College of Science and Technology

Royal University of Bhutan

LESSON – 21

WEB SERVER - 2

LEARNING OUTCOMES

- Web server Security
- Apache Directories
- Virtual Hosts
- Troubleshooting Apache

Standard Apache Security Configuration

- How?
  - You can configure several layers of security for the Apache web server.
  - Firewalls based on the iptables [limit access to specific hosts]. Now, **firewalld**
  - Security based on rules in Apache configuration file [Limit access to specific users, groups, and hosts]

- Ports and Firewalls?
  - With the Listen and NameVirtualHost directives the standard communication ports for both HTTP & HTTPS protocols, 80 and 443 are specified.
  - To allow external communication through noted ports, set both ports as trusted services in Firewall configuration tool.
  - If HTTP and HTTPS are configured on nonstandard ports, adjust the associated firewalld rules accordingly

Standard Apache Security Configuration

- Ports and Firewalls (Contd..)
  - It would be always appropriate to set up custom rule to limit access to one or more systems or networks.
  - For example: if you want to allow network 192.168.1.0/24 except 192.168.1.200 over port 80, then following rules have to apply in iptables or firewalld:
  - **Firewalld rules**:

```
#firewall-cmd - -zone=work - -add-source=192.168.1.200; firewall-cmd -  zone=work - -
add-port=80/tcp
```

Standard Apache Security Configuration

- Security Within Apache
  - Security setting within security file /etc/apache2/conf.d/security

ServerTokens Prod

- Limits page information displayed to following when non-existing server access:

Apache/[version] [OS Name] Server at localhost Port 80

If changed to:

ServerTokens Full

- Limits page information displayed to following when non-existing server access:

Apache/2.2.17 CentOS DAV/2 mod_ssl/2.2.17 OpenSSL/1.0.0-fips .. Server at localhost Port 80

What will happen? ***Your Server will face addition risks.***

Standard Apache Security Configuration

- Security Within Apache
  - Using Curl Command

    - is the most common and versatile CLI tool for this task. It's often pre-installed on Linux and macOS.

    You have two main options with cURL:

    1. To get only the headers (no body): Use the -I
       curl -I https://example.com

    2. To get the headers and body: Use the -i

       curl -i https://example.com

Standard Apache Security Configuration

- User-Based Security
  - To set basic authentication, need an AuthType Basic directive first
  - To refer to a web server password database you need a htpasswd file in /etc/apache2/ directory

    ```
    sudo htpasswd -c /etc/apache2/.htpasswd jiwan
    ```
  - To limit the site access to a single user named jiwan, you will need a Require user jiwan directive
  - Example code under <Virtual Host> container:

```
<Directory "/var/www/your_domain">
AuthType Basic
AuthName "Restricted Content"
AuthUserFile /etc/apache2/.htpasswd
Require valid-user
</Directory>
```

Note: When accessing through Web Browser, you’re prompted for a username and password

- Reference: https://www.digitalocean.com/community/tutorials/how-to-set-up-password-authentication-with-apache-on-ubuntu-20-04

Virtual Host

- Regular and Secure Virtual Hosts
  - Multiple sites for single IP address.
  - Virtual hosts can be configured both for normal and secure web server.
  - **<VirtualHost>** container is used to specify the options that pertain to a particular virtual host.
  - The Standard Virutal Host:
    - Activate the virtual host directive :

      #NameVirtualHost *:80

- For multiple name-based virtual hosts. Otherwise replace by IP address

Virtual Host

- Regular and Secure Virtual Hosts
  - The Standard Virtual Host:
    - Activate the virtual host directive :

```
<Directory “/var/www/html/example1”>
        options Indexes FollowSymlinks
        AllowOverride All
        Order allow,deny
        Allow from all
</Directory>

<VirtualHost *:80>
        ServerAdmin admin@cst.bt
        DocumentRoot /var/www/html/example1
        ServerName www.cst.bt
        ErrorLog logs/example1.com-error_log
        CustomLog logs/example1.com-access_log common
</VirtualHost>
```

  - Check apache2 config:

```
sudo apache2ctl configtest
```

Virtual Host

- Secure Virtual Hosts
  - The file location: /etc/apache2/site-available/000-default-ssl.conf:
  - Before editing ssl.conf file, do backup the file
  - The following command loads the SSL module

```
sudo a2enmod ssl
```

  - Make sure that Listen directive is active

```
Listen 443
```

/etc/apache2/ports.conf

** Listen 443   -> make sure it is enabled*

Virtual Host

- Secure Virtual Hosts cont.
  - Include a NameVIrtualHost directive for Port 443:
    *NameVirtualHost *:443*
  - In ssl.conf file, Change the <VirtualHost _default_:433> directive to

    *<virtualHost *:443>*
  - Example:

```
<Directory “/var/www/html/example1”>
        options Indexes FollowSymlinks
        AllowOverride All
        Order allow,deny
        Allow from all
</Directory>

<VirtualHost *:443>
        ServerAdmin admin@cst.bt
        DocumentRoot /var/www/html/example1
        ServerName www.cst.bt
        ErrorLog logs/example1.com-error_log
        CustomLog logs/example1.com-access_log common
</VirtualHost>
```

Virtual Host

- Syntax Checker
  - The apachectl restart commands will reveal the syntax problems.
    The following command checks the work that you have done in Apache configuration file: `[root@cst ~]#sudo apache2ctl configtest`
  - Apache Troubleshooting: Some Apache errors fall into the following categories:
    - Error Message about an inability to bind to an address: Another network process may already be using the default http port (80)
    - Network address or routing errors: double-check network settings
    - Apache isn't running: check error_log file
    - Apache isn't running after a reboot: use systemctl enable apache2 command
    - You need to stop Apache: use kill –TERM or alternatively you can use apache2l stop command

Reference

- https://hostadvice.com/how-to/web-hosting/ubuntu/how-to-harden-your-apache-web-server-on-ubuntu-18-04/

- https://linuxconfig.org/setting-up-a-secure-apache-server-on-ubuntu-24-04

- https://medium.com/@ravipatel.it/step-by-step-guide-creating-installing-and-configuring-ssl-certificate-on-apache-server-vm-7587193dbef6

SUMMARY

- **You have learnt;**
  - How to configure standard Apache Web server and secure web server
  - Configure Virtual hosts to hosts multiple web sites in a single IP Apache Server
  - How to troubleshoot Apache quickly