Hping kullanarak TCP/IP Paketleriyle Oynama

Hping-I

Security Lab

11/2/2009

[Network Penetrasyon testlerinin vazgeçilmez aracı olan hping'in detaylı inceleneceği bu yazı dizisi 5 bölümden oluşmaktadır ve temelden başlayıp en ileri seviye kullanıma kadar çeşitli örneklerle Hping'in efektif kullanımını amaçlamaktadır.]

İçerik Tablosu

Hping Nedir?

Hping, istenilen türde TCP/IP paketleri oluşturmak için kullanılan harikulade bir araçtır. Her ne kadar adı ping komutundan esinlenilse de klasik ping uygulamasından çok daha gelişmiş bir uygulamadır.

Hping, oluşturulacak paketlerde tüm alanları kendimize özgü belirlenebilmesi, dinleme modu ile hostlar arası dosya transferi ve komut çalıştırma özelliği(Truva atı özelliği), IDS/IPS testleri için özel veri alanı belirtilebilmesi(ids imzalarinin testi) gibi ileri düzey özelliklere sahiptir.

Hping'i tüm özellikleriyle 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 gibi). Kısacası hping maharetli ellerde kaliteli bir hamur işlevi görmektedir.

Hping'in kullanılacağı alanlar

Hping'i iyi bir şekilde öğrenip kullanma TCP/IP'nin geçerli olduğu yerlerde(tüm iletişim dünyası) avantaj sağlayacaktır. Kısa kısa hping'in somut olarak nerelerde ne amaçla kullanılacağını listeleyecek olursak;

- İsteğe göre düzenlenmiş TCP, UDP, ICMP, Raw-IP paketleri üretme
- Güvenlik duvarı işlevsellik ve performans testleri
- DOS engelleme sistemleri testleri
- Saldırı Tespit ve Engelleme Sistemleri işlevsellik ve performans testleri
- Gelişmiş port tarama
- Gelişmiş dosya transferi
- TCP/IP protokolleri üzerinden hedef sistemlerden bilgi toplama
- Geçmiş TCP/IP zaafiyetlerinin lab. Ortamında tekrar edilmesi

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.

```
C:\Documents and Settings\root\Desktop\hping2.win32>hping -v
hping version 2.0.0-b1 Support for XP SP2 (Fri March  17 2006)
libpcap based binary

C:\Documents and Settings\root\Desktop\hping2.win32>
```

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

Not: Windows sistemlerde hping'in bazı özellikleri sağlıklı çalışmamaktadır. Hping'in gerçek gücünü görmek için mutlaka Linux/UNIX tabanlı bir sistemde denenmelidir.

Temel Hping Kullanımı

Hping'in paket göndermek için çeşitli modları ve komut satırı parametreleri vardır. Temel olarak hping ile raw ip, icmp, tcp ve udp paketleri üretilebilir. Üretilecek paketlere ait tüm özellikler komut satırından belirtilebilir. Hping ile birlikte kullanılabilecek seçenekleri görmek için –h parametresi kullanılır.

```
[root@mail ~]# 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
```

Hping versiyonu öğrenme

Hping'in yaygın kullanılan iki sürümü vardır. Bunlar; hping2 ve hping3 . Her iki sürümde de bazı özellikleri diğer sürüm tarafından desteklenmemektedir. Hping3, hping2'e göre daha fazla özellik barındırdığı için tercih edilebilir. Kullandığınız sistemde hangi sürüm hping'in kurulu olduğunu öğrenmek için –v parametresi kullanılabilir.

Hping2 kurulu bir sistemden alınacak çıktı

 # hping -v

hping version 2.0.0-rc3 (Mon May 3 10:56:19 CEST 2004)
libpcap based binary

Hping3 kurulu sistemden alınacak çıktı

$ hping -v

hping version 3.0.0-alpha-1 ($Id: release.h,v 1.4 2004/04/09 23:38:56 antirez Exp $)
This binary is TCL scripting capable

Hping Çalışma Modları

Hping çeşitli türde tcp/ip paketleri üretip bunları kullanabilir demiştik. Öntanımlı olarak hping TCP paketleri üretir, bunu değiştirmek için(udp, icmp veya ip yapmak için) aşağıdaki parametreler kullanılabilir.

-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

Hping ile paket gönderimi

Hping kullanarak ilk paketimizi gönderelim. Öntanımlı olarak hping icmp yerine TCP paketlerini kullanır. Yine öntanımlı olarak boş(herhangi bir bayrak set edilmemiş) bir tcp paketini hedef sistemin 0 portuna gönderir ve gelen cevabı ekrana basar. Dolayısıyla hping'de komut satırı parametreleri çok önemlidir. 0. Porta gönderilecek null bayraklı bir

TCP paketi tüm Firewall/IPS cihazları tarafından engellenecektir.

 # 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

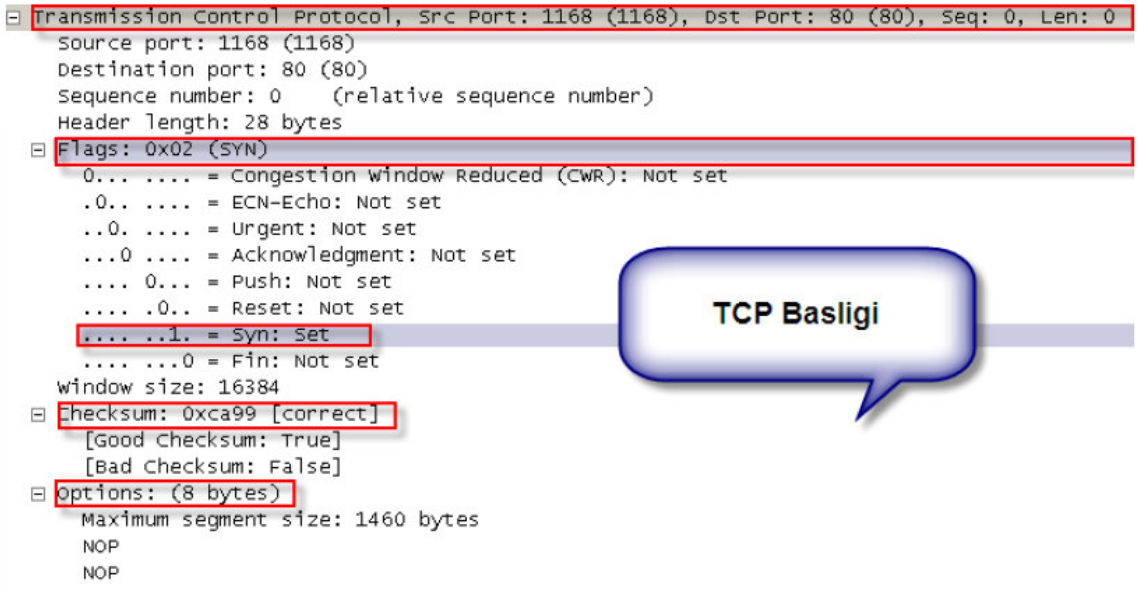
 # tcpdump -i eth0 -tttnn tcp port 0

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

TCP Paketleriyle Oynama

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

TCP oturumunda en önemli bilesen bayrak(flags)lardır. Oturumun kurulması, veri aktarımı, baglantının koparılması vb gibi islerin tamamı bu bayraklar aracılıgı ile yapılır. Hping kullanarak paket oluşturacağımız diğer protokollerde(IP, ICMP, UDP) bayrak tanımı yoktur.



TCP'deki bayraklar ve hping parametreleri

TCP'de 6+2 bayrak vardır. Yoğun olarak 6 tanesi kullanılır ve hping ile aşağıdaki gibi belirtilir(komut satırı parametreleri)

SYN (hping -S)

FIN (hping -F)

RST (hping -R)

ACK (hping -A)

PUSH (hping -P)

URG (hping -U)

İlk oluşturacağımız paket her TCP oturumunun kurulmasında ilk adım olan 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 olusturulan 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.

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
```

Yukarıdaki çıktıda görüleceği üzere hping ile oluşturulan SYN bayraklı TCP paketi hedef sistemin 0. Portuna gitmeye çalışmış ve hedef işletim sistemi tarafından RST paketiyle düşürülmüştür. 0. Port yerine daha farklı portlara paketler gönderilirse farklı sonuçlar elde edilecektir.

Hping çıktısını yorumlama

Hping çıktısı gönderilen pakete dönen cevaı içerir. Eğer paket gönderilen hedef sistem cevap dönmüyorsa ekran boş kalacaktır.

Gönderilen paket:

 # hping -S vpn.lifeoverip.net -p 80

HPING vpn.lifeoverip.net (bce1 91.93.119.80): S set, 40 headers + 0 data bytes

Dönen cevap

len=46 ip=91.93.119.80 ttl=64 DF id=48348 sport=80 flags=SA seq=0 win=65535 rtt=0.1 ms

len => dönen paketin boyutu

ip => paketi gönderen ip adresi(hedef sistem)

ttl => paketin yaşam süresi

DF => Parçalama biti aktif durumda

İd => Ip paketine ait tanımlayıcı biricik(uniq) bilgi

Sport => paketin gönderildiği kaynak port

Flags => aktif TCP bayrakları

seq => paketin sıra numarası

win => paketin pencere boyutu

rtt => Round trip time süresi(milisaniye)

Hping kullanımında port belirtimi

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

-s parametresi ile kaynak TCP portu degistirilebilir, öntanımlı olarak bu deger rastgele atanır.

80.porta SYN bayraklı paket göndermek için

#hping –S –p 80 localhost

Komutu yeterli olacaktır.

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

RST Bayraklı TCP paketleri olusturmak

 # hping -R -c 3 192.168.1.1 –p 80
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 sekilde –R yerine diger TCP bayrak tipleri konularak istenilen türde TCP paketi olusturulabilir.

Aynı pakette birden fazla bayrak kullanımı

Hping ile TCP paketleri oluştururken tek bayrak kullanılmasızorunlu değildir. İstenirse tüm bayrakları set edilmiş TCP paketleri de üretilebilir(tabi bu paket firewallar tarafından düşürülecektir). Özellikle durum korumalı olmayan sistemleri test etmek için SYN/ACK , RST/ACK payraklı paketler kullanılabilir.

 # hping -S -A localhost -p 80

HPING localhost (lo0 127.0.0.1): SA set, 40 headers + 0 data bytes
len=40 ip=127.0.0.1 ttl=64 DF id=54904 sport=80 flags=R seq=0 win=0 rtt=0.0 ms
len=40 ip=127.0.0.1 ttl=64 DF id=54955 sport=80 flags=R seq=1 win=0 rtt=0.0 ms
^C