



Hping ile IP, ICMP ve UDP Paketleri Oluşturma

Hping -II

Huzeyfe ÖNAL <huzeyfe@lifeoverip.net>

10 Kasım 2009

[Hping yazısının ikinci bölümünde IP, ICMP ve UDP paketlerinin detayları ve hping ile bu protokollere ait özelleştirilmiş paketlerin nasıl oluşturulacağından bahsedilecektir.]

Contents

IP Paketleriyle Oynama	3
Hping ile spoof edilmiş paketler oluşturma(IP Spoofing)	3
ICMP Paketleriyle Oynama	5
Broadcast ICMP Paketleri	6
UDP Paketleriyle Oynama	7
UDP kullanarak traceroute	7
Broadcast UDP Paketleri.....	8

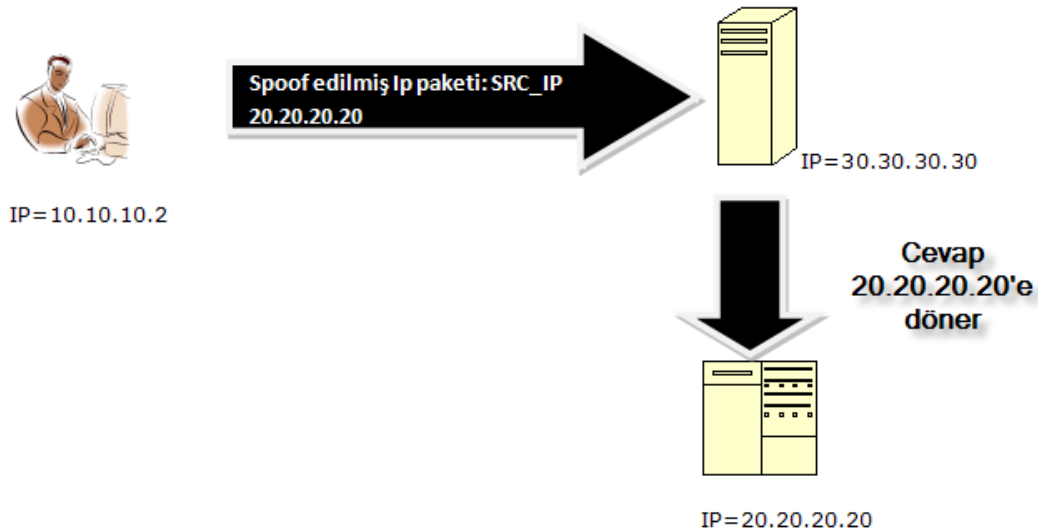
IP Paketleriyle Oynama

Hping ile IP paketlerine ait istenilen alanlar düzenlenebilir. IP başlığına bakılırsa en önemli alanların kaynak_ip adresi, hedef_ip adresi, paket parçalama opsiyonu ve ip id numarası olduğu görülecektir.

```
Internet Protocol, Src: 91.93.119.80 (91.93.119.80), Dst: 192.168.2.27 (192.168.2.27)
  Version: 4
  Header length: 20 bytes
  Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  Total Length: 108
  Identification: 0xfb7e (64382)
  Flags: 0x04 (Don't Fragment)
    0... = Reserved bit: Not set
    .1.. = Don't fragment: Set
    ..0. = More fragments: Not set
  Fragment offset: 0
  Time to live: 56
  Protocol: TCP (0x06)
  Header checksum: 0xb19c [correct]
    [Good: True]
    [Bad : False]
  source: 91.93.119.80 (91.93.119.80)
  destination: 192.168.2.27 (192.168.2.27)
```

IP Başlığı

Hping ile spoof edilmiş paketler oluşturma(IP Spoofing)



Hping kullanarak istenilen ip adresinden geliyormuş gibi paketler üretilebilir. Burada dikkat edilmesi gereken husus kaynak ip adresini spoof ederek gönderdiğimiz paketler hedefe ulaştıktan sonra dönecek cevabın bize değil spoof edilmiş ip adresine döneceğidir.

Örnek: www.lifeoverip.net adresine 10.10.10.10 ip adresinden geliyormuş gibi SYN paketleri gönderelim.

```
# hping -a 10.10.10.10 -S -p 80 www.lifeoverip.net
```

```
HPING www.lifeoverip.net (r10 91.93.119.80): S set, 40 headers + 0 data bytes
```

```
--- www.lifeoverip.net hping statistic ---
```

```
3 packets tramitted, 0 packets received, 100% packet loss
```

```
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Ekrandaki sonuç incelenirse geriye hiç paket dönmediği(**100% packet loss**) görülecektir. Bunun sebebi gönderdiğimiz paketlere dönen cevapların 10.10.10.10 ip adresine gitmesidir.

10.10.10.10 ip adresi de –eğer varsa böyle bir adres- kendisine gelen bu paketlere RST bayraklı TCP paketleriyle cevap dönecektir.

Rastgele Spoof edilmiş ip adreslerinden paket gönderme

Özellikle DOS/DDOs saldırılarının simülasyonlarında faydalı olan bir özelliktir. Hedef sisteme milyonlarca farklı ip adresinden geliyormuş gibi istek gönderilebilir.

```
# hping --rand-source -S -p 80 www.lifeoverip.net
```

Paketlerin TTL değeriyle oynanması

Paket oluştururken ip seviyesinde belirlenebilecek diğer bir özellik de paketlerin yaşam süresini belirleyen TTL değeridir. Hping ile istediğimiz ttl değerini pakete atayabiliriz.

```
#hping -t 10 www.google.com -p 80 -S
```

Burada dikkat edilmesi gereken husus TTL değerleri düşükse paketimizin hedefe ulaşmadan zaman aşımına uğramasıdır.

```
# hping -t 10 www.google.com -p 80 -S
```

```
HPING www.google.com (r10 209.85.229.104): S set, 40 headers + 0 data bytes
```

```
TTL 0 during transit from ip=209.85.255.176 name=UNKNOWN
```

```
TTL 0 during transit from ip=209.85.255.176 name=UNKNOWN
```

```
TTL 0 during transit from ip=209.85.255.176 name=UNKNOWN
```

```
TTL 0 during transit from ip=209.85.255.178 get hostname...^C
```

```
--- www.google.com hping statistic ---
```

```
4 packets tramitted, 3 packets received, 25% packet loss
```

```
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

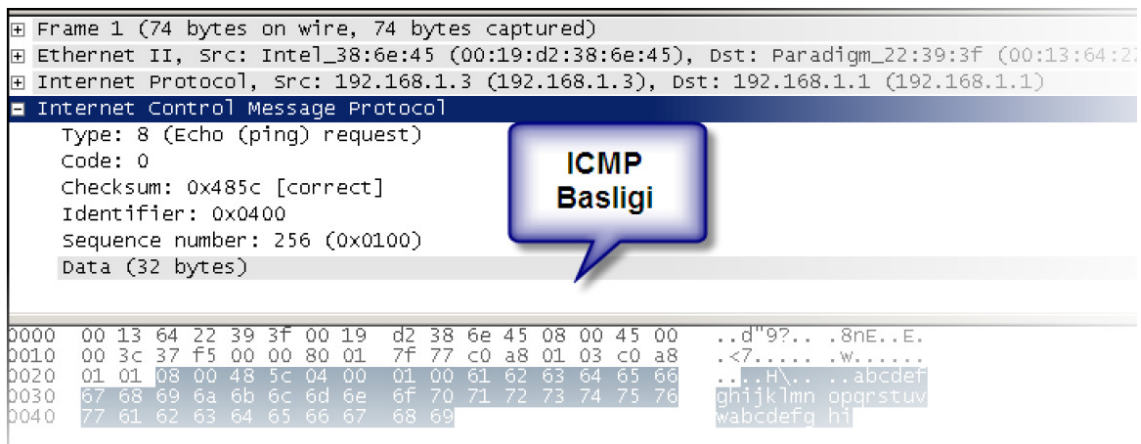
Çıktıdan da görüleceği gibi ttl değerini 10 yapıp gönderdiğimiz paketler Google.com'a ulaşmadan aradaki bir Router tarafından düşürülüyor ve bize bilgi mesajı olarak icmp paketleri dönüyor.

Ham IP Paketleri Oluşturma

Raw ip paketleri oluşturmak için hping'e ilk olarak -rawip parametresinin verilmesi gerekir. Özellikle network cihazlarının testlerinde bu tip paketler çok işe görmektedir.

ICMP Paketleriyle Oynama

ICMP diğer protokollere yardımcı olmak amacıyla tasarlanmış bir protokoldür. IP ve UDP paketlerinde herhangi bir hata mekanizmasının olmaması(ttl expire olunca geriye icmp mesajı dönmesi, kapalı udp portundan icmp mesajı dönmesi) ICMP'nin kullanımını kaçınılmaz kılmaktadır.



```

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 (00:13:64:22:39:3f)
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 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 ;

Icmp type 3 mesajı "Destination Unreachable"

Manasına gelmektedir fakat hedef ulaşılamaz(**Destination Unreachable**) mesajı da farklı anlamlar içerebilir. İşte 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]

Tüm icmp type/code degerlerine <http://www.iana.org/assignments/icmp-parameters> adresinden ulasilabilir.

Hping ile ICMP tipi ve kodu belirtmek için kullanılan parametreler.

-C --icmp-type type
-K --icmp-code code

icmp paket olustururken kullanilabilecek diger seceenekler için **hping -icmp-help** komutu kullanilabilir.

Klasik ping paketi(icmp echo request) olusturmak

Hatırlatma: Hergün defalarca kullandığımız ping aracı ICMP paketleriyle çalışır

hping --icmp 10.10.10.2 -K 0 -C 8

```
HPING 10.10.10.2 (r1 10.10.10.2): icmp mode set, 28 headers + 0 data bytes
len=46 ip=10.10.10.2 ttl=64 id=23972 icmp_seq=0 rtt=0.2 ms
len=46 ip=10.10.10.2 ttl=64 id=23981 icmp_seq=1 rtt=0.1 ms
^C
```

UDP ve ICMP ilişkisi

UDP'de TCP benzeri bayrak mekanizması olmadığı için paketin durumuna ait bilgiler icmp mesajlarıyla iletilir. Mesela TCP'de kapalı porta gönderilecek bağlantı isteğine RST bayraklı cevap dönülecek ve gönderen işletim sistemi portun kapalı olduğunu anlayacaktır.

UDP'de ise bayrak mekanizması olmadığı için bu işi ICMP yapar. Yani kapalı UDP portuna gönderilen cevaplar icmp dest. Port unreachable mesajıyla cevap verilir.

hping --udp -p 80 10.10.10.2

```
HPING 10.10.10.2 (r1 10.10.10.2): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=10.10.10.2 name=blog.lifeoverip.net
--- 10.10.10.2 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Broadcast ICMP Paketleri

Broadcast paketler tek bir adrese gönderilip o adres altındaki tüm canlı sistemlere ulaşan paketlerdir. Mesela 192.168.2.0 networkünün broadcasti olan 192.168.2.255 adresine bir adet paket gönderirsek bu ağda açık olan tüm sistemler o paketi alır ve uygun cevabı döner(di).

ICMP paketleri broadcast tipte olabilir, bu da çeşitli smurf saldırılarında icmp'nin kullanılabileceğini gösterir. 2000'li yıllarda broadcast adreslere gönderilen icmp paketleriyle ciddi DOS/DDOS saldırıları gerçekleştirilmiştir. Bu saldırılardan edinilen tecrübeler ışığında işletim sistemi ve sınır güvenlik cihazları broadcaste gelen paketlere cevap dönmeyecek şekilde yapılandırılmaya başlandı.

Hping ile hem ip spoofing hem de icmp broadcast özelliği kullanılarak geçmişte yapılan DDOS/DOS saldırıları simüle edilebilir.

UDP Paketleriyle Oynama

TCP/IP ailesinin en basit protokollerinden biridir. Gönderici port numarası, alıcı port numarası , paket boyutu ve checksum değerlerinden oluşan başlık bilgisine sahiptir.

```
[- User Datagram Protocol, Src Port: 64736 (64736), Dst Port: domain (53)
  Source port: 64736 (64736)
  Destination port: domain (53)
  Length: 44
  [- Checksum: 0x3a73 [correct]
    [Good Checksum: True]
    [Bad Checksum: False]
```

Hping ile UDP paketi oluşturma

hping --udp -p 54 localhost

```
HPING localhost (lo0 127.0.0.1): udp mode set, 28 headers + 0 data bytes
ICMP Port Unreachable from ip=127.0.0.1 name=localhost
ICMP Port Unreachable from ip=127.0.0.1 name=localhost
```

Aynı paket açık bir porta gönderilirse cevap dönmeyecektir. Bunun sebebi UDP'nin açık portlara gelen sıradan isteklere cevap dönmemesidir.

hping 10.10.10.1 --udp -p 53

```
HPING 10.10.10.1 (r1 10.10.10.1): udp mode set, 28 headers + 0 data bytes
--- 10.10.10.1 hping statistic ---
4 packets tramitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

istenirse “-s port_numarasi “ parametresiyle kaynak port değeri de belirtilebilir.

UDP kullanarak traceroute

Traceroute genellikle ağlar arası ulaşım yollarını ve bir ağa ulaşmada kullanılacak ağ cihazlarının keşfinde kullanılır. Klasik traceroute programları yüksek numaralı udp portlarına istek göndererek dönen cevapları analiz edip sonuç çıkarmaya çalışır.

Günümüzde güvenlik duvarları bu tip paketlere izin vermediği için genellikle traceroute denemeleri başarısızlıkla sonuçlanır. Hping ile istediğimiz udp portundan trace çekerek sonuca ulaşabiliriz. Özellikle UDP port 53(DNS istekleri) hemen her sistemde açık olacağı için bu port tercih edilebilir.

```
#hping --udp -p 53 195.175.39.49 -T
```

Broadcast UDP Paketleri

UDP paketleri de icmp paketleri gibi broadcast adreslere gönderilebilir. Bunun sonucu olarak yüksek derecede DDOS saldırıları oluşturulabilir. Hping ile hem ip spoofing özelliği hem de udp broadcast mesaj gönderme özelliği kullanılarak bu tip DOS saldırıları simule edilebilir.

Bu yazıda anlatılan konuları daha detaylı ve uygulamalı olarak görmek isterseniz [Uygulamalı TCP/IP Eğitimine](#) katılabilirsiniz.