Nust Cyber Security Team 2020

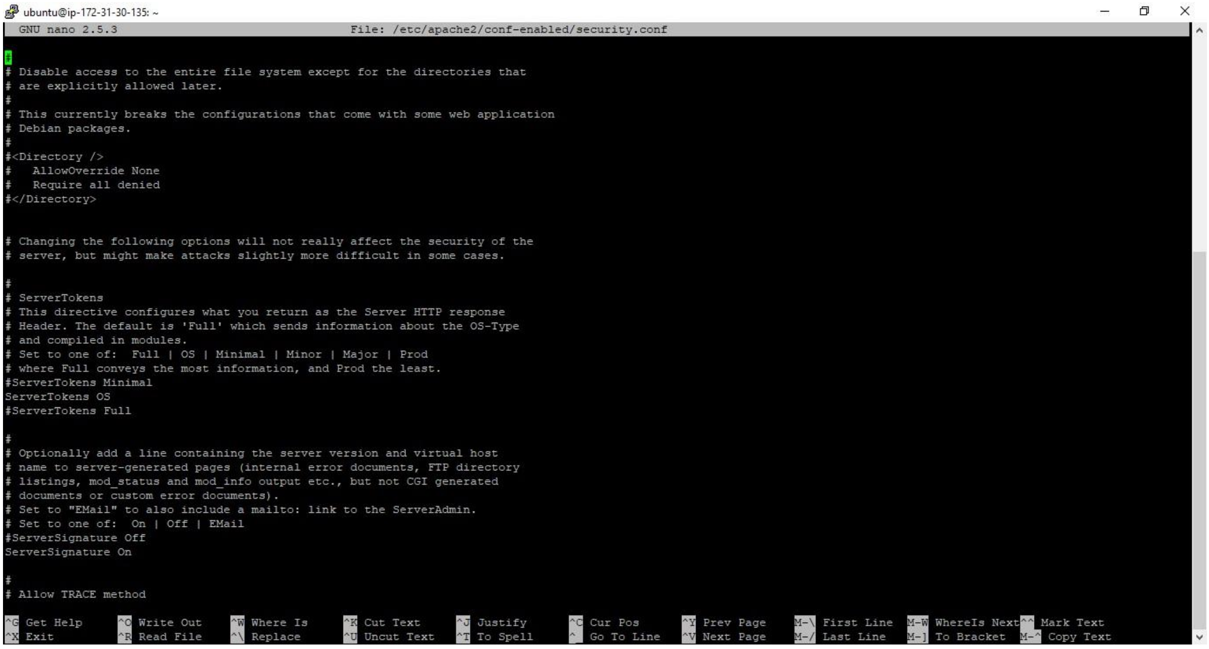
Activity: Securing Apache2 – Ubuntu 18.04

Objectives:

1. Prevent the Apache server signature that is printed as part of a web request - this is not needed and gives would-be hackers info about your server.
2. Prevent directory browsing
3. Install and configure firewall
4. Web server File permissions

Open the Apache config file: sudo nano

/etc/apache2/conf-enabled/security.conf



ubuntu@ip-172-31-30-135: ~

```
  GNU nano 2.5.3                        File: /etc/apache2/conf-enabled/security.conf

#
# Disable access to the entire file system except for the directories that
# are explicitly allowed later.
#
# This currently breaks the configurations that come with some web application
# Debian packages.
#
#<Directory />
#   AllowOverride None
#   Require all denied
#</Directory>


# Changing the following options will not really affect the security of the
# server, but might make attacks slightly more difficult in some cases.

#
# ServerTokens
# This directive configures what you return as the Server HTTP response
# Header. The default is 'Full' which sends information about the OS-Type
# and compiled in modules.
# Set to one of:  Full | OS | Minimal | Minor | Major | Prod
# where Full conveys the most information, and Prod the least.
#ServerTokens Minimal
ServerTokens OS
#ServerTokens Full

#
# Optionally add a line containing the server version and virtual host
# name to server-generated pages (internal error documents, FTP directory
# listings, mod_status and mod_info output etc., but not CGI generated
# documents or custom error documents).
# Set to "EMail" to also include a mailto: link to the ServerAdmin.
# Set to one of:  On | Off | EMail
#ServerSignature Off
ServerSignature On

#
# Allow TRACE method

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     ^Y Prev Page   M-\ First Line  M-W WhereIs Next^^ Mark Text
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  ^V Next Page   M-/ Last Line   M-] To Bracket  M-^ Copy Text
```

Make the following changes:

ServerSignature Off

ServerTokens Prod

```
# Protect a specified range of files from direct access

<FilesMatch "

^(wp-config\.php|php\.ini|php5\.ini|install\.php|php\.info|readme\.md|README\.md|readme\.html|bbconfig\.php|\.htaccess|\.htpasswd|readme\.txt|timthumb\.php|error_log|error\.log|PHP_errors\.log|\.svn)
">

   Require all denied

</FilesMatch>
```

2. Prevent Directory Browsing

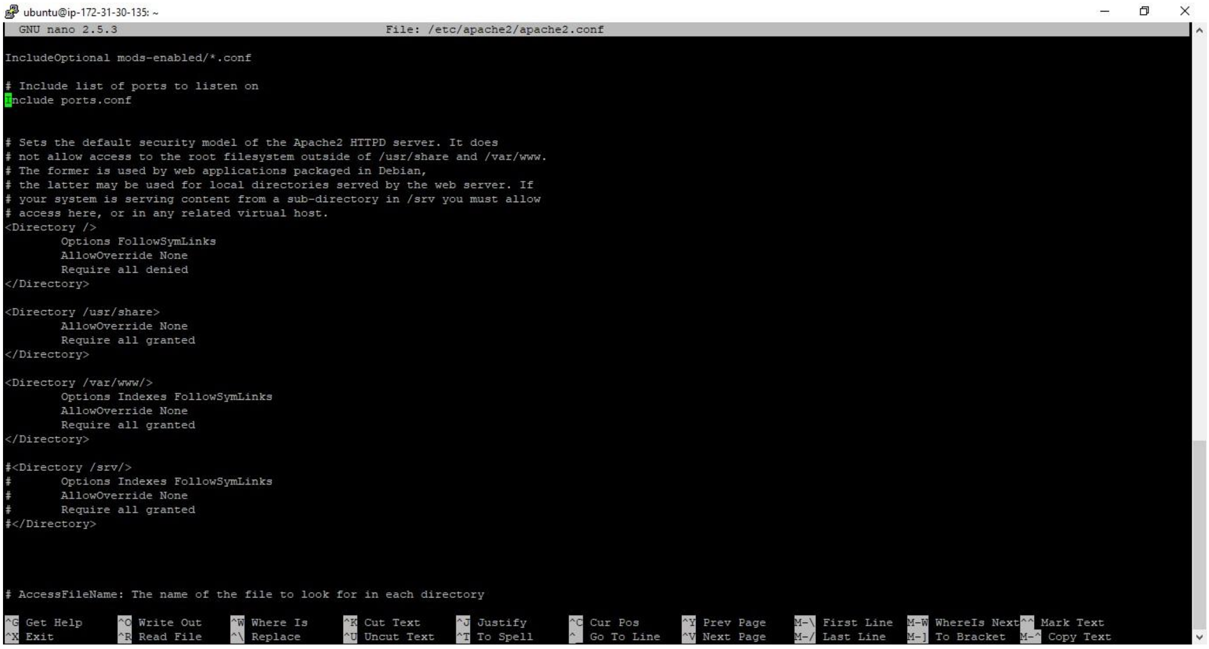
# Consider making a backup of the original first:

```
cp  /etc/apache2/apache2.conf

/etc/apache2/apache2.conf.bak
```

# Open the file for editing:

```
sudo nano /etc/apache2/apache2.conf
```



```
  GNU nano 2.5.3                         File: /etc/apache2/apache2.conf

IncludeOptional mods-enabled/*.conf

# Include list of ports to listen on
Include ports.conf


# Sets the default security model of the Apache2 HTTPD server. It does
# not allow access to the root filesystem outside of /usr/share and /var/www.
# The former is used by web applications packaged in Debian,
# the latter may be used for local directories served by the web server. If
# your system is serving content from a sub-directory in /srv you must allow
# access here, or in any related virtual host.
<Directory />
        Options FollowSymLinks
        AllowOverride None
        Require all denied
</Directory>

<Directory /usr/share>
        AllowOverride None
        Require all granted
</Directory>

<Directory /var/www/>
        Options Indexes FollowSymLinks
        AllowOverride None
        Require all granted
</Directory>

#<Directory /srv/>
#       Options Indexes FollowSymLinks
#       AllowOverride None
#       Require all granted
#</Directory>




# AccessFileName: The name of the file to look for in each directory

^G Get Help    ^O Write Out   ^W Where Is    ^K Cut Text    ^J Justify     ^C Cur Pos     ^Y Prev Page   M-\ First Line M-W WhereIs Next^^ Mark Text
^X Exit        ^R Read File   ^\ Replace     ^U Uncut Text  ^T To Spell    ^_ Go To Line  ^V Next Page   M-/ Last Line  M-] To Bracket  M-^ Copy Text
```

Remove/Comment out:

```
<Directory /var/www/>
```

```
    Options Indexes FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

Add this block:

```
# Disable directory browsing
<Directory /var/www/>
    Options -Indexes
    Options FollowSymLinks
    AllowOverride None
    Require all granted
</Directory>
```

Restart Apache:

```
sudo /etc/init.d/apache2 restart
```

5. Install and configure Firewall

UFW - Uncomplicated Firewall is a basic firewall that works very well and easy to configure with its Firewall configuration tool – gufw

Check if ufw is installed on your system, if not install ufw:

```
sudo apt-get install ufw
```

Check what the firewall is permitting, List all the profiles provided by installed packages :

```
sudo ufw app list
```

Allow access to Apache

```
sudo ufw allow ‘Apache’
```

OR

Allow access to Apache on both port 80 and 443:

```
sudo ufw allow ‘Apache Full’
```

See the full status of UFW:

```
ufw status verbose
```

4. File permissions

Web servers are left open to hackers when using open file permissions (777 or -rwxrwxrwx / drwxrwxrwx). It’s important to make sure that your web server is given proper permissions to access and write directories, without opening them to hackers and visitors. One simple way to do this is to disable write and execution tags where applicable in the permissions for folders and files.

To change all directories within your web folder to 755 (rwxr-xr-x):

```
find /var/www/html -type d -exec chmod 755 {} \;
```

To change all files within your web folder to 644 (rw-r--r--):

```
find /var/ww/html -type f -exec chmod 644 {} \;
```