
# Hping ile Ağ Keşif Çalışmaları

## [Hping-III Port/Host Tarama ]

**Huzeyfe ÖNAL <huzeyfe@lifeoverip.net>**

**28 Mart 2010**

*[Hping serisinin bu bölümünde Hping kullanarak TCP/IP ağlarda bilgi toplama konusu işlenmiştir. ]*

# Contents

# Ağ Keşif Çalışmaları

Güvenlik denetimi testlerinde(pentest)hedef sistem hakkında bilgi toplama ilk ve en önemli adımdır. Bilgi toplama adımı aynı zamanda en geniş adımdır ve yapılış şekline göre çeşitli kategorilere ayrılır. Bu kategorilerden biri ağ keşif çalışmalarıdır ve hedef sisteme çeşitli paketler göndererek ağ üzerinden hangi noktalardan nasıl erişilir, hedef sistem üzerinde hangi servisler hizmet vermektedir gibi bilgileri çıkartılmaya çalışılır.

Ağ keşif(Host/Port tarama) işlemi ile hedef sistem hakkında aşağıdaki bilgiler edinilebilir

- Hedef sistemin açık olup olmadığı
- Hedef sistem üzerindeki açık portlar/servisler
- Hedefin işletim sistemi
- Hedef sistemin önündeki router, firewall ve IPS sistemleri
- Hedef sisteminin uptime süresi
- ...

Host/port tarama için çeşitli araçlar vardır. Bunlar arasında en bilinenleri Nmap ve Hping'dir. Nmap bu kategorinin tartışmasız lideridir. Hping de sağladığı özelliklerle çeşitli port tarama işlemlerini yapabilmektedir.

## Host/Port Tarama Çeşitleri

Ağ keşif çalışmalarında hedef sistemlere çeşitli TCP/IP paketleri göndererek dönen cevaplar dan hedef sistem hakkında bilgi toplanır. Gönderilecek paketlerin tiplerine göre taramaların isimleri değişmektedir.

Mesela hedef sisteme TCP SYN bayraklı paketler gönderilerek portun durumunu yoklanıyorsa bu tarama çeşidi TCP SYN Scan olarak adlandırılır.

Aşağıda en sık kullanılan host/port tarama adlandırlamarını bulabilirsiniz.

### Host Keşif Türleri

- Ping
- TCP Ping
- UDPing
- Arping

### Port Tarama Türleri

- TCP Connect() Scan

- TCP SYN Scan
- TCP FIN Scan
- TCP ACK Scan
- TCP XMAS Scan
- TCP NULL Scan
- TCP Window Scan
- UDP Scan
- IP Protocol Scan
- Version detecxtion(Sürüm belirleme)

## Port Tarama Araçları

Güvenlik testlerinde tercih edilen port tarama araçlarını sıralandığında listede mutlaka bulunması gerekenler: Nmap, Nessus, Hping, Unicornscan, scanrand.

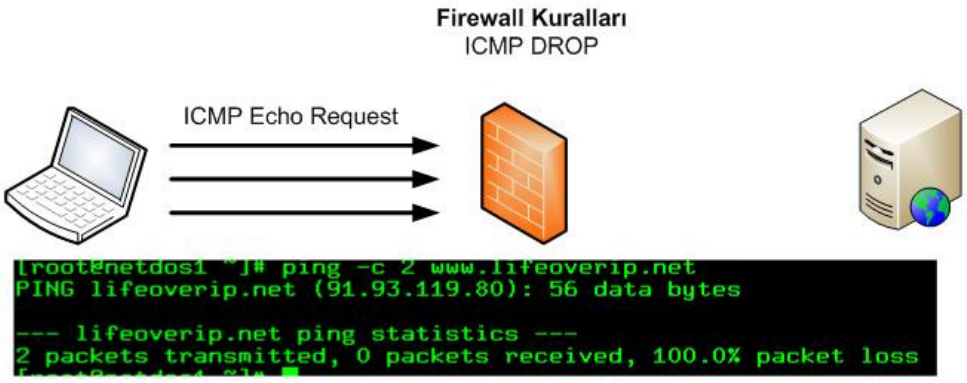
```
[root@netdos1 ~]# nmap --top-ports 10 localhost

Starting Nmap 5.00 ( http://nmap.org ) at 2010-03-28 21:06 EEST
Interesting ports on localhost (127.0.0.1):
PORT     STATE  SERVICE
21/tcp   closed ftp
22/tcp   open   ssh
23/tcp   open   telnet
25/tcp   open   smtp
80/tcp   open   http
110/tcp  closed pop3
139/tcp  closed netbios-ssn
443/tcp  closed https
445/tcp  closed microsoft-ds
3389/tcp closed ms-term-serv

Nmap done: 1 IP address (1 host up) scanned in 2.32 seconds
```

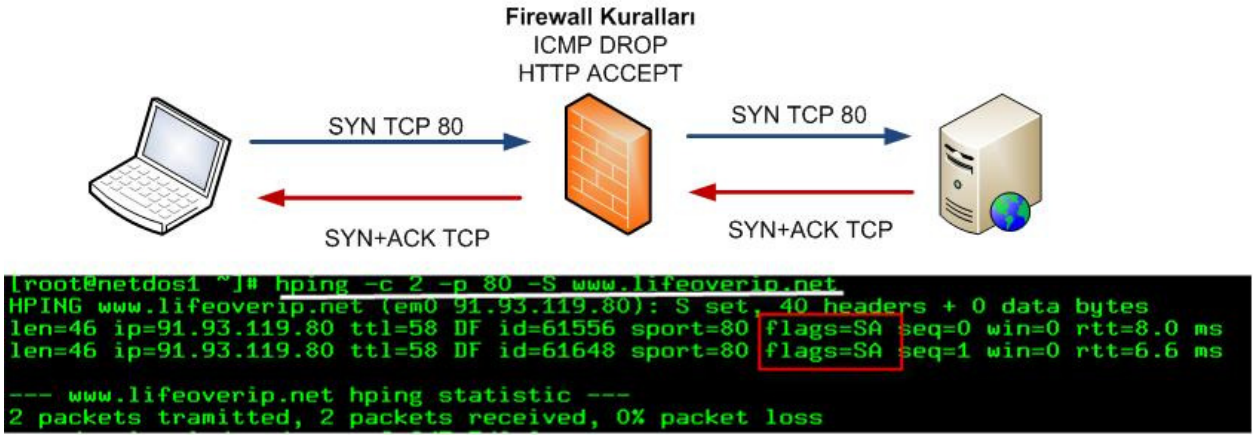
Bu yazının konusu Hping olduğu için bundan sonraki adımlar Hping kullanılarak gerçekleştirilecektir.

## Hping ile Host/Ağ Keşif Çalışmaları

Hping kullanarak herhangi bir IP adresine istediğiniz özelliklerde paket gönderilebilir. Bir IP adresinin çalışır olduğunu anlamanın en klasik yolu ping komutunu çalıştırmaktır. Ping, ICMP echo-request paketleri göndermektedir ve çoğu sistem icmp paketlerini ağa girişte ve çıkışta yasaklamıştır. Burada hedef sistemin durumunu belirleme için TCP ping veya UDP ping kullanılması daha sağlıklı sonuçlar verecektir.

TCP ping, klasik ping progdamındaki icmp paketleri yerine TCP paketlerini kullanır. Hedef sistemde açık olacağını düşündüğünüz portlara çeşitli TCP bayraklı paketler göndererek hedef sistemin açık olup olmadığını anlayabilirsiniz.




## Hping ile Port Tarama

Hedef sistemin açık olduğu belirlendikten sonra hizmet veren servisler(açık portlar) belirleme amacıyla port taraması yapılır. Hping hem TCP hem de UDP üzerinden port tarama yapabilir. Hping ile port tarama yapmadan önce bilinmesi gereken iki temel husus:

1. Hping Nmap gibi özelleştirilmiş port tarama aracı değildir, TCP/IP paket üretim aracıdır.
2. Hping port taramalarında birden fazla host taramak için ideal değildir.

TCP kullanan port tarama tipleri bayraklarla oynayarak gerçekleştirlir. Hping ile de istenilen türde TCP paketleri oluşturulacağı için diğer port tarama araçlarındaki port tarama çeşitleri rahatlıkla hping ile gerçekleştirilebilir.

## Hping ile SYN Scan

```
#hping -S vpn.lifeoverip.net -p 21 -c 2
HPING vpn.lifeoverip.net (fxp0 80.93.212.86): S set, 40 headers + 0 data bytes
len=46 ip=80.93.212.86 ttl=64 DF id=39414 sport=21 flags=SA seq=0 win=16384
rtt=0.4 ms
```

### SYN Tarama İncelemesi

1. Hping hedef sisteme SYN bayraklı TCP paketi gönderir.
2. Hedef sistem SYN bayraklı paketi alır ve uygun TCP paketini (SYN/ACK ya da RST ) cevap olarak döner.
3. Paket gönderen (hping çalıştıran ) taraftaki işletim sistemi böyle bir paket beklemedigi için dönen SYN/ACK bayraklı TCP paketine RST cevabı döner.

```
#tcpdump -i fxp0 -tttnn tcp port 21
000000 IP 172.16.10.2.2023 > 80.93.212.86.21: S 706083143:706083143(0) win 512
000213 IP 80.93.212.86.21 > 172.16.10.2.2023: S 3082095413:3082095413(0) ack
706083144 win 16384 <mss 1460>
000224 IP 172.16.10.2.2023 > 80.93.212.86.21: R 706083144:706083144(0) win 0
```

++port_numarası kullanarak her seferinde port numarasının bir artmasını sağlanıp dönen dönen cevaplardan portların durumu hakkında bilgi edinilebilir. Dönen cevap SA ise port açık demektir, RA ise kapalıdır. Cevap dönmüyorsa firewall vardır ya da host kapalıdır denilebilir.

```
# hping -S 192.168.1.1 -p  ++22

HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=22 flags=SA seq=0 win=5840 rtt=6.2 ms
len=46 ip=192.168.1.1 ttl=64 DF id=0 sport=23 flags=SA seq=1 win=5840 rtt=0.9 ms
len=46 ip=192.168.1.1 ttl=255 DF id=0 sport=24 flags=RA seq=2 win=0 rtt=0.8 ms
```

```
len=46 ip=192.168.1.1 ttl=255 DF id=0 sport=25 flags=RA seq=3 win=0 rtt=0.8 ms
len=46 ip=192.168.1.1 ttl=255 DF id=0 sport=26 flags=RA seq=4 win=0 rtt=0.7 ms
len=46 ip=192.168.1.1 ttl=255 DF id=0 sport=27 flags=RA seq=5 win=0 rtt=0.7 ms
--- 192.168.1.1 hping statistic ---
13 packets tramitted, 13 packets received, 0% packet loss
round-trip min/avg/max = 0.7/1.2/6.2 ms
```

## FIN Scan

Hedef sisteme FIN bayraklı TCP paketleri göndererek sistemin port durumlarını belirlenebilir.

### FIN Scan Örnegi

**Kapalı Portlar için RST beklenir**

```
# hping -F -p 1000 192.168.1.3 -n -c 1
HPING 192.168.1.3 (eth0 192.168.1.3): F set, 40 headers + 0 data bytes
len=46 ip=192.168.1.3 ttl=128 id=22870 sport=1000 flags=RA seq=0 win=0 rtt=72.2 ms
```

**Açık/Firewalla korunmuş portlar için :** Herhangi bir cevap dönmez

```
# hping -F -p 111 192.168.1.4 -c 2
HPING 192.168.1.4 (eth0 192.168.1.4): F set, 40 headers + 0 data bytes
--- 192.168.1.4 hping statistic ---
2 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

## XMAS Scan

Bu tarama tipinde amaç hedef sisteme FIN/URG/PSH bayrakları set edilmis TCP paketleri Gönderilip kapalı sistemler için RST/ACK, açık sistemler için cevap dönmemesini beklenir.

### Hping ile XMAS tarama

#hping –FUP hedef_sistem -p 80

Port numarasını tarama esnasında arttırma için Ctrl+z tuş kombinasyonu kullanılabilir.

```
# hping -FUP www.lifeoverip.net -p 80
HPING www.lifeoverip.net (em0 91.93.119.80): FPU set, 40 headers + 0 data bytes
83: ^Z
84:
^C
--- www.lifeoverip.net hping statistic ---
8 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

## Gelişmiş Port Tarama Seçenekleri

Hping ile yapılan port taramalarda klasik port tarama araçlarına benzer düzenli çıktı almak için –scan parametresi kullanılabilir. Birden fazla port tarama için port numaralarını aralarına virgül ekleyerek çoğaltılabilir ya da port aralığını test etmek için – işareti kullanılır.

```
# hping --scan 21,22,23,80,110,130-143 -S 194.27.72.88
Scanning 194.27.72.88 (194.27.72.88), port 21,22,23,80,110,130-143
19 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name | flags |ttl| id | win | len |
+----+-----------+---------+---+-----+-----+-----+
21 ftp : .S..A... 56 52428 65535 46
22 ssh : .S..A... 56 52684 65535 46
80 http : .S..A... 56 52940 65535 46
110 pop3 : .S..A... 56 53196 65535 46
All replies received. Done.
Not responding ports: (130 cisco-fna) (131 cisco-tna) (132 cisco-sys) (133 statsrv) (134
ingres-net) (135 loc-srv) (136 profile) (137 netbios-ns) (138 netbios-dgm) (139 netbiosssn
) (140 emfis-data) (141 emfis- cntl) (142 bl-idm) (143 imap)
```

Tüm portları taramak için all , wellknown portları taramak için known kelimeleri kullanılabilir.

## Hedef Belirleme

Hping ile port tarama yaparken birden fazla host seçimi yapılamaz fakat subnet taramaları için ip adresinin son byte'ına x yazılarak o ip subnetini random olarak tarama yapması sağlanabilir.

#hping -S --scan 22 --rand-dest 91.93.119.x -I em0 –V

--rand-dest kullanımında –I arabirim_ismi ile paketlerin hangi arabirimden çıkacağı belirltilmelidir.

## Port Taramalarda kaynak port belirtimi

Öntanımlı olarak paket gönderiminde kaynak portu rastgele belirlenir ve her gönderilen paket için bu değer bir arttırılır. –s parametresi kullanılarak paket gönderiminde kaynak portu istenilen değere ayarlanabilir ve kaynak portun her pakette artmaması için –k parametresi kullanılır.

```
# hping -s 80 -S www.lifeoverip.net -p 80 -c 2
HPING www.lifeoverip.net (em0 91.93.119.80): S set, 40 headers + 0 data bytes
len=46 ip=91.93.119.80 ttl=58 DF id=9552 sport=80 flags=SA seq=0 win=0 rtt=2.7 ms
len=46 ip=91.93.119.80 ttl=58 DF id=9631 sport=80 flags=SA seq=1 win=0 rtt=3.1 ms

--- www.lifeoverip.net hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 2.7/2.9/3.1 ms
```

### Tcptimestamp taraması ile sistemlerin uptime sürelerini belirleme

Hping kullanarak hedef sistemin uptime süresi –eğer özellikle kapatılmamışsa- belirlenebilir. Bunun için –tcp-timestamp parametresi kullanılır.

```
# hping --tcp-timestamp hackme.lifeoverip.net -p 80 -S -c 2
HPING hackme.lifeoverip.net (em0 91.93.119.77): S set, 40 headers + 0 data bytes
len=56 ip=91.93.119.77 ttl=58 DF id=0 sport=80 flags=SA seq=0 win=5792 rtt=7.9 ms
  TCP timestamp: tcpts=3285074461

len=56 ip=91.93.119.77 ttl=58 DF id=0 sport=80 flags=SA seq=1 win=5792 rtt=6.1 ms
  TCP timestamp: tcpts=3285075489
  HZ seems hz=1000
  System uptime seems: 38 days, 0 hours, 31 minutes, 15 seconds

[root@netdos1 ~]#
```

Eğer tcp-timestamp alma engellenmişse aşağıdakine benzer çıktı alınacaktır.

```
# hping --tcp-timestamp www.lifeoverip.net -p 9100 -S
HPING www.lifeoverip.net (em0 91.93.119.80): S set, 40 headers + 0 data bytes
len=46 ip=91.93.119.80 ttl=58 DF id=55256 sport=9100 flags=SA seq=0 win=0 rtt=7.8 ms
len=46 ip=91.93.119.80 ttl=58 DF id=55290 sport=9100 flags=SA seq=1 win=0 rtt=7.3 ms
```

## TCP Sıra numarası güçlülük testi

Hping kullanarak hedef sistemin ürettiği TCP sıra numaralarının tahmin edilebilir olup olmadığı anlaşılabilir.

```
# hping --seqnum -p 80 www.lifeoverip.net -S
HPING www.lifeoverip.net (em0 91.93.119.80): S set, 40 headers + 0 data bytes
3856045788 +3856045788
3482308560 +3921230067
 147723720 +960382455
3878839756 +3731116036
1018419143 +1434546682
3603746947 +2585327804
 105817863 +797038211
```

Eğer tcp sıra numarası tahmin edilebilir bir sistemse aşağıdakine benzer çıktı verecektir.

```
#hping –seqnum –p 23 10.10.10. –S
2361294848 +2361294848
 2411626496 +50331648
2545844224 +134217728
2713616384 +167772160
2881388544 +167772160
3049160704 +167772160
3216932864 +167772160
3384705024 +167772160
3552477184 +167772160
3720249344 +167772160
```

## Hping ile Port Taramalarında IPS/Firewall Şaşırtma

Test yapılacak sistemin önünde yapılan port taramalarını izleyen ve alarm üreten bir yapı varsa bu yapı tuzak sistemler kullanarak yanıltılabilir. Hping'in Nmap'deki "–Decoy Scan" e benzer bir özelliği olmasa da aynı anda iki adet hping çalıştırarak birinde gerçek ip adresimizden diğerinde de spoof edilmiş ip adreslerinden paket göndererek hedef sisteme yapılacak port taramaların IDS/IPS loglarında anlaşılmayacak şekilde loglanması sağlanabilir.

Örnek:

Farklı ip adreslerinden geliyormuş gibi gözüken tarama

#hping --rand-source -p ++22 -S www.lifeoverip.net

Gerçek IP adresinden yapılan tarama

# hping --scan 22-1000 -S www.lifeoverip.net

## Tarama sonucu dönen cevapları inceleme

Nmap'in –reason parametresi port taramalarında bir portun neden açık/kapalı olduğunu ekranda göstermeye yarar. Benzer çıktıyı Hping ile almak için –V parametresi kullanılır.

Nmap –reason

```
# nmap -p1-22 localhost –reason

Starting Nmap 4.90RC2 ( http://nmap.org ) at 2009-08-06 10:53 EDT
Warning: Hostname localhost resolves to 2 IPs. Using 127.0.0.1.
Interesting ports on localhost (127.0.0.1):
PORT   STATE    SERVICE     REASON
1/tcp  closed   tcpmux      reset
2/tcp  closed   compressnet reset
3/tcp  closed   compressnet reset
4/tcp  closed   unknown     reset
5/tcp  closed   unknown     reset
6/tcp  closed   unknown     reset
20/tcp filtered ftp-data    no-response
21/tcp open     ftp         syn-ack
22/tcp open     ssh         syn-ack

Nmap done: 1 IP address (1 host up) scanned in 1.26 seconds
```

```
# hping -V --scan 1-22 -S localhost
using lo, addr: 127.0.0.1, MTU: 16436
Scanning localhost (127.0.0.1), port 1-22
22 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+
|port| serv name |  flags  |ttl| id  | win |
+----+-----------+---------+---+-----+-----+
   1 tcpmux    : ..R.A...  64    0    0
   2 nbp       : ..R.A...  64    0    0
   3           : ..R.A...  64    0    0
   4 echo      : ..R.A...  64    0    0
   5           : ..R.A...  64    0    0
   6 zip       : ..R.A...  64    0    0
   7 echo      : ..R.A...  64    0    0
```

```
  8          : ..R.A...  64    0    0
  9 discard  : ..R.A...  64    0    0
 10          : ..R.A...  64    0    0
 11 systat   : ..R.A...  64    0    0
 12          : ..R.A...  64    0    0
 13 daytime  : ..R.A...  64    0    0
 14          : ..R.A...  64    0    0
 15 netstat  : ..R.A...  64    0    0
 16          : ..R.A...  64    0    0
 17 qotd     : ..R.A...  64    0    0
 18 msp      : ..R.A...  64    0    0
 19 chargen  : ..R.A...  64    0    0
 21 ftp      : .S..A...  64    0 32792
 22 ssh      : .S..A...  64    0 32792
All replies received. Done.
Not responding ports: (20 ftp-data)
```

-V parametresi çıkartılırsa sadece açık olan portlar çıktı verir.
Burada 20. Port için herhangi bir cevap dönmediğimi görüyoruz, bu 20.portun Firewall tarafından korunduğunu gösterir.

## Syncookie aktif olan makinlerde port tarama

Sistemleri internetten gelecek SynFLood ataklarına karşı korumak için Syncookie/proxy korumalı cihazlar varsa bu sistemlere karşı yapılacak taramaların sonuçları şaşırtıcı olacaktır. Syncookie tüm gelen SYN isteklerine doğrudan SYN-ACK döneceği için SYN Scan ve TCP Connect Scan türleri sağlıklı sonuç vermeyecektir. Bu gibi durumlarda versiyon belirleme özelliklerine sahip araçlar kullanılmalıdır.

```
# hping  --scan 22-1000 -S www.lifeoverip.net
Scanning www.lifeoverip.net (91.93.119.80), port 22-1000
979 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+-----+
|port| serv name |  flags  |ttl| id  | win | len |
+----+-----------+---------+---+-----+-----+-----+
  68 bootpc     : .S..A...  58 48400    0   46
  72 netrjs-2   : .S..A...  58 48656    0   46
  95 supdup     : .S..A...  58  1809    0   46
  22 ssh        : .S..A...  58 48912    0   46
  96 dixie      : .S..A...  58  2321    0   46
  23 telnet     : .S..A...  58 49168    0   46
  24            : .S..A...  58 49424    0   46
```

```
25 smtp      : .S..A...  58 49680    0   46
27 nsw-fe    : .S..A...  58 49936    0   46
29 msg-icp   : .S..A...  58 50448    0   46
26           : .S..A...  58 50192    0   46
28           : .S..A...  58 50704    0   46
30           : .S..A...  58 50960    0   46
31 msg-auth  : .S..A...  58 51216    0   46
32           : .S..A...  58 51472    0   46
35           : .S..A...  58 51728    0   46
34           : .S..A...  58 51984    0   46
33 dsp       : .S..A...  58 52240    0   46
```

## Traceroute Aracı olarak Hping

Windows tracert aracı ICMP paketlerini kullanarak, Linux traceroute aracı yüksek numaralı udp portlarını kullanarak hedef sistemlere giden yolu bulabilir.(Router-Firewall-Sunucu). Günümüzde çoğu sistem icmp paketlerini ve yüksek numaralı udp portlarına geçiş izni vermeyeceği için yapılan klasik trace çalışmaları sağlıklı sonuçlar üretemez. Hping kullanarak hem istenilen udp portundan hem de tcp portundan hedef sistemlere trace çalışması yapılabilir.

### TCP kullanarak traceroute

```
# hping -T 1 194.27.72.88 -p 80 -S -n
HPING 194.27.72.88 (eth0 194.27.72.88): S set, 40 headers + 0 data bytes
TTL 0 during transit from ip=192.168.1.1
2: TTL 0 during transit from ip=88.235.72.1
TTL 0 during transit from ip=88.235.72.1
3: TTL 0 during transit from ip=212.156.24.150
7: TTL 0 during transit from ip=193.255.0.62
TTL 0 during transit from ip=193.255.0.62
8: TTL 0 during transit from ip=194.27.72.88
TTL 0 during transit from ip=194.27.72.88
9: len=46 ip=194.27.72.88 ttl=56 DF id=46970 sport=80 flags=SA seq=31 win=65535
rtt=20.8 ms
len=46 ip=194.27.72.88 ttl=56 DF id=46972 sport=80 flags=SA seq=32 win=65535
rtt=18.2 ms
10: len=46 ip=194.27.72.88 ttl=56 DF id=46973 sport=80 flags=SA seq=33 win=65535
rtt=18.7 ms
--- 194.27.72.88 hping statistic ---
```

```
34 packets tramitted, 17 packets received, 50% packet loss
round-trip min/avg/max = 18.2/19.2/20.8 ms
```

-t ile ilk paketin hangi TTL degeri ile başlayacağı belirtilir. –z ile TTL degeri istenildiği zaman Ctrl ^z tus fonksiyonları ile arttırılabilir.

-p ile port numarası belirtilir, herhangi bir port numarası belirledikten sonra tarama esnasında CTRL^z tusuna basarak her pakette port numarasının bir arttırılmasını saglayabiliriz

## UDP Kullanarak Traceroute.

Klasik traceroute araçları yüksek seviyeli UDP portlarını kullandığı için birçok ağa girişte engellenmiştir.

Klasik Traceroute komutu çıktısı

```
# traceroute 195.175.39.40
traceroute to 195.175.39.40 (195.175.39.40), 64 hops max, 40 byte packets
 1  212.98.228.241 (212.98.228.241)  0.658 ms  0.674 ms  0.607 ms
 2  62.244.216.145 (62.244.216.145)  0.229 ms  0.216 ms  0.234 ms
 3  212.98.229.240 (212.98.229.240)  0.231 ms  0.206 ms  0.228 ms
 4  84.44.45.21 (84.44.45.21)  1.657 ms  0.588 ms  0.655 ms
 5  195.175.51.157 (195.175.51.157)  238.309 ms  32.824 ms  20.187 ms
 6  gayrettepe-t2-1-gayrettepe-t3-2.turktelekom.com.tr (212.156.118.17)  2.176 ms  5.532 ms
10.456 ms
 7  * * *
 8  * *^C
```

Hping kullanarak istenilen UDP portundan hedef sisteme trace işlemi yapılabilir. Özellikle birçok ağda DNS sunucu olduğu için UDP 53 portuna doğru trafik açık bırakılır.

```
# hping --udp -T 195.175.39.40 -p 53
HPING 195.175.39.40 (em0 195.175.39.40): udp mode set, 28 headers + 0 data bytes
hop=1 TTL 0 during transit from ip=212.98.228.241 name=UNKNOWN
hop=1 hoprtt=4.7 ms
len=155 ip=195.175.39.40 ttl=56 DF id=0 seq=0 rtt=0.0 ms
hop=2 TTL 0 during transit from ip=62.244.216.145 name=UNKNOWN
```

hop=2 hoprtt=0.3 ms
len=155 ip=195.175.39.40 ttl=56 DF id=0 seq=0 rtt=0.0 ms
***hop=3 TTL 0 during transit from ip=212.98.229.240 name=UNKNOWN***
hop=3 hoprtt=0.6 ms
len=73 ip=195.175.39.40 ttl=56 DF id=0 seq=0 rtt=0.0 ms
len=73 ip=195.175.39.40 ttl=56 DF id=0 seq=0 rtt=0.0 ms
***hop=4 TTL 0 during transit from ip=84.44.45.21 name=UNKNOWN***
hop=4 hoprtt=0.7 ms
len=152 ip=195.175.39.40 ttl=56 DF id=0 seq=0 rtt=0.0 ms
***hop=5 TTL 0 during transit from ip=195.175.51.157 name=UNKNOWN***
hop=5 hoprtt=11.9 ms
len=141 ip=195.175.39.40 ttl=56 DF id=0 seq=0 rtt=0.0 ms
***hop=6 TTL 0 during transit from ip=212.156.118.17 name=gayrettepe-t2-1-gayrettepe-t3-2.turktelekom.com.tr***
hop=6 hoprtt=1.2 ms
len=284 ip=195.175.39.40 ttl=56 DF id=0 seq=0 rtt=0.0 ms
***hop=7 TTL 0 during transit from ip=195.175.39.2 name=UNKNOWN***
hop=7 hoprtt=0.6 ms
len=139 ip=**195.175.39.40** ttl=56 DF id=0 seq=0 rtt=0.0 ms

## Hping ile ICMP Üzerinden Bilgi Toplama

Çoğu networkte icmp request paketleri engellenmekte fakat icmp sadece bu iki tipten oluşmamaktadır. Icmp kullanarak MITM saldirilari, dos saldırıları, hedef sistemler hakkında bilgi toplama yapılabilmekte ve bu tip icmp mesajları guvenlik duvarlarindan açık unutulmaktadır.

### ICMP paketleriyle subnet mask öğrenme

**# hping --icmp-addr -c 1 10.10.10.1**
HPING 10.10.10.1 (bce1 10.10.10.1): icmp mode set, 28 headers + 0 data bytes

--- 10.10.10.1 hping statistic ---
1 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

Eger bu tip icmp paketlerine cevap veriyor olsaydı aşağidaki gibi bir sonuç verecekti.

**ICMP address mask: icmpam=255.255.255.0**

--icmp yardım menusu

```
# hping --icmp-help
ICMP help:
 ICMP concerned packet options:
  --icmp-ipver     set ip version              ( default 4 )
  --icmp-iphlen    set ip header lenght        ( default IPHDR_SIZE >> 2)
  --icmp-iplen     set ip total lengtht        ( default real lenght )
  --icmp-ipid      set ip id                   ( default random )
  --icmp-ipproto   set ip protocol             ( default IPPROTO_TCP )
  --icmp-ipsrc     set ip source               ( default 0.0.0.0 )
  --icmp-ipdst     set ip destination          ( default 0.0.0.0 )
  --icmp-srcport   set tcp/udp source port     ( default random )
  --icmp-dstport   set tcp/udp destination port ( default random )
  --icmp-cksum     set icmp checksum           ( default the right cksum)
```