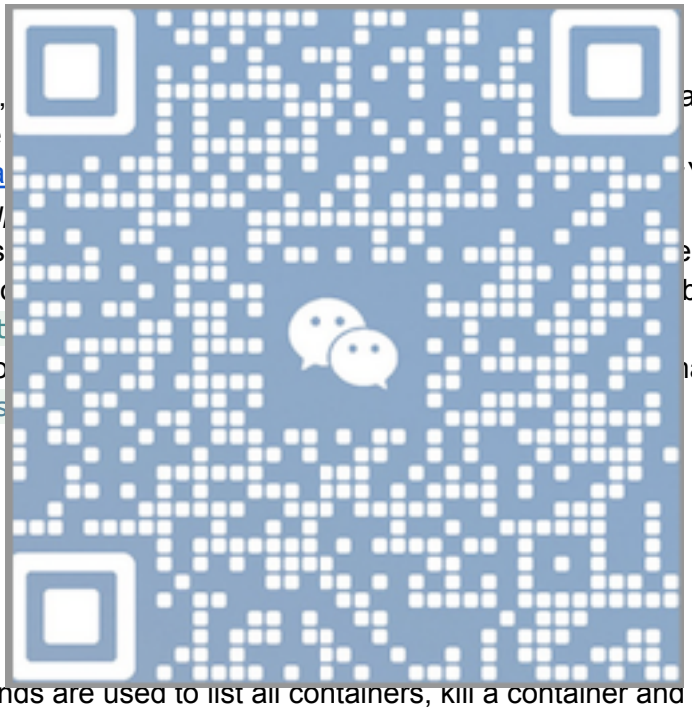
Course Title: Cyber Security
Course Code: COMP SCI 1500
Final Assignment
Weighting: 15%

Introduction

In this assignment, you are provided with a docker container which has an Apache Web Server and your task is to scan the web server for vulnerabilities and patch the vulnerabilities. For this assignment, you will submit a report with screenshots and explanations wherever specified in this document as well as answer to the questions in this document.

Pre-Requisites

You will need to set up the following to complete this assignment. Use your Kali virtual machine to set it up.



1. **Docker** - First, al Machine. To do this, follow the https://www.ka *You might need to run sudo apt u*
2. **Nikto** - Nikto s e using some other distributi b command:
   `git clone ht`
3. **testssl.sh** - To nand:
   `sudo apt ins`

Instructions

1. **Setting Up**

Clean Up
The following commands are used to list all containers, kill a container and remove any unused network. Try running these commands to clean up your environment if you have other docker containers running on your system.

```
Command: docker ps -a
Command: docker kill <id>
Command: docker network prune
```

Setup the docker container
We first pull the docker container using the following command,

```
Command: docker pull joeltmenayathil/apachescan:latest
```

Now, run the docker container using the following command,

```
Command: docker run --name apachescan -p 80:80 -p 443:443 -it
joeltmenayathil/apachescan
```

The parameters are as follows:

--name apachescan: Set the container name to apachescan
-p 80:80: Bind port 80 of container to port 80 of host VM
-p 443:443: Bind port 443 of container to port 443 of host VM
-it: Start the container in interactive mode
joeltmenayathil/apachescan: Name of the container to run.

Note: You will be prompted for the admin password for the container. The password for the admin user is admin.
This command will start a pre-configured apache server and ssh server in the container.

Exit the container using the command(this will shut down the container as well):

```
Command: exit
```

Start the container usi

```
Command: docker s
```

Note down the ip addr d the IP for sshing into the system at a la

```
Command: docker i
```

Verify that the apache

```
Command: curl htt
```

Screenshot 1: Take a erver.

Verify that you can ssh

```
Command: ssh admin@<container ip>
```

Exit the container.

2. **Generating a Self Signed Certificate**

Log into the docker container as admin with SSH using the command:

```
Command: ssh admin@<container ip>
```

Generate a private key and self signed certificate for the container using the command:

```
Command: sudo openssl req -x509 -nodes -days 365 -newkey rsa:2048
-keyout apache-server.key -out apache-server.crt
```

You can use any random information for generating the certificate. Run the command below and take a screenshot of the certificate:

```
Command: openssl x509 -in apache-server.crt -text -noout
```

Screenshot 2: Take a screenshot of the certificate

This should have generated a private key and certificate in your current folder. Complete the following to get the certificate working on your web server

- Copy the private key apache-server.key to /etc/ssl/private
- Copy the certificate apache-server.crt to /etc/ssl/certs

Once the above step is complete, restart the apache server by running the following,

```
Command: sudo service apache2 restart
```

3. **Scanning with**

Download the latest v lready installed one in Kali Linux.

Scan the apache webs

```
Command: perl ./n
```

Or

```
Command: nikto -h
```

Screenshot 3: Take a Start Time field as well)

Scan the apache web server for SSL related issues using the command:

```
Command: testssl --htmlfile scan_output.html https://<ip-address>
```

4. **Fixing the Vulnerabilities**

Nikto

You need to fix any 5 of the following vulnerabilities found in the above scan:

1. The Content-Encoding header is set to "deflate" this may mean that the server is vulnerable to the BREACH attack.
2. The anti-clickjacking X-Frame-Options header is not present.

3. The X-XSS-Protection header is not defined.
4. The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
5. The X-Content-Type-Options header is not set.
6. Server may leak inodes via ETags, header found with file /.
7. Fix /test/ and /icons/README issues by disabling directory indexing

Scan the apache web server hosted in the container with Nikto after fixing 5 of the above Vulnerabilities.

testssl.sh

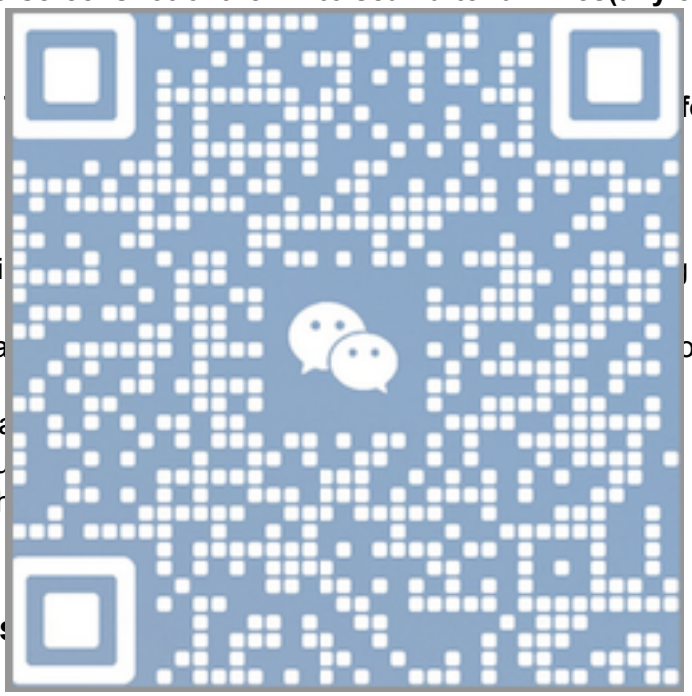
You need to fix the following vulnerabilities:

1. Configure the server to use the Cipher Suite: ECDHE-RSA-AES256-GCM-SHA384
2. Make sure that TLSv1.3 protocol is enabled

Screenshot 4.1 - 4.5: Take a screenshot for every fix you made(You can combine fixes into a single screenshot as well)

Screenshot 5: Take a screenshot of the Nikto scan after all fixes(any 5 fixes) for the Nikto section

Screenshot 6.1, 6.2: for TLS/SSL



Final Report

For the Final Report, i details.

Provide detailed expla llowing three key questions:

1. Why is this a
2. How did you
3. How does th

Grading(15 Point

1 points - Lab Setup
1 points - Generating a self signed certificate
1 points - Scanning with Nikto and testssl.sh
6 points - Fixing vulnerabilities and final scan
6 points - Provide proper explanation for each fix in lab report