

UNIVERSIDAD AUTÓNOMA DE CHIAPAS
FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN, CAMPUS I
LICENCIATURA EN INGENIERÍA EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE

CATEDRÁTICO: DR. LUIS GUTIÉRREZ ALFARO
MATERIA: ANÁLISIS DE VULNERABILIDADES

NOMBRE: JOSÉ JULIÁN MOLINA OCAÑA
MATRICULA: A200002
SEMESTRE: 7°
GRUPO: "M"

PROTECCIÓN DE APACHE 2 PARA PÁGINAS EN PHP, COMO DVWA (WAF) INSTALACIÓN DE MOD-EVASIVE

En esta segunda práctica sobre WAF nos ha tocado instalar la característica de seguridad contra ataques DDoS, mod-evasive.

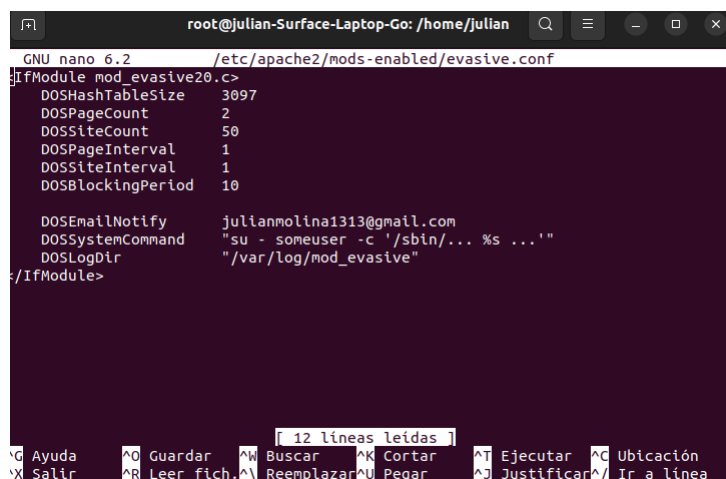
Cómo instalarla:

```
sudo apt-get update  
sudo apt-get install libapache2-mod-evasive
```

Después de eso, hay que habilitar el modulo:
`sudo a2enmod evasive`

Ahora hay que modificar el archivo de configuración de mod-evasive:
`sudo nano /etc/apache2/mods-enabled/evasive.conf`

Debemos de quitar los comentarios y dejar el mod-evasive para que no permita ataques de DDoS, de esta manera:



```
GNU nano 6.2 /etc/apache2/mods-enabled/evasive.conf  
#IfModule mod_evasive20.c>  
#    DOSHashTableSize     3097  
#    DOSPageCount         2  
#    DOSSiteCount         50  
#    DOSPageInterval      1  
#    DOSSiteInterval      1  
#    DOSBlockingPeriod    10  
  
#    DOSEmailNotify       julianmolina1313@gmail.com  
#    DOSSystemCommand     "su - someuser -c '/sbin/... %s ...'"  
#    DOSLogDir             "/var/log/mod_evasive"  
#IfModule>
```

Este código lo he configurado con mi correo, de esta manera cuando algún intruso intente realizar un ataque de denegación de servicios en el puerto de Apache 2, este será detenido y asegurado con un mensaje en mi correo electrónico donde se especifica que alguien intento realizar dicho ataque.

Captura 1. Configuración de mod-evasive

Se tiene que reiniciar apache, de la siguiente manera: `sudo service apache2 restart`, o también a traves de:
`systemctl restart apache2`

EVIDENCIAS DE ATAQUES REALIZADOS A LA PÁGINA DVWA y verificación de defensa de diferentes ataques:

