CÔNG CỤ HPING3

Giới thiệu chung:

Hping là một trình phân tích gói tin TCP / IP định hướng dòng lệnh. Giao diện được lấy cảm hứng từ lệnh ping (8) unix. Nó hỗ trợ các giao thức TCP, UDP, ICMP và RAW-IP, có chế độ theo dõi, khả năng gửi tệp giữa một kênh được phủ sóng và nhiều tính năng khác. Trong khi hping chủ yếu được sử dụng như một công cụ bảo mật trước đây, nó có thể được sử dụng theo nhiều cách bởi những người không quan tâm đến bảo mật để kiểm tra mạng và máy chủ. Một tập hợp con của những thứ bạn có thể thực hiện bằng cách sử dụng hping:

- Kiểm tra tường lửa
- Quét cổng nâng cao
- Kiểm tra mạng, sử dụng các giao thức khác nhau, TOS, phân mảnh
- Phát hiện MTU đường dẫn thủ công
- Tiến trình theo dõi nâng cao, theo tất cả các giao thức được hỗ trợ
- Lấy dấu vân tay hệ điều hành từ xa
- Đo thời gian hoạt động từ xa
- Kiểm tra ngăn xếp TCP / IP

Hping cũng có thể hữu ích cho người đang học TCP / IP.

Hping hoạt động trên các hệ thống sau: Linux, FreeBSD, NetBSD, OpenBSD, Solaris, MacOs X, Windows.

Các lệnh cơ bản:

Hiển thị danh sách lệnh

➔**hping3 --help**

Kiểm tra ping cơ bản

➔**hping3 host -1 -c 4**

Quét cổng máy chủ mục tiêu

➔**hping3 host -8 19-80,443 -S -V**

Kiểm tra kết nối, giao tiếp mạng bằng TCP SYN scan

➔**hping3 host -S -p [Port Number] -c 4**

Tạo nhiều request để kiểm tra tấn công DoS

➔**hping3 host -S -p [Port Number] –flood**

Tấn công DdoS

➔**hping3 host -S -p [Port Number] –flood --rand-source**

Tấn công giả mạo IP

➔**hping3 host -a FakeIP -S -p [Port Number] –flood**

Mô phỏng các kiểu tấn công từ chối dịch vụ từ layer 4 đến layer 7:

Thực hiện mô phỏng tấn công Spoofed SYN Flood.

➔**hping3 host -p [Port Number] -a FakeIP -S --flood**

Thực hiện mô phỏng tấn công ACK Number Flood.

➔**hping3 host -p [Port Number] -A --flood**

Thực hiện mô phỏng tấn công Invalid UDP/TCP Checksum.

➔**hping3 host -p [Port Number] -b –flood**

Thực hiện mô phỏng tấn công TCP SYN Flood.

➔**hping3 host -p [Port Number] -S --flood**

Thực hiện mô phỏng tấn công ICMP Flood.

➔**hping3 host -p [Port Number] -1 --flood**

Thực hiện mô phỏng tấn công UDP Flood.

➔**hping3 host -p [Port Number] -2 --flood**

Cheatography

Hping3 version 1.4 Cheat Sheet

by ramkumaplays via cheatography.com/60600/cs/15755/

Base 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)
	--faster	alias for -i u1000 (100 packets for second)
	--flood	sent packets as fast as possible. Don't show replies.
-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
	--beep	beep for every matching packet received

Mode

default mode		TCP
-0	--rawip	RAW IP mode
-1	--icmp	ICMP mode
-2	--udp	UDP mode
-8	--scan	SCAN mode

Mode (cont)

		Example: hping --scan 1-30,70-90 -S www.target.host
-9	--listen	listen mode

IP

-a	--spoof	spoof source addess
	--rand-dest	random destionation address mode
	--rand-source	random source address mode
-t	--ttl	ttl (default 64)
-N	--id	id (default random)
-W	--winid	use win* id byte ordering
-r	--rel	relativize id field (to estimate host traffic)
-f	--frag	split packets in more frag
-x	--morefrag	set more fragments flag
-y	--dontfrag	set don't fragment flag
-g	--fragoff	set the fragment offset
-m	--mtu	set virtual mtu, implies --frag if packet size > mtu
-o	--tos	type of service (default 0x00), try --tos help
-G	--rroute	includes RECORD_ROUTE option and display the route buffer
	--lsrr	loose source routing and record route
	--ssrr	strict source routing and record route
-H	--ipproto	set the IP protocol field, only in RAW IP mode

ICMP

-C	--icmptype	icmp type (default echo request)
-K	--icmpcode	icmp code (default 0)
	--force-icmp	send all icmp types (default send only supported types)
	--icmp-gw	set gateway address for ICMP redirect (default 0.0.0.0)
	--icmp-ts	Alias for --icmp --icmptype 13 (ICMP timestamp)
	--icmp-addr	Alias for --icmp --icmptype 17 (ICMP address subnet mask)
	--icmp-help	display help for others icmp options

UDP/TCP

-s --baseport	base source port (default random)

By **ramkumaplays**

cheatography.com/ramkumaplays/

Not published yet.

Last updated 10th May, 2018.