

Hping3

Hping3 هو تطبيق طرفي لـ **لينكس** سيتيح لنا تحليل حزم TCP / IP وتجميعها بسهولة. بخلاف اختبار ping التقليدي المستخدم لإرسال حزم ICMP ، يسمح هذا التطبيق بإرسال حزم TCP و UDP و RAW-IP. إلى جانب تحليل الحزم ، يمكن أيضًا استخدام هذا التطبيق لأغراض أمنية أخرى ، على سبيل المثال ، لاختبار فعالية **جدار الحماية** من خلال البروتوكولات المختلفة ، واكتشاف الحزم المشبوهة أو المعدلة ، وحتى الحماية من الهجمات DoS. لنظام أو جدار حماية.

أمثلة على استخدام Hping3

اختبار بينج بسيط:

```
(kali@kali)-[~]
$ sudo hping3 192.168.56.102
HPING 192.168.56.102 (eth0 192.168.56.102): NO FLAGS are set, 40 headers + 0 data bytes
len=46 ip=192.168.56.102 ttl=128 DF id=16834 sport=0 flags=RA seq=0 win=0 rtt=3.9 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16835 sport=0 flags=RA seq=1 win=0 rtt=6.9 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16836 sport=0 flags=RA seq=2 win=0 rtt=1.9 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16837 sport=0 flags=RA seq=3 win=0 rtt=9.0 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16838 sport=0 flags=RA seq=4 win=0 rtt=4.9 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16839 sport=0 flags=RA seq=5 win=0 rtt=7.9 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16840 sport=0 flags=RA seq=6 win=0 rtt=2.5 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16841 sport=0 flags=RA seq=7 win=0 rtt=12.7 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16842 sport=0 flags=RA seq=8 win=0 rtt=12.4 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16843 sport=0 flags=RA seq=9 win=0 rtt=6.9 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16844 sport=0 flags=RA seq=10 win=0 rtt=5.9 ms
```

فحص المنفذ باستخدام علامة TCP SYN

تتيح لنا هذه الأداة أيضًا إرسال الحزم بموجب بروتوكول TCP ، في أنقى صورها **نمب** أسلوب. لإجراء مسح باستخدام هذه الطريقة ، سنكتب في المحطة الطرفية "hping3 -S [Destination IP] -p [Port]" ، والنتيجة مماثلة لما يلي:

نتيجة هذا الاختبار سترجع SA العلم ، مما يعني أنه يتوافق مع مزامنة / أك ، وهذا يعني أنه تم قبول الاتصال ، أو ما هو نفسه ، هذا **المنفذ مفتوح** .خلاف ذلك ، إذا كانت القيمة RAعليه يتوافق مع RST / ACKأو ما هو نفسه ، أن الاتصال لم يتم بشكل صحيح بسبب **المنفذ مغلق** أو تصفيتها.

```

(kali@kali)-[~]
$ sudo hping3 -S 192.168.56.102 -p 80
HPING 192.168.56.102 (eth0 192.168.56.102): S set, 40 headers + 0 data bytes
len=46 ip=192.168.56.102 ttl=128 DF id=16908 sport=80 flags=RA seq=0 win=0 rtt=3.6 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16909 sport=80 flags=RA seq=1 win=0 rtt=6.1 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16910 sport=80 flags=RA seq=2 win=0 rtt=6.1 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16911 sport=80 flags=RA seq=3 win=0 rtt=5.2 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16912 sport=80 flags=RA seq=4 win=0 rtt=7.8 ms
len=46 ip=192.168.56.102 ttl=128 DF id=16913 sport=80 flags=RA seq=5 win=0 rtt=1.9 ms
^C
--- 192.168.56.102 hping statistic ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max = 1.9/5.1/7.8 ms
(kali@kali)-[~]

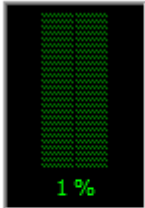

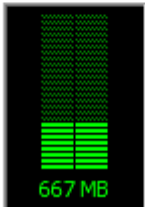
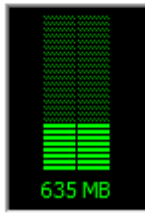
```

إنشاء طلبات متعددة لاختبار حماية DDoS و DoS

```

(kali@kali)-[~]
$ sudo hping3 -S 192.168.56.102 --flood
HPING 192.168.56.102 (eth0 192.168.56.102): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown

```

before		after	
<div>CPU Usage</div>  <div>1 %</div>		<div>CPU Usage</div>  <div>46 %</div>	
<div>Memory</div>  <div>667 MB</div>		<div>Memory</div>  <div>635 MB</div>	

Scan	Commands
ICMP ping	<code>hping3 -1 10.0.0.25</code>
ACK scan on port 80	<code>hping3 -A 10.0.0.25 -p 80</code>
UDP scan on port 80	<code>hping3 -2 10.0.0.25 -p 80</code>
Collecting initial sequence number	<code>hping3 192.168.1.103 -Q -p 139 -s</code>
Firewalls and timestamps	<code>hping3 -S 72.14.207.99 -p 80 --tcp-timestamp</code>
SYN scan on port 50-60	<code>hping3 -8 50-56 -S 10.0.0.25 -v</code>
FIN, PUSH and URG scan on port 80	<code>hping3 -F -P -U 10.0.0.25 -p 80</code>
Scan entire subnet for live host	<code>hping3 -1 10.0.1.x --rand-dest -I eth0</code>
Intercept all traffic containing HTTP signature	<code>hping3 -9 HTTP -I eth0</code>
SYN flooding a victim	<code>hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood</code>