HPING - Generador de paquetes TCP, UDP o ICMP

Submitted by freed0m on Fri, 06/05/2005 - 10:52.Aplicaciones

Hping es una herramienta muy versátil, que permite la manipulación de paquetes TCP/IP desde línea de comandos.
Es factible modificar la información contenida en las cabeceras de los paquetes ya sean TCP, UDP e ICMP, en función de los parámetros con que ejecutemos Hping.

PARÁMETROS BÁSICOS DE FUNCIONAMIENTO

Entre los parámetros básicos de funcionamiento se incluyen los siguientes:

-c --count esta opción permite especificar el número de paquetes que queremos enviar o recibir.

-i --interval especifica el número de segundos, -iX donde X son los segundos, o micro segundos -iuX, donde X son los segundos, que tienen que transcurrir entre el envió de cada paquete.

--fast alias de tiempo para indicar -i u10000. Para enviar 10 paquetes por segundo.

--faster alias de tiempo para indicar -i u1.

-n --numeric trata la salida de datos únicamente como números, no hace resolución inversa de host, etc..

-I --interface permite especificar el interfaz de red por donde enrutar el tráfico generado.

-D --debug la información que nos aporta el debug nos permitirá identificar errores de parámetros.

-z --bind asocia la combinación de teclas Ctrl+z para incrementar o reducir el TTL de los paquetes.

-Z --unbind desasocia la anterior combinación de teclas.

SELECCIÓN DE PROTOCOLOS

Por defecto Hping2 utiliza el protocolo TCP en las conexiones incluyendo en las cabeceras TCP un tamaño de ventana de 64 y con puerto destino 0, sin especificar ningún otro parámetro.

Modo RAW (-0 --rawiP)

Usando este modo se enviarán las cabeceras IP con datos añadidos mediante el uso de los parámetros --signature y/o --file.

Modo ICMP (-1 --icmp)

Con este modo se enviarán paquetes ICMP echo-request, es factible emplear otros códigos o tipos de icmp mediante las opciones --icmptype e --icmpcode

Modo UDP (-2 --udp)

Con este modo el tráfico que se generará será UDP, los parámetros útiles para este modo son --baseport --destport y --keep

Modo SCAN (-8 --scan)

Permite realizar análisis de puertos, se pueden especificar distintas opciones para los puertos, rangos, excluir determinados puertos, los puertos incluidos
en /etc/services, etc.

Modo LISTEN (-9 --listen)

Este modo ejecutado con --listen información, realiza un volcado de la información contenida en los paquetes en busca de la palabra "información" y la muestra.

PARÁMETROS DE CONFIGURACIÓN ADICIONALES

Los parámetros de configuración también nos permiten especificar las siguientes opciones:

-s --baseport puerto origen base (por defecto es aleatorio)

-p --destport puerto destino, por defecto es 0

-k --keep mantener el puerto origen

-w --win tamaño de ventana (por defecto 64)

-O --tcpoff enviar tamaños de datos modificados (en lugar de el tamaño de la cabecera entre 4, tcphdrlen / 4)

-Q --seqnum muestra únicamente los números de secuencia tcp

-b --badcksum (intentará) enviar paquetes con checksum inválido

-M --setseq se establece un número de secuencia TCP

-L --setack se envía un paquete TCP con el flag de inicio de conexión (ack)

Existen muchos otros parámetros en Hping que permiten la creación de paquetes TCP, UDP e ICMP con todas sus combinaciones.

EMPLEANDO HPING COMO ANALIZADOR DE PUERTOS

Cuando se generan paquetes TCP se pueden especificar los siguientes flags:

-F --fin flag FIN
-S --syn flag SYN
-R --rst flag RST
-P --push flag PUSH
-A --ack flag ACK
-U --urg flag URG
-X --xmas flag X
-Y --ymas flag Y

Si además de estas opciones en TCP, especificamos el puerto y la IP destino, podemos emplear esta herramienta como un scanner de puertos:

```
satelite:~# hping -I eth0 -S www.anysite.com -p 80
HPING www.anysite.com (eth0 X.X.X.X): S set, 40 headers + 0 data bytes
len=46 ip=X.X.X.X ttl=49 DF id=0 sport=80 flags=SA seq=0 win=5840
rtt=94.1 ms
len=46 ip=X.X.X.X ttl=49 DF id=0 sport=80 flags=SA seq=1 win=5840
rtt=93.6 ms
len=46 ip=X.X.X.X ttl=49 DF id=0 sport=80 flags=SA seq=2 win=5840
rtt=96.5 ms
len=46 ip=X.X.X.X ttl=49 DF id=0 sport=80 flags=SA seq=3 win=5840
rtt=96.1 ms
len=46 ip=X.X.X.X ttl=49 DF id=0 sport=80 flags=SA seq=4 win=5840
rtt=101.4 ms
```

Analizamos la respuesta...

Se envía un paquete TCP con longitud 46, con destino la dirección IP X.X.X.X, con ttl (Time To Live) 49, puerto de
destino 80, y con el flag S de inicio de conexión, en la respuesta podemos observar los flags SYN de inicio de conexión y ACK de aceptación de la negociación lo que indica que el puerto esta abierto, la variable seq indica el número de secuencia, win el tamaño de ventana y rtt el Round Trip Time.
Si en la respuesta los flags son RA esto nos indicará que el puerto esta cerrado.

Si queremos que Hping vaya incrementando en uno el puerto a la hora de realizar el análisis, usaremos los caracteres ++
precediendo al número de puerto desde el que queremos iniciar el análisis:

```
satelite:~# hping2 -I eth0 -S 192.168.192.19 -p ++21
HPING 192.168.192.19 (eth0 192.168.192.19): S set, 40 headers + 0 data
bytes
```

```
len=46 ip=192.168.192.19 ttl=255 DF id=0 sport=21 flags=RA seq=0 win=0
rtt=0.5 ms
len=46 ip=192.168.192.19 ttl=64 DF id=0 sport=22 flags=SA seq=1
win=5840 rtt=0.5 ms
len=46 ip=192.168.192.19 ttl=255 DF id=0 sport=23 flags=RA seq=2 win=0
rtt=0.4 ms
len=46 ip=192.168.192.19 ttl=255 DF id=0 sport=24 flags=RA seq=3 win=0
rtt=0.4 ms
len=46 ip=192.168.192.19 ttl=255 DF id=0 sport=25 flags=RA seq=4 win=0
rtt=0.4 ms
```

Podemos ver en el anterior ejemplo que en el puerto 22 sport=22 los flags son SYN y ACK por lo que podemos determinar que el puerto esta abierto, sin embargo, el resto de los puertos del ejemplo, 21, 23, 24 y 25 responden con el flag RA lo que nos indica que se esta recibiendo un RST luego el puerto esta cerrado.
Si lo que queremos es analizar rangos de puertos, como haríamos con un port scanner, con Hping usaremos el parámetro --scan, especificando el rango entre comilla simple '10-15':

```
satelite:~# hping -V --scan '10-15' -S 192.168.192.19
using eth0, addr: 192.168.192.18, MTU: 1500
Scanning 192.168.192.19 (192.168.192.19), port 10-15
6 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+
|port| serv name | flags |ttl| id | win |
+----+-----------+---------+---+-----+-----+
10 : ..R.A... 255 0 0
11 systat : ..R.A... 255 0 0
12 : ..R.A... 255 0 0
13 daytime : ..R.A... 255 0 0
14 : ..R.A... 255 0 0
15 netstat : ..R.A... 255 0 0
All replies received. Done.
Not responding ports:
```

(El parámetro -v indica verbose, lo que muestra más información). Podemos ver que hemos obtenido respuesta de RST, puerto cerrado y que los 6 puertos analizados han respondido.

Un ejemplo con puertos abiertos:

```
satelite:~# hping -V --scan '21-22' -S 192.168.192.19
using eth0, addr: 192.168.192.18, MTU: 1500
Scanning 192.168.192.19 (192.168.192.19), port 21-22
2 ports to scan, use -V to see all the replies
+----+-----------+---------+---+-----+-----+
|port| serv name | flags |ttl| id | win |
+----+-----------+---------+---+-----+-----+
21 ftp : ..R.A... 255 0 0
22 ssh : .S..A... 64 0 5840
All replies received. Done.
Not responding ports:
```

En el resultado podemos observar que el puerto 21 respondió con flaq RA (puerto cerrado) y el 22 con los flags SA (puerto abierto).

IDENTIFICANDO REGLAS EN UN FIREWALL.

Hping se puede utilizar de la misma forma que traceroute o Firewalk usando paquetes ICMP, TCP o UDP.

Emplearemos los parámetros:

-t establece el valor inicial del ttl en la cabecera IP.
-z establece que la combinación de teclas "control+z" modificará el TTL, lo que quiere decir que cada vez que se pulse "control+z" el TTL se incrementa.

Para identificar el número de saltos desde un host a otro host, con traceroute sería:

satelite:~# traceroute 192.168.207.26
traceroute to 192.168.207.26 (192.168.207.26), 30 hops max, 38 byte packets
1 192.168.13.60 (192.168.13.60) 0.260 ms 0.169 ms 0.160 ms
2 192.168.207.26 (192.168.207.26) 0.531 ms 0.322 ms 0.315 ms

Ahora mediante Hping vamos a identificar si el puerto 80 esta abierto, además de identificar el número de saltos entre hosts:

```
satelite:~# hping -I eth0 -z -t 1 -S 192.168.207.26 -p 80
HPING 192.168.207.26 (eth0 192.168.207.26): S set, 40 headers + 0 data
bytes
TTL 0 during transit from ip=192.168.13.60 name=UNKNOWN
TTL 0 during transit from ip=192.168.13.60 name=UNKNOWN
TTL 0 during transit from ip=192.168.13.60 name=UNKNOWN 2:
len=46 ip=192.168.207.26 ttl=127 id=16554 sport=80 flags=SA seq=3
win=16384 rtt=0.7 ms
len=46 ip=192.168.207.26 ttl=127 id=16558 sport=80 flags=SA seq=4
win=16384 rtt=0.4 ms
len=46 ip=192.168.207.26 ttl=127 id=16562 sport=80 flags=SA seq=5
win=16384 rtt=0.4 ms
len=46 ip=192.168.207.26 ttl=127 id=16570 sport=80 flags=SA seq=6
win=16384 rtt=0.4 ms
```

--- 192.168.207.26 hping statistic ---
7 packets tramitted, 7 packets received, 0% packet loss
round-trip min/avg/max = 0.4/0.5/0.7 ms

Podemos observar que con ttl 1, no se identifica el host ni si el servicio esta abierto o no, por lo que al pulsar "control+z" aumentamos el TTL en uno y ya si podemos ver en los flags el código "S" que identifica que el servicio esta abierto y el número de saltos desde el host origen al host destino.

Hping incorpora un modo -T o --traceroute con esta opción el ttl se va auto incrementando en uno.

Referencias: man hping, hping.org, Manual de Hping by radarhack