## Hping 3 Nedir?

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.

## Hping 3 Nasıl İndirilir?

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?

- 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 gerçekleştirebiliriz.

hping3 -h: tüm parametreleri açıklamalarıyla birlikte gösterir.

```
root@kali:~# hping3 -h
usage: hping3 host [options]
  -h  --help      show this help
  -v  --version   show version
  -c  --count     packet count
  -i  --interval  wait (uX for X microseconds, for example -i u1000)
      --fast      alias for -i u10000 (10 packets for second)
      --faster    alias for -i u1000 (100 packets for second)
      --flood      sent packets as fast as possible. Don't show replies.
  -n  --numeric   numeric output
  -q  --quiet     quiet
  -I  --interface interface name (otherwise default routing interface)
  -V  --verbose   verbose mode
  -D  --debug     debugging info
  -z  --bind      bind ctrl+z to ttl           (default to dst port)
  -Z  --unbind    unbind ctrl+z
      --beep      beep for every matching packet received
Mode
  default mode     TCP
  -0  --rawip      RAW IP mode
  -1  --icmp       ICMP mode
  -2  --udp        UDP mode
  -8  --scan       SCAN mode.
                   Example: hping --scan 1-30,70-90 -S www.target.host
  -9  --listen     listen mode
IP
  -a  --spoof      spoof source address
  --rand-dest      random destionation address mode. see the man.
  --rand-source    random source address mode. see the man.
  -t  --ttl        ttl (default 64)
  -N  --id         id (default random)
  -W  --winid      use win* id byte ordering
  -r  --rel        relativize id field          (to estimate host traffic)
  -f  --frag       split packets in more frag.  (may pass weak acl)
```

```
-x  --morefrag   set more fragments flag
-y  --dontfrag   set don't fragment flag
-g  --fragoff    set the fragment offset
-m  --mtu        set virtual mtu, implies --frag if packet size > mtu
-o  --tos        type of service (default 0x00), try --tos help
-G  --rroute     includes RECORD_ROUTE option and display the route buffer
--lsrr           loose source routing and record route
--ssrr           strict source routing and record route
-H  --ipproto    set the IP protocol field, only in RAW IP mode
CMP
-C  --icmptype   icmp type (default echo request)
-K  --icmpcode   icmp code (default 0)
    --force-icmp send all icmp types (default send only supported types)
    --icmp-gw    set gateway address for ICMP redirect (default 0.0.0.0)
    --icmp-ts    Alias for --icmp --icmptype 13 (ICMP timestamp)
    --icmp-addr  Alias for --icmp --icmptype 17 (ICMP address subnet mask)
    --icmp-help  display help for others icmp options
DP/TCP
-s  --baseport   base source port             (default random)
-p  --destport   [+][+]<port> destination port(default 0) ctrl+z inc/dec
-k  --keep       keep still source port
-w  --win        winsize (default 64)
-O  --tcpoff     set fake tcp data offset     (instead of tcphdrlen / 4)
-Q  --seqnum     shows only tcp sequence number
-b  --badcksum   (try to) send packets with a bad IP checksum
                 many systems will fix the IP checksum sending the packet
                 so you'll get bad UDP/TCP checksum instead.
-M  --setseq     set TCP sequence number
-L  --setack     set TCP ack
-F  --fin        set FIN flag
-S  --syn        set SYN flag
-R  --rst        set RST flag
-P  --push       set PUSH flag
-A  --ack        set ACK flag
-U  --urg        set URG flag
-X  --xmas       set X unused flag (0x40)
-Y  --ymas       set Y unused flag (0x80)
```

```
  --tcpexitcode    use last tcp->th_flags as exit code
  --tcp-mss        enable the TCP MSS option with the given value
  --tcp-timestamp  enable the TCP timestamp option to guess the HZ/uptime
Common
  -d  --data       data size                     (default is 0)
  -E  --file       data from file
  -e  --sign       add 'signature'
  -j  --dump       dump packets in hex
  -J  --print      dump printable characters
  -B  --safe       enable 'safe' protocol
  -u  --end        tell you when --file reached EOF and prevent rewind
  -T  --traceroute traceroute mode               (implies --bind and --ttl 1)
  --tr-stop        Exit when receive the first not ICMP in traceroute mode
  --tr-keep-ttl    Keep the source TTL fixed, useful to monitor just one hop
  --tr-no-rtt       Don't calculate/show RTT information in traceroute mode
ARS packet description (new, unstable)
  --apd-send       Send the packet described with APD (see docs/APD.txt)
```

## Temel Komutlar

v –version, hping3'ün güncel sürümünü gösterir

-c –count paket sayacı

-i – aralık zaman aşımı (X mikrosaniye için uX, örneğin -i u1000)

–İ u10000 için hızlı takma adlar (saniyede 10 paket)

–İ u1000 için daha hızlı takma ad (saniyede 100 paket)

–Flood, paketleri olabildiğince hızlı gönderir, yanıtları göstermez.

-n - sayılarla sayısal çıktı

-q - ekranda göstermeden sessiz sessiz komut

-I – arayüz adı, eğer hiçbir şey ayarlanmadıysa, varsayılan olarak yukarıdaki öntanımlı geçidin arayüzüdür.

-V - hata ayıklama için ayrıntılı mod

-D –debug hata ayıklama bilgileri

-z –bind bind ctrl + za ttl (varsayılan olarak hedef bağlantı noktasıdır)

-Z –bağlamayı kaldırır ctrl + z

Eşleşen her alınan paket için bip sesi

## Modlar:

Varsayılan mod TCP'dir

-0 –rawip RAW IP modu

-1 –icmp ICMP modu

-2 –udp UDP modu

-8 - tarama modu TARAMA modu.

-9 - hazır dinleme modu

Örnek: hping –scan 1-30,70-90 -S www.target.com

## IP:

-a –spoof kaynak IP adresi sahteciliği

–Rand-hedef rastgele hedef IP adresi.

–Rand-kaynaklı rastgele kaynak IP adresi.

-t –ttl ttl (varsayılan 64)

-N –id id (rastgele varsayılan)

-W - win * id bayt sırasını kullanır

-r –rel kimlik alanını göreli hale getirir (ana bilgisayar trafiğini tahmin etmek için)

-f - paketleri birden fazla parçaya böler, zayıf ACL'leri geçebilir

-x –morefrag parçaları daha fazla

-y –dontfrag paketleri parçalamaz.

-g –fragoff parça ofsetini ayarlar

-m –mtu sanal bir MTU ayarlar, paketin parçasının MTU'dan daha büyük olduğu anlamına gelir.

-o –tos hizmet türü (varsayılan 0x00), –tos yardım yapmayı deneyin

-G –route, RECORD_ROUTE seçeneğini içerir ve yol arabelleğini gösterir

–Lsrr gevşek kaynak yönlendirme ve rota günlüğü

–Ssrr katı kaynak yönlendirme ve rota günlüğü

-H –ipproto, IP protokolünü yalnızca RAW IP modu için ayarlar.

## ICMP:

-C –icmptype ICMP türü (varsayılan olarak ICMP Yankı isteğidir)

-K –icmpcode ICMP kodu (varsayılan 0'dır)

–Force-icmp tüm ICMP türlerini gönderir (varsayılan olarak yalnızca desteklenen türleri gönderir)

–Icmp-gw, ICMP yönlendirmesi için varsayılan ağ geçidi adresini ayarlar (varsayılan 0.0.0.0)

–İcmp –icmptype 13 için –Icmp-ts takma adları (ICMP zaman damgası)

–İcmp –icmptype 17 için –Icmp-addr takma adı (ICMP alt ağ maskesi adresi)

–Icmp-help, diğer icmp seçenekleri için yardım görüntüler.

## ICMP kodları

Hping3'ün bize gösterebileceği bazı ICMP kodlarını bilmek çok yararlıdır, aşağıda en çok kullanılan kodlara sahipsiniz:

| Código | Descripción |
|---|---|
| 0 | Network unreachable |
| 1 | Host unreachable |
| 2 | Protocol unreachable |
| 3 | Port unreachable |
| 4 | Fragmentation needed, but do not fragment bit set |
| 5 | Source route failed |
| 6 | Destination network unknown |
| 7 | Destination host unknown |
| 8 | Source host isolated error (military use only) |
| 9 | The destination network is administratively prohibited |
| 10 | The destination host is administratively prohibited |
| 11 | The network is unreachable for Type Of Service |
| 12 | The host is unreachable for Type Of Service |
| 13 | Communication administratively prohibited (administrative filtering prevents packet from being forwarded) |
| 14 | Host precedence violation (indicates the requested precedence is not permitted for the combination of host or network and port) |
| 15 | Precedence cutoff in effect (precedence of datagram is below the level set by the network administrators) |

## TCP / UDP

-s –baseport temel kaynak bağlantı noktası, varsayılan rastgele

-p –destport [+] [+] hedef konum (varsayılan 0) ctrl + z inc / dec

-k - kaynak bağlantı noktasını koru

-w –win pencere boyutu, varsayılan 64

-O –tcpoff, tcp veri ofsetini yanlış ayarlıyor (tcphdrlen / 4 yerine)

-Q –seqnum yalnızca sıra numarasını gösterir

-b –badcksum (deneyin) sahte IP sağlama toplamı ile paket gönderirken, birçok sistem paketi gönderirken bu sağlama toplamını düzeltir, böylece UDP / TCP düzeyinde yanlış bir sağlama toplamına sahip olursunuz.

-M –setseq, TCP sıra numarasını ayarlar

-L –setack, TCP ack'i ayarlar

-F –fin FIN işaretini ayarlar

-S –syn, SYN bayrağını ayarlar

-R –rst, RST bayrağını ayarlar

-P –push, PUSH işaretini ayarlar

-A –ack ACK işaretini ayarlar

-U –urg, URG işaretini ayarlar

-X –xmas kullanılmayan X bayrağını ayarlar (0x40)

-Y –ymas, Y bayrağını kullanılmayan ayarlar (0x80)

–Tcpexitcode, çıkış kodu olarak son tcp-> th_flags'ı kullanır

–Tcp-mss, verilen değerle TCP MSS seçeneğini etkinleştirir

–Tcp-timestamp, TCP zaman damgası seçeneğinin çalışma süresini tahmin etmesini sağlar.

## Herkes için ortak seçenekler

d –veri veri boyutu, varsayılan 0'dır.

-E –bir dosyadan dosya verileri.

-e –sign bir imza ekler

-j –dump paketleri onaltılık olarak döker

-J - yazdırılabilir karakterleri dökümler

-B –safe, "güvenli" protokolü etkinleştirir

-u –end bir dosyanın sonuna ulaştığında size söyler

-T –traceroute traceroute modu (–bind ve –ttl 1 anlamına gelir)

–Tr-stop Traceroute modunda ICMP olmayan ilk paket alındığında çıkın

–Tr-keep-ttl Kaynak TTL'yi sabit tutun, yalnızca bir sekmeyi izlemek için kullanışlıdır

–Tr-no-rtt Traceroute modunda RTT bilgilerini hesaplamaz ve görüntülemez

ARS paketi açıklaması (yeni ve kararsız)

–Apd-send APD ile açıklanan paketleri gönder

## Örnekler

### Basit ping testi

# hping3 www.google.es

Bu aracı geleneksel ping komutu gibi kullanabiliriz ve pratik olarak aynı sonuçları elde edebiliriz.

### Bağlantı yolunu çiz

"Tracert" seçeneğine benzer şekilde Windows veya Linux'ta “traceroute”, bu araçla, bir paketin bilgisayarımızdan ayrıldığı andan hedefine ulaştığı ana kadar ağlar arasındaki tüm sıçramaları da takip edebiliriz, herhangi bir zamanda içinde bir tür sorun olup olmadığını anlayabiliriz. bağ.

# hping3 redeszone.net -t 1 --traceroute

## TCP SYN bayrağını kullanarak bağlantı noktası taraması

Bu araç aynı zamanda en saf haliyle, TCP protokolü altında paketler göndermemizi sağlar. Nmap tarzı. Bu yöntemi kullanarak bir tarama gerçekleştirmek için, "hping3 –S [Hedef IP] –p [Port]" terminalini yazacağız.

#  hping3 -S www.google.es –p 80

Bu testin sonucu bir SA bayrak, yani karşılık geldiği anlamına gelir SYN / ACK yani iletişim kabul edildi veya aynısı, liman açık. Aksi takdirde, değer ise RA onu tekabül RST / ACK veya aynı şey, iletişimin doğru şekilde gerçekleştirilmediğini, çünkü liman kapalı veya filtrelenmiş.

Bu şekilde, örneğin belirli bir bağlantı noktasına iletişime izin verilip verilmediğini veya aksi takdirde Güvenlik Duvarının onu filtrelediğini öğrenebiliriz.

### Paketleri özel bir metin dosyasıyla imzalayın

Bu aracı, gönderdiğimiz paketleri değiştirmek ve bunlara imzaya benzer kişiselleştirilmiş bir mesaj eklemek için kullanmak mümkündür. Bunu yapmak için şunu yazmamız yeterlidir:

# hping3 redeszone.net -d 50 -E firmaredeszone.txt

Bu komut, belirtilen txt dosyasının içeriğini Ping paketlerine tanıtacaktır. Bu paketleri WireShark gibi uygun bir yazılımla analiz edersek, içlerinde söz konusu dosyanın içeriğinin olduğunu görürüz.

Girilen parametrelerin anlamı:

-d: Gireceğimiz mesajın uzunluğu, bu durumda 50.

-E: Paketlere tanıtmak istediğimiz mesaj imzasını alacağımız dosya.

Bu paketleri göndermek istediğimiz portu belirtmek için -p veya paketleri UDP protokolü üzerinden göndermek için -2 gibi diğer parametreleri de kullanabiliriz.

## Örnekler

ICMP ping'i

# hping3 -1 10.0.0.25

Hping, komut satırında -1 bağımsız değişkenini belirterek bir ICMP ping taraması gerçekleştirir. Komut satırında –ICMP of -1 argümanını kullanabilirsiniz. Yukarıdaki komutu vererek, hping, 10.0.0.25'e ICMP-echo isteği gönderir ve bir ping yardımcı programında olduğu gibi ICMP-yanıtını alır.

80 numaralı bağlantı noktasında ACK taraması

# hping3 –A 10.0.0.25 –p 80

Hping, komut satırında -A bağımsız değişkeni belirtilerek bir ACK taraması gerçekleştirecek şekilde yapılandırılabilir. Burada, prob paketlerinde ACK bayrağını ayarlıyorsunuz ve taramayı gerçekleştiriyorsunuz. Bu taramayı, bir ana bilgisayar bir ping isteğine yanıt vermediğinde gerçekleştirirsiniz. Bu komutu vererek, Hping bir ana bilgisayarın ağda canlı olup olmadığını kontrol eder. Canlı bir ana bilgisayar ve açık bir bağlantı noktası bulursa, bir RST yanıtı döndürür.

80 numaralı bağlantı noktasında UDP taraması

# hping3 -2 10.0.0.25 –p 80

Hping, varsayılan protokolü olarak TCP'yi kullanır. Komut satırında -2 bağımsız değişkeninin kullanılması, Hping'in UDP modunda çalıştığını belirtir. Komut satırındaki bağımsız değişkenlerden herhangi --udpbirini kullanabilirsiniz. -2Hping, yukarıdaki komutu vererek UDP paketlerini ana bilgisayardaki 80 numaralı bağlantı noktasına gönderir (10.0.0.25). Bağlantı noktasının kapalı olduğunu tespit ederse ICMP bağlantı noktasına ulaşılamaz mesajı verir ve bağlantı noktası açıksa bir mesajla yanıt vermez.

İlk Sıra Numarasını Toplama

# hping3 192.168.1.103 -Q -p 139 –s

Hping, komut satırında -Q bağımsız değişkenini kullanarak, hedef ana bilgisayar (192.168.1.103) tarafından oluşturulan tüm TCP sıra numaralarını toplar.

Güvenlik Duvarları ve Zaman Damgaları

# hping3 -S 72.14.207.99 -p 80 --tcp-timestamp

Birçok güvenlik duvarı, TCP Zaman Damgası seçeneği ayarlanmamış olan TCP paketlerini düşürür. Komut satırına –tcp-timestamp argümanını ekleyerek, Hping'de TCP zaman damgası seçeneğini etkinleştirebilir ve hedef ana bilgisayarın (72.14.207.99) zaman damgası güncelleme sıklığını ve çalışma süresini tahmin etmeye çalışabilirsiniz.

50-60 numaralı bağlantı noktasında SYN taraması

# hping3 -8 50-60 –S 10.0.0.25 –V

Komuttaki argümanı -8(veya) kullanarak --scan, hedef ana bilgisayardaki bir dizi bağlantı noktasını taramak için Hping'i tarama modunda çalıştırıyorsunuz. -S bağımsız değişkeninin eklenmesi, bir SYN taraması gerçekleştirmenize olanak tanır. Bu nedenle, yukarıdaki komut, hedef ana bilgisayardaki 50-60 bağlantı noktalarında bir SYN taraması gerçekleştirir.

80 numaralı bağlantı noktasında FIN, PUSH ve URG taraması

# hping3 –F –P –U 10.0.0.25 –p 80

Komuta –F, -P ve –U argümanlarını ekleyerek, araştırma paketlerinde FIN, PUSH ve URG paketlerini ayarlarsınız. Bu komutu vererek, hedef ana bilgisayardaki 80 numaralı bağlantı noktasında (10.0.0.25) FIN, PUSH ve URG taramaları gerçekleştiriyorsunuz. Hedefte 80 numaralı bağlantı noktası açıksa, yanıt almazsınız. Bağlantı noktası kapatılırsa, Hping bir RST yanıtı döndürür.

Canlı ana bilgisayar için tüm alt ağı tarayın

# hping3 -1 10.0.1.x --rand-dest –I eth0

Bu komutu vererek Hping, 10.0.1.x alt ağının tamamında bir ICMP ping taraması gerçekleştirir; --rand-destyani 10.0.1.0 – 10.0.1.255 arası eth0 arayüzüne bağlı tüm hostlara rastgele ( ) ICMP-echo isteği gönderir. Bağlantı noktaları açık olan ana bilgisayarlar, bir ICMP yanıtıyla yanıt verecektir. Bu durumda, bir bağlantı noktası ayarlamadınız, bu nedenle Hping, paketleri varsayılan olarak tüm IP adreslerinde bağlantı noktası 0'a gönderir.

HTTP imzası içeren tüm trafiği durdur

# hping3 -9 HTTP –I eth0

-9 argümanı, Hping'i dinleme moduna ayarlayacaktır. Böylece, -9 HTTP komutunu vererek, Hping bağlantı noktası 0'ı (ağda eth0 arabirimine bağlı tüm aygıtların) dinlemeye başlar, HTTP imzası içeren tüm paketleri yakalar ve imza ucundan paketin sonuna boşaltır. Örneğin, hping2 -9 HTTP komutu verildiğinde, Hping 234-09sdflkjs45-HTTPhello_world verilerini içeren bir paketi okursa sonucu merhaba_world olarak görüntüler.

SYN bir kurbanı sular altında bırakıyor

# hping3 -S 192.168.1.1 -a 192.168.1.254 -p 22 --flood

Saldırgan, DoS saldırısı gerçekleştirmek için sahte IP adreslerini kullanarak TCP SYN taşma tekniklerini kullanır.

Ping sayısını belirleyin

# hping3 -c 3 10.10.10.10

Burada -c 3, hedef makineye yalnızca üç paket göndermek istediğimiz anlamına gelir.

Rastgele kaynak adresi kullan

--rand-source

Veri boyutunu ayarla

Veri paketi boyutunu bayt olarak ayarla--data <size>

Sahte kaynak adresi

# hping3 -S <IP address attacked> -a <spoofed IP address>

# hping3 -S <IP address attacked> --spoof <spoofed IP address>

# hping3 <Target IP> -Q -p 139 -s

Hping, komut satırında -Q bağımsız değişkenini kullanarak, hedef ana bilgisayar tarafından oluşturulan tüm TCP sıra numaralarını toplar.

# hping3 –A <Target IP> –p 80

Bu komutu vererek, Hping bir ana bilgisayarın ağda canlı olup olmadığını kontrol eder. Canlı bir ana bilgisayar ve açık bir bağlantı noktası bulursa, bir RST yanıtı döndürür.

# hping3 -S <Target IP> -p 80 --tcp-timestamp

Hping, komut satırına –tcp-timestamp argümanını ekleyerek TCP zaman damgası seçeneğini etkinleştirir ve hedef ana bilgisayarın zaman damgası güncelleme sıklığını ve çalışma süresini tahmin etmeye çalışır.

# hping3 –F –P –U 10.0.0.25 –p 80

Saldırgan, bu komutu vererek, hedef ana bilgisayardaki 80 numaralı bağlantı noktasında FIN, PUSH ve URG taramaları gerçekleştirebilir.

# hping3 –scan 1-3000 -S 10.10.10.10

Burada –scan parametresi taranacak port aralığını tanımlar ve –S SYN bayrağını temsil eder

# hping3 10.10.10.10 --udp --rand-source --data 500

UDP paket işçiliği gerçekleştirin

**DoS ve DDoS korumasını test etmek için birden fazla istek oluşturun**

Bu araç aynı zamanda, sistemimizin DoS ve DDoS gibi ağ saldırılarına karşı kararlılığını kontrol etmemize olanak tanıyarak ya localhost'a ya da ağın içindeki (ya da dışındaki) başka bir sunucuya yönelik gerçek testler oluşturur.

TCP / IP paketlerinde aynı kaynak IP'sini basitçe yazarak değiştirerek bir dizi benzersiz ping yapabiliriz:

# hping3 --rand-source 192.168.1.1

Aynı şekilde, paketlerin gerçek zamanlı olarak toplu olarak gönderilmesi için –flood parametresini ekleyebiliriz. Bu şekilde, öncelikle güvenlik duvarımızın çalışıp çalışmadığını ve ikinci olarak sistemimizin bir DDoS saldırısı tehdidine ne kadar iyi yanıt verdiğini kontrol edebileceğiz.

# hping3 --rand-source --flood 192.168.1.1

Sadece birkaç saniye içinde 25,000'den fazla paket ürettik, bu yüzden ağımız engellenmiş ve kullanılamaz olabileceğinden dikkatli olmalıyız.

Bununla birlikte, sürekli olarak hedef sunucuya (bu durumda 192.168.1.1) gönderilecek olan "yanlış kökenli" (rand-source parametresi sayesinde) çok sayıda paket üretilmeye başlayacaktır. Bu şekilde, sistemimizin DDoS saldırılarına karşı sağlamlığını doğrulayabiliriz, çünkü sistem çalışmayı durdurursa veya çökerse, bir yapılandırma hatası olabilir ve bunun gerçek bir ortamda olmasını önlemek için ilgili önlemleri uygulamamız gerekir.

Bu araç çok kullanışlıdır, ancak her zaman kapalı ve kontrollü ortamlarda kullanılmalıdır, çünkü dışarı çıkarken yapmamamız gereken bir takıma hizmet reddi saldırısı gerçekleştirmemiz mümkündür, bu yasa dışıdır ve yaptırımla sonuçlanabilir.

## KAYNAKÇA


https://tools.kali.org/information-gathering/hping3

http://www.cozumpark.com/blogs/gvenlik/archive/2010/03/07/hping-kullanarak-tcp_3101_p-paketleriyle-oynama-b-l-m-1.aspx

https://www.bgasecurity.com/2011/07/hping-kullanarak-dns-flood-dosddos/

https://nmap.org/book/idlescan.html

https://networkkampus.com/centos-hping3-komutu/

https://www.ozztech.net/siber-guvenlik/hping3-nedir/

http://wiki.hping.org/94

https://www.kali.org/tools/hping3/

https://www.turkhackteam.org/konular/hping3-nedir-ne-ise-yarar-nasil-kullanilir-eronmay.1867813/

https://yemresarica.medium.com/hping3-nedir-nas%C4%B1l-kullan%C4%B1l%C4%B1r-8a0314b20c45

https://ozdenercin.com/2018/08/01/hping3-kurulumu-ve-kullanimi/

https://hayalindekiyazilim.com/penetration/hping3-nedir-nasil-kullanilir-wireshark/

https://diarium.usal.es/pmgallardo/2020/10/16/hping3-syntax/

https://iphelix.medium.com/hping-tips-and-tricks-85698751179f