

**Hping3 Nedir?**

Burada hping’den bahsetmeden ping nedir onu tanımlayalım öncelikle.  
*Ping*, en temel anlatımıyla sunucunun veya makinenin yanıt verip vermediğini ölçmek amacıyla kullanılan, bir paketin hedefe doğru bir şekilde ulaşıp ulaşılmadığını kontrol eden bir programdır.  
Kısaca bağlantı sınama işlemi gerçekleştirir. Hping3 ise ping’in gelişmiş versiyonudur. Tıpkı ping’de olduğu gibi hedefe paketler atabiliriz.

**Hping3 Nasıl İndirilir/Yüklenir**

Hping3 programını hem Windows hem de Linux işletim sistemlerinde kullanabilirsiniz. Eğer dosyalarını indirip kullanacaksanız bu dosyaları derlemeden kullanmanız mümkün değildir. Fakat Linux indirme depolarında Hping programı hazır halde olduğu için sadece komut girerek yükleyebilir ve kullanabilirsiniz.  
**Linux’a yüklemek için gerekli komut:** *apt-get install hping3*

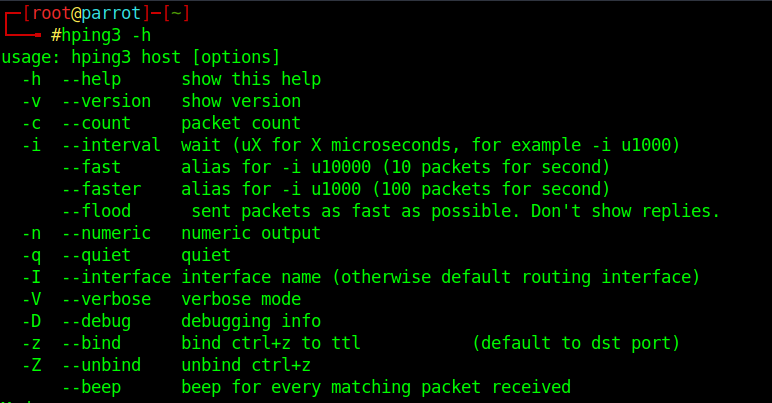
**Hping3 ile Neler Yapılabilir**

Hping3'ün ne olduğunun temelini artık biliyoruz. Fakat bu programla neler yapabiliriz detaylı olarak açıklayalım.  
Şimdi yazacağım bu kavramları bilmiyorsanız kısa bir araştırma ile tanımlarına bakarsanız bilmeyenler için daha açıklayıcı olacaktır.  
***Hping3 ile;***  
• TCP, UDP, ICMP, Raw-IP paketleri üretebiliriz.  
• Güvenlik duvarları oluşturabilir ve DOS saldırılarına karşı önlemler alabiliriz.  
• Herhangi bir saldırıya maruz kalınması durumunda tespit etme işlemi yapılabilir ve kısa sürede müdahale edebiliriz.  
• Gelişmiş bir port tarayıcısıdır ve dosya transferi yapabilir.  
• TCP/IP paketleri toplaması yapabiliriz ve bunların testlerini ***gerçekleştirebiliriz.***

**Hping3 Kullanımı ve Tüm Parametreleri**

Bu başlık altında biraz zor olan bir iş yapacağız. Hping3'ün tüm parametrelerini anlatmayı hedefledim. Umarım düzgün bir şekilde anlatabilmişimdir. Hemen ilk parametre ile başlayalım.  
Ben Linux dağıtımlarından olan Parrot OS’u kullanacağım sizlerede bir Linux dağıtımını kullanmanızı öneririm.

***hping3 -h:*** terminalde bu komutu çalıştırdığımızda hping3'e ait tüm parametreleri bize açıklamalarıyla birlikte gösterir.  
Şimdi bu komutu çalıştırdıktan sonra görselde görüldüğü gibi tüm parametreler ve parametrenin ne iş yaptığı yazıyor.  
Elbette bu parametrelerin tümünü denemek veya bilmek biraz zor olabilir ama ben bütün parametrelerin yanına Türkçesini yazacağım.  
Okuyucular denemek isterse dikkatli bir şekilde denemelerini gerçekleştirebilirler. Şimdi sözü fazla uzatmadan parametreleri Türkçeleştirelim.



**Kullanım Kalıbı:** hping3 host\_adı(veya IP adresi) [Parametre]  
**Kullanım Kalıbı:** hping3 [Parametre] host\_adı(veya IP adresi)

**-h — help**Yardım alma listesini gösterir.  
**-v — version** Hping3 sürümünü gösterir  
**-c — count**Paket sayısını belirtir  
**-i — interval**bekleme süresi veya paket gönderme sıklığı (X mikrosaniye için uX, örneğin -i u1000)  
**— fast**-i u10000 için saniyede 10 paket  
**— faster** -i u1000 için saniyede 100 paket  
**— flood** Paketlerin en hızlı bir şekilde gönderir ve yanıt göstermez.  
**-n — numeric** Sayısal çıktılar  
**-q — quiet**Sessiz(Gizli bir şekilde işlem yapar, sanırım log tutturmaz.)  
**-I — interface** Arayüz/arabirim adı (belirtmezseniz avrsayılan arayüz/arabirim kullanılır)  
**-V — verbose** Ayrıntılı mod  
**-D — debug** Debug(Hata ayıklama) bilgilerini ifade eder.  
**-z — bind** ctrl+z ile ttl’ye bağlanır(varsayılan olarak dst portuna bağlanır)  
**-Z — unbind** ctrl+z ile bağlanmayı çözer  
**— beep** Her paket için bip sesi üretir.

**Modlar**  
Varsayılan mod TCP  
**-0 — rawip** RAW IP paketleri  
**-1 — icmp**ICMP paketleri  
**-2 — udp** UDP paketleri  
**-8 — scan** Normal tarama  
**Örneğin:** hping3 — scan 1–30,70–90 -S [www.hedef.host](http://www.hedef.host/)  
**-9 — listen** Dinleme modu

**IP**  
**-a — spoof** IP Spoofing(IP Sahtekarlığı)  
**— rand-dest** Rastgele hedef adres modu  
**— rand-source** Rastgele kaynak adres modu(ip gizleme gibi)  
**-t — ttl**ttl (varsayılan 64)  
**-N — id** id (varsayılan rastgele)  
**-W — winid** win\* id bayt sıralaması  
**-r — rel** Ana bilgisayar trafiğini göreceli hale getirme  
**-f — frag** Frag paketlerini daha fazla parçaya bölmek için  
**-x — morefrag** daha fazla parça bayrağı ayarlar  
**-y — dontfrag** parçalama bayrağını göstermez  
**-g — fragoff**parça ofsetini ayarlar  
**-m — mtu** sanal mtu ayarlar, implies — frag if packet size > mtu  
**-o — tos** hizmet türü (varsayılan 0x00)  
**-G — rroute** RECORD\_ROUTE seçeneğini içerir ve yol arabelleğini görüntüler  
**— lsrr**gevşek kaynak yönlendirme ve kayıt yolu  
**— ssrr**katı kaynak yönlendirme ve kayıt yolu  
**-H — ipproto**P protokol alanını yalnızca RAW IP modunda ayarlar

**ICMP**  
**-C — icmptype** icmp türü  
**-K — icmpcode** icmp kodu (varsayılan 0)  
**— force-icmp** tüm icmp türlerini gönder (varsayılan yalnızca desteklenen türleri gönder)  
**— icmp-gw** ICMP yönlendirmesi için ağ geçidi adresini ayarla (varsayılan 0.0.0.0)  
**— icmp-ts — icmp** — icmptype 13 takma eki için (ICMP zaman damgası)  
**— icmp-addr — icmp** — icmptype 17 takma eki için (ICMP adresi alt ağ maskesi)  
**— icmp-help** Diğer icmp seçenekleri için yardımı görüntüleme

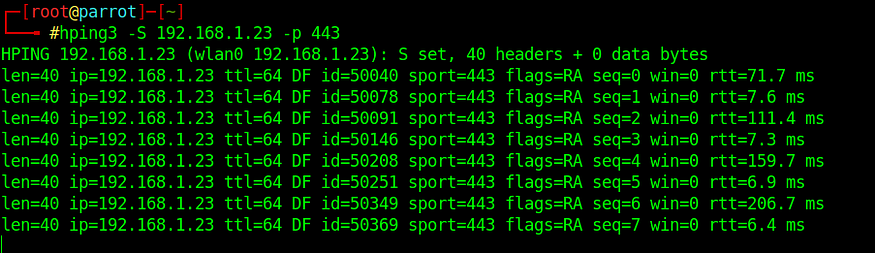
**UDP/TCP**  
**-s — baseport** temel kaynak bağlantı noktası (Varsayılan rastgele)  
**-p — destport** [+][+]<port> hedef port(varsayılan 0) ctrl+z arttır/azalt  
**-k — keep** kaynak bağlantı noktasını koru  
**-w — win** winsize (varsayılan 64)  
**-O — tcpoff** sahte tcp veri ofsetini ayarla  
**-Q — seqnum** yalnızca tcp sıra numarasını gösterir  
**-b — badcksum** kötü bir IP sağlama toplamına sahip paketler gönderir  
birçok sistem paketi gönderen IP sağlama toplamını düzeltir  
böylece bunun yerine hatalı UDP / TCP sağlama toplamı alırsınız.  
**-M — setseq**TCP sıra numarası ayarlama  
**-L — setack** TCP ack ayarlama  
**-F — fin**FIN bayrağı ayarlama  
**-S — syn** SYN bayrağı ayarlama  
**-R — rst** RST bayrağı ayarlama  
**-P — push** PUSH bayrağı ayarlama  
**-A — ack** ACK bayrağı ayarlama  
**-U — urg** URG bayrağı ayarlama  
**-X — xmas** Kullanılmayan X bayrağı ayarlama (0x40)  
**-Y — ymas** Kullanılmayan Y bayrağı ayarlama (0x80)  
**— tcpexitcode** tcp->th\_flags’ı çıkış kodu olarak kullanır  
**— tcp-mss** verilen değerle TCP MSS seçeneğini etkinleştirir  
**— tcp-timestamp** HZ(çalışma süresini) tahmin etmek için TCP zaman damgası seçeneğini etkinleştirir

**Yaygın Kullanılan Parametreler**  
**-d — data** Veri boyutu(varsayılan 0)  
**-E — file** dosyadan veri dosyası  
**-e — sign**imza ekleme  
**-j — dump**hex paketlerini boşaltma  
**-J — print** yazdırılabilir karakterleri dökümü yazdır  
**-B — safe** güvenli protokolü etkinleştirir  
**-u — end** Sonlanrımak için  
**-T — traceroute** traceroute(izleme yolu) modu ( — bind ve — ttl 1 anlamına gelir)  
**— tr-stop** Traceroute modunda birden fazla ICMP’yi aldığınızda çıkış yapar  
**— tr-keep-ttl** Kaynak TTL’yi sabit tutun, yalnızca bir sekmeyi izlemek için kullanışlıdır  
**— tr-no-rtt** Traceroute modunda RTT bilgilerini hesaplama/gösterme

**ARS paket açıklaması (yeni, kararsız)**  
**— apd-send**APD ile açıklanan paketi gönderin (bkz.docs/APD.txt)

**Hping3 ile örnek taramalar**

Şimdi burada ilk olarak basit bir tarama gerçekleştirelim ve tarama sonuçlarını yorumlayalım. Tarama sonuçlarını yorumlamayı bilmemek tarama yapmanın bir anlamı olmadığını ifade eder.  
Basit bir tarama gerçekleştirelim. Bunun için kullanacağımız komut kalıbı şöyledir.  
  
*hping3 -S Hedef\_IP\_Adresi -p <port\_numarası>*



Burada “-S” parametresi ile SYN paketlerini ve “-p” parametresi ile port numarasını belirtiyoruz. Ben ağa bağlı olan bir cihaz  
üzerinden denedim ve hedefin 443 nolu portuna işlem yaptım. Aşağıdaki resimde bazı ifadeler görüyoruz. Bunları açıklayalım.

**len:** *Dönen paketlerin boyutu*  
**ip:** *Paketin gönderildiği hedef makinenin ip adresi*  
**ttl:** *paketin süresi*  
**DF:** *Parçalama baytının aktifliği*  
**id:** *Uniq bilgisi*  
**sport:** *paketlerin göderilgiği port*  
**flags:** *TCP bayrağı*  
**seq:** *paketlerin sıra numarası*  
**win:***Win(pencere) paket boyutu*  
**rtt:***Milisaniye cinsinden süre*

Burada paketleri yorumladık fakat bilmeyenler için araştırma tavsiye ederim Bunun için genel TCP/IP bilgisi yeterlidir.

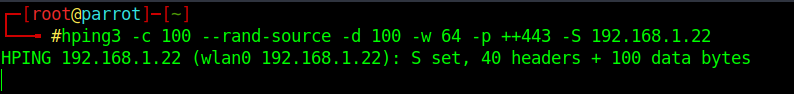
İstersek birden fazla taramayı aynı anda gerçekleştirebiliriz. Bunun için sadece gireceğimiz komuta parametre eklememiz yeterli  
olacaktır.

*hping3 -S -F <IP\_Adresi>*

Modlar kısmında açıklamasını yaptığımız parametreleri de sadece komuta numara olarak eklersek o taramayı da gerçekleştirebiliriz.

Şimdi basit bir DDOS atağı gerçekleştirelim. **Bunun için kullanacağımız komut:**  
*hping3 -c <paket\_sayısı> — rand-source -d <data\_boyutu> -w <pencere\_boyutu> -p <port\_numarası> -S <IP\_Adresi>*

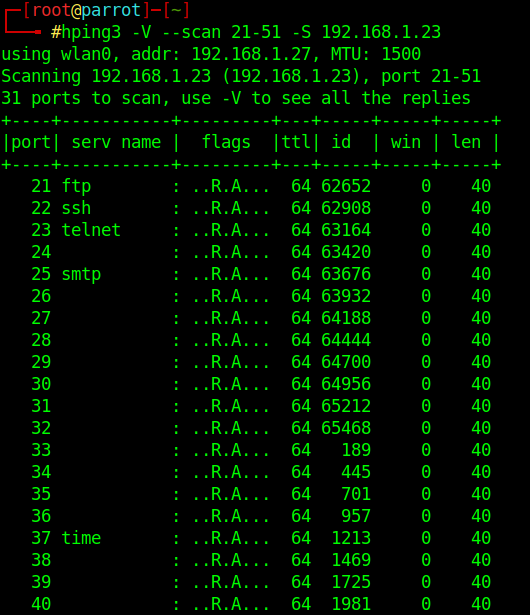
Normalde bu tarama sonsuz döngüdedir ve siz durdurmayana kadar durmadan devam edecektir. Burada “-c” parametresi ile istediğimiz  
kadar paket gönderebiliriz ve sayısını belirleyebiliriz. “-w” parametresi ile pencere boyutunu ayarlayabiliyoruz. “-p” ile kaynak portu berlirledik. Normal taramada “-d” yani datanın boyutu 0(sıfır)’dır bunu sayısal oalrak belirleyebiliriz. “ — rand-source” parametresi ile farklı ip adresinden paket gönderiyormuş gibi göründük. İstersek belirli bir ip adreside belirtebiliriz. Komutumuzun açıklaması bu kadar. İStersek Firewall performans testi de gerçekleştirebiliriz.  
Aşağıdaki resimde saldırının başladığını görebilisiniz, sonlanmadığı için bir görsel oluşturamadık ama sanırım anlaşılmıştır.



Şimdi bir sistemde Firewall olup olmadığına bakalım.  
**Bunun için kullanacağımız komut:**

*hping3 -V — scan <port\_numarası/aralığı> -S <IP\_Adresi>*

***Şimdi bu komutu açıklayalım.***  
“-V” parametresi ile verbose modunu açtık. Yani daha detaylı bir gösterim olacktır. “ — scan” parametresi ile normal bir tarama yapmak istediğimizi belirttik ve port numarasını belirttik. Burada 21 ile 51 arasındaki portları denemesini istedik. “-S” parametresi ile SYN paketleri gönderiyoruz ve aşağıdaki gösrselde sonucu görebiliyoruz. Görseli inceleyin ve devam edelim.



Görselde anlaşılan ifadeler gördüğünüzü varsayarak devam ediyoruz. Şimdi burda Firewall olup olmadığını nasıl anlayacağız?  
Çok basit bir şekilde çıktıyı(görseli) kontrol etmeniz gerekli. Eğer belirlediğiniz port aralığında herhangi bir portu göremiyorsanız yani 21–51 arasında hepsi var ama 45 nolu portu çıktıda göremiyorsanız o port bir Firewall tarafından korunuyor demektir.

**Sonuç**

Hping3 ile bu anlattıklarımdan daha fazlasını da yapabiliriz. Fakat yanında yardımcı bir program kullanarak hping3'ü daha işlevli hale getiriyoruz. Zaten genelde hping’den sonra yardımcı bir program kullanılarak işlemlere devam edilir.