Hping

Usage:
`# hping [Options] [TargetIPaddr]`

Send packets to `[TargetIPaddr]` as specified by `[Options]`

Options:
`--count [N]`: Number of packets to send
`--beep`: Beep when a packet is *received*
`--file [FileName]`: Send contents of file as a payload, must be used with `--data`
`--data [N]`: Length of payload to send in bytes, if no `--file` is specified, payload is all X's
`--interface [Interface]`: Use specified interface name

Speed Options:
`--fast`: Ten packets per second
`--faster`: One million packets per second
`--flood`: Send packets as fast as possible
`--interval [Seconds]/u[Microseconds]`: Interval in seconds/microseconds between sent packets

Modes:
Default Mode: TCP
`--rawip`: Send raw IP packets, no TCP/UDP
`--icmp`: Send ICMP packets
`--udp`: Send UDP packets

Source Selection:
`--spoof [Hostname]`: Send all packets from specified source address

Hping (continued)

Target Address Selection:
Single Target:
`# hping [TargetIPaddr]`
Send packets to `[TargetIPaddr]`

Random Multiple Targets:
`# hping --rand-dest 10.10.10.x`
`--interface eth0`
Send packets to 10.10.10.x with x being randomly chosen for each packet between 1 and 255
`--interface` must be used with `--rand-dest`

Dest Port Selection:
Single Port:
`--destport [Port]`
`[Port]`: Send packets to this port
`+[Port]`: Increment port number by one for each *response received*
`++[Port]`: Increment port number by one for each packet *sent*
Multiple/Range of Ports:
`--scan [PortRange/List]`: Scan this target range or list of ports (x-y,z,known). The known keyword tells Hping to send packets to the list of ports in /etc/services

Source Port Selection:
Default: Use source port > 1024 assigned by OS, incrementing for each packet sent
`--baseport [Port]`: Start with this source port, incrementing for each packet sent
`--keep`: Use only a single source port for all packets

SANS INSTITUTE

Purpose

The purpose of this cheat sheet is to describe some common options for a variety of security assessment and pen test tools covered in SANS 504 and 560.

Tools Described on This Sheet

Metasploit 3.X
The Metasploit Framework is a development platform for developing and using security tools and exploits.

Metasploit Meterpreter
The Meterpreter is a payload within the Metasploit Framework which provides control over an exploited target system, running as a DLL loaded inside of any process on a target machine.

Fgdump
FGDump is a tool for locally or remotely dumping runtime Windows password hashes.

Hping
Hping is a command-line TCP/IP packet assembler/analyzer