这意味着该系统可能正在运行基于 TLS 的 Web 服务器，那么可以让程序只扫描 443 端口。不扫描无关的端口将为你节省大量的时间。

示例 3-19：使用 masscan 进行高速扫描

```
root@rosebud:~# masscan -sS --ports 0-1500 192.168.86.0/24

Starting masscan 1.0.3 (http://bit.ly/14GZzcT) at 2017-12-31 20:27:57 GMT
 -- forced options: -sS -Pn -n --randomize-hosts -v --send-eth
Initiating SYN Stealth Scan
Scanning 256 hosts [1501 ports/host]
Discovered open port 445/tcp on 192.168.86.170
Discovered open port 22/tcp on 192.168.86.30
Discovered open port 1410/tcp on 192.168.86.37
Discovered open port 512/tcp on 192.168.86.239
Discovered open port 445/tcp on 192.168.86.239
Discovered open port 22/tcp on 192.168.86.46
Discovered open port 143/tcp on 192.168.86.238
Discovered open port 1410/tcp on 192.168.86.36
Discovered open port 53/tcp on 192.168.86.1
Discovered open port 1400/tcp on 192.168.86.36
Discovered open port 80/tcp on 192.168.86.38
Discovered open port 80/tcp on 192.168.86.1
```

你可以使用多功能实用程序进行端口扫描，同时也可以控制发送消息之间的时间间隔。虽然 *masscan* 使用异步方法来加快扫描速度，但是 *hping3* 可以指定数据包之间的间隔。这并没有使它能够进行真正的高速扫描，但是 *hping3* 确实包含可以执行其他任务的功能。*hping3* 支持通过命令行开关制作数据包。将 *hping3* 用作扫描器的挑战在于，它实际上是一个过度活跃的 ping 程序，而不是试图重新创建 *nmap* 和其他扫描程序提供的功能。

不过，如果要对单个主机执行扫描并探测其特征，*hping3* 是一款出色的工具。示例 3-20 是针对 10 个端口的 SYN 扫描。-S 参数是告知 *hping3* 设置一个 SYN 标记。我们使用 *-p* 选项来指定要扫描的端口。通过将 ++ 符号添加到 *-p* 参数中，这是告知 *hping3* 希望它自动增加端口号。我们可以使用 *-c* 参数来控制端口号的计数。在这种情况下，*hping3* 将扫描 10 个端口并停止。最后，我们可以使用 *-s* 选项和一个端口号来设置源端口。对于此扫描，源端口并不重要，但在某些情况下这是必要的。