Challenge #9
Harden a web server

Anchoring and overview

Modul:	681	Angriffe auf ICT-Infrastrukturen detektieren und abwehren
Handlungsziele:	HZ 3	Wählt geeignete Schutzlösungen und Härtungsmassnahmen zur host- und anwendungsbasierten Erkennung und Abwehr von Angriffen aus und nimmt diese in Betrieb.
	HZ 7	Testet die Funktion und Wirksamkeit von Überwachungs- und Schutzlösungen regelmässig und korrigiert bei Bedarf die Konfiguration.
Leistungskriterien PO:	LK-B-4	CSS sind fähig, technische Lösungen zur Erkennung von Angriffen zu erläutern und deren Funktion zu gewährleisten.
	LK-B-3	CSS sind fähig, geeignete Verfahren und Werkzeuge für die Überwachung von Systemen auszuwählen und einzusetzen.

Formulation of task (candidate view)

Harden a web server

Resources

[1] Apache 2.4 HTTP server on Ubuntu Linux and configuration editor as Docker

Introduction

The Docker in the resource section contains a default installation of an Apache 2.4 HTTP server on Ubuntu Linux. No configuration for hardening has been made so far.

You do not have direct access to the Docker's file system. However, calling the URL xxx [URL and Port, depends on integration in HL] in your browser returns a simple graphical interface of an editor, in which the configuration of the web server can be extended. Within this editor you can

- view the enabled and loaded modules,
- edit the configuration file,
- save the configuration, which triggers a syntax check by running `apachectl checkconfig`,
- view the output of the syntax check,
- revert changes you have made,
- download the configuration file for submission.

Goal and tasks

The web server must now be hardened. Expand the configuration in the scope of the preconfigured virtual host to meet the requirements in the following table. Please comment your edits in the configuration file with the respective requirement number.

#	Requirement
R1	For better protection against DoS attacks, the maximum number of header fields in HTTP requests must be limited to 50. In addition, the maximum size for one header field must be limited to 1024 bytes.
R2	The maximum size for the request body must be limited to 2 MB.
R3	The timeout for TCP packets when reading requests from clients must be limited to 20 seconds.
R4	There must be a scope with the URL /admin and access to this URL must be restricted to private IP ranges (A/B/C class) only.
R5	Client-side MIME type sniffing must be avoided by setting a response header indicating that type settings in Content-Type headers should be followed.
R6	Client-side click-jacking attacks must be prevented by setting a response header instructing browsers to restrict content framing to frames from the same origin as the page itself only.
R7	The already enabled module "mod evasive" increases DoS protection. For testing purposes, the localhost should be excluded from the settings of this module. However, this configuration must be conditional on the presence of the module.
R8	Support of HTTP request methods must be limited to GET, POST, HEAD and OPTIONS for directory /var/www/html.
R9	Support of HTTP 1.0 protocol must be disabled to prevent session hijacking.

Submission

Download the configuration with your edits in the integrated editor, check that it is the version with your latest changes and submit the configuration file.

Specifications for correction

Evaluation criteria

C01:	add R1: LimitRequestFields with value 50 (header fields) configured	= 1 pt.
C02:	add R1: LimitRequestFieldsize with value 1024 (bytes) configured	= 1 pt.
C03:	add R2: LimitRequestBody with value 2097152 (bytes) configured	= 1 pt.
C04:	add R3: Timeout with value 20 (seconds) configured	= 1 pt.
C05:	add R4: Directive <Location> for URL /admin configured	= 1 pt.
C06:	add R4: Access restriction to 10.0.0.0/8, 172.16.0.0/12 and 192.168.1.0/24 configured	= 2 pt.
C07:	add R5: Header X-Content-Type-Options with value "nosniff" set	= 1 pt.
C08:	add R6: Header X-Frame-Options with value " SAMEORIGIN" appended and appendage marked as always	= 1 pt.
C09:	add R7: Whitelisting for localhost 127.0.0.1 configured	= 1 pt.
C10:	add R7: Conditional configuration for whitelisting set	= 1 pt.
C11:	add R8: Restriction for request methods configured correctly	= 1 pt.
C12:	add R8: Restriction for request methods configured for correct directory	= 1 pt.
C13:	add R9: Disabling of HTTP 1.0 implemented	= 2 pt.

Correction instructions

- This challenge gives a maximum of **15 points**.
- Given scores on the criteria may not be further subdivided.
- Only solutions given to the tasks within the config file are counting.
- The implementation of the task may vary from the sample solution. As long as the solution works and fulfills the task it is correct.

Sample solutions

```
# ------------------------------------------------------------------------
# Challenge #9:
# ------------------------------------------------------------------------

##############################################################################
# Do not change any existing configuration only add new ones!                #
##############################################################################

<VirtualHost *:80>

    ServerAdmin webmaster@example.com
    DocumentRoot /var/www/html

    ErrorLog ${APACHE_LOG_DIR}/error.log
    CustomLog ${APACHE_LOG_DIR}/access.log combined

    # R1
    LimitRequestFields 50
    LimitRequestFieldsize 1024

    # R2 (2MB = 2097152 Bytes)
    LimitRequestBody 2097152

    # R3
    Timeout 20

    # R4
    <Location /admin>
        Require ip 10.0.0.0/8
        Require ip 172.16.0.0/12
        Require ip 192.168.1.0/24
    </Location>

    # R5
    Header set X-Content-Type-Options: "nosniff"

    # R6
    Header always append X-Frame-Options SAMEORIGIN

    # R7
    <IfModule mod_evasive20.c>
        DOSWhitelist 127.0.0.1
    </IfModule>


    <Directory /var/www/html>
      AllowOverride AuthConfig Limit
      # R8
      <LimitExcept GET HEAD POST OPTIONS>
        Require all denied
      </LimitExcept>
    </Directory>

    # R9
    RewriteEngine On
    RewriteCond %{THE_REQUEST} !HTTP/1.1$
    RewriteRule .* - [F]

</VirtualHost>
```

Config Editor