
lusy@localhost.localdomain /etc/nginx/conf.d (0.628s)
sudo yum install -y epel-release
Last metadata expiration check: 2:30:45 ago on Wed 06 Sep 2023 10:28:16 AM IST.
Package epel-release-9-7.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

2.sudo yum install -y ufw

```
lusy@localhost.localdomain /etc/nginx/conf.d (0.479s)
sudo yum install -y ufw
Last metadata expiration check: 2:31:20 ago on Wed 06 Sep 2023 10:28:16 AM IST.
Package ufw-0.35-24.el9.noarch is already installed.
Dependencies resolved.
Nothing to do.
Complete!
```

3.Check the status of ufw using "sudo ufw status" (Inactive)

```
lusi@localhost.localdomain /etc/nginx/conf.d (0.131s)
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)
```

4.Enable the ufw using the command "sudo ufw enable"

```
lusi@localhost.localdomain /etc/nginx/conf.d (3.888s)
sudo ufw enable
Command may disrupt existing ssh connections. Proceed with operation (y|n)? y
Firewall is active and enabled on system startup
```

5.Check the status of ufw using "sudo ufw status" (Active)

```
lusi@localhost.localdomain /etc/nginx/conf.d (0.296s)
```

```
sudo ufw deny from 192.168.43.23
```

```
Rule added
```

```
lusi@localhost.localdomain /etc/nginx/conf.d (0.272s)
```

```
sudo ufw deny 80
```

```
Rule added
```

```
Rule added (v6)
```

6. (Try to access your server (nginx) from the machine where the Ip address is blocked the site can't be reached error should display

```
lusy@localhost.localdomain /etc/nginx/conf.d (0.296s)
sudo ufw deny from 192.168.43.23
```

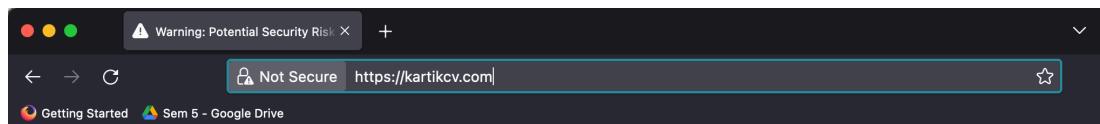
Rule added

```
lusy@localhost.localdomain /etc/nginx/conf.d (0.272s)
sudo ufw deny 80
```

Rule added

Rule added (v6)

7.(Now if you try to access the server it should allow)



8.Deny a port number using command " sudo ufw deny portnumber" (rule added (Try to access the port from outside it should be blocked)

```
lusi@localhost.localdomain /etc/nginx/conf.d (0.403s)
sudo ufw allow 80

lusi@localhost.localdomain /etc/nginx/conf.d (0.134s)
sudo ufw status
Status: active

To           Action    From
--           -----    ---
SSH          ALLOW     Anywhere
224.0.0.251 mDNS    ALLOW     Anywhere
Anywhere      ALLOW     192.168.43.23
80           ALLOW     Anywhere
SSH (v6)      ALLOW     Anywhere (v6)
ff02::fb mDNS  ALLOW     Anywhere (v6)
80 (v6)       ALLOW     Anywhere (v6)

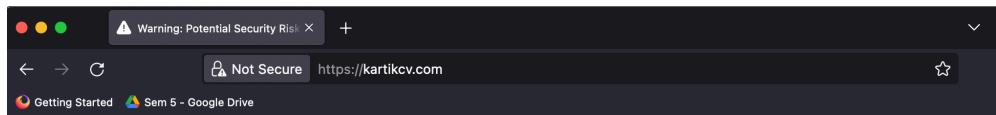
lusi@localhost.localdomain /etc/nginx/conf.d (0.351s)
sudo ufw allow from 192.168.43.23 port 80
Rule added

lusi@localhost.localdomain /etc/nginx/conf.d (3.679s)
sudo ufw reload
Firewall reloaded

lusi@localhost.localdomain /etc/nginx/conf.d (0.373s)
sudo ufw deny from 192.168.43.23 port 80
Rule updated

lusi@localhost.localdomain /etc/nginx/conf.d (3.747s)
sudo ufw reload
Firewall reloaded

lusi@localhost.localdomain /etc/nginx/conf.d
```



Warning: Potential Security Risk Ahead

Firefox detected a potential security threat and did not continue to **kartikcv.com**. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.

[Learn more...](#)

[Go Back \(Recommended\)](#)

[Advanced...](#)

kartikcv.com uses an invalid security certificate.