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

Misc Tools Cheat Sheet

By Ed Skoudis

POCKET REFERENCE GUIDE

http://www.sans.org

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

Metasploit Console (msfconsole)

Search for module:
```
msf > search [regex]
```

Specify an Exploit to use:
```
msf > use exploit/[ExploitPath]
```

Specify a Payload to use:
```
msf > set PAYLOAD [PayloadPath]
```

Show options for the current modules:
```
msf > show options
```

Set Options:
```
msf > set [Option] [Value]
```

Start Exploit: `msf > exploit`

Metasploit Meterpreter

Base Commands:

`? / help`: Display a summary of commands
`exit / quit`: Exit the Meterpreter session
`sysinfo`: Show the system name and OS type
`shutdown / reboot`: Self-explanatory

File System Commands:

`cd`: Change directory
`lcd`: Change directory on local (attacker's) machine
`pwd / getwd`: Display current working directory
`ls`: Show contents of a directory
`cat`: Display contents of a file on screen
`download /upload` : Move files to/from target machine
`mkdir / rmdir`: Make / Remove directory
`edit`: Open a file in an editor, default is vi

Metasploit Meterpreter (contd)

Process Commands:

`getpid`: Display the process ID that Meterpreter is running inside
`getuid`: Display the user ID that Meterpreter is running with
`ps`: Display process list
`kill`: Terminate a process given its process ID
`execute`: Run a given program with the privileges of the process the Meterpreter is loaded in
`migrate`: Jump to a given destination process ID

- Target process must have same or lesser privileges
- Target process may be a more stable process
- When inside a process, can access any files that process has a lock on

Network Commands:

`ipconfig`: Show network interface information
`portfwd`: Forward packets through TCP session
`route`: Manage/view the system's routing table

Misc Commands:

`idletime`: Display the duration that the GUI of the target machine has been idle
`uictl [enable/disable] [keyboard/mouse]`: Enable/Disable either the mouse or keyboard of the target machine

Additional Modules:

`use [module]`: Load the specified module
Example:
`use priv`: Load the Priv module
`hashdump`: Dump the hashes from the box
`timestomp`: Alter NTFS file timestamps

FGDump

Usage:
```
C:\> fgdump [Options] -h [TargetIPaddr]
-u [Username] -p [Password]
```
Dump password hashes from **`[TargetIPaddr]`** with Admin credentials: **`[Username]/[Password]`**

Options:

`-c`: Skip cache dump
`-w`: Skip password dump
`-s`: Perform protected storage dump
`-r`: Ignore existing pw/cachedump files and don't skip hosts
`-v`: Verbose output
`-l [FileName]`: Keep logs in **`[FileName]`**

Examples:

Dump info from local machine using current user:
```
C:\> fgdump
```

Dump from a local machine using a different user:
```
C:\> fgdump -h 127.0.0.1 -u [Username]
```

Dump from a remote machine using a specified user:
```
C:\> fgdump -h [TargetIPaddr] -u
[Username] -p [Password]
```

Dump from a remote machine without cachedump:
```
C:\> fgdump -h [TargetIPaddr] -u
[Username] -c
```