SCTPscan - Copyright (C) 2002 - 2009 Philippe Langlois.

SCTPscan comes with ABSOLUTELY NO WARRANTY; for details read the LICENSE or COPYING file.

使用方法： sctpscan [options]

选项：

-p, --port <port> (default: 10000)

指定远程端口号

-P, --loc\_port <port> (default: 10000)

指定本地端口号

-l, --loc\_host <loc\_host> (default: 127.0.0.1)

loc\_host指定地方（绑定）和可选的本地端口号的SCTP流主机

-r, --rem\_host <rem\_host> (default: 127.0.0.2)

rem\_host指定远程（SendTo）和可选的远程端口号的SCTP流地址

-s --scan -r aaa[.bbb[.ccc]]

扫描网络内的所有机器

-m --map

地图上所有传输端口从0到65535（端口）

-F --Frequent

Portscans the frequently used SCTP ports

Frequent SCTP ports: 1, 7, 9, 20, 21, 22, 80, 100, 128, 179, 260, 250, 443, 1167, 1812, 2097, 2000, 2001, 2010, 2011, 2020, 2021, 2100, 2110, 2120, 2225, 2427, 2477, 2577, 2904, 2905, 2906, 2907, 2908, 2909, 2944, 2945, 3000, 3097, 3565, 3740, 3863, 3864, 3868, 4000, 4739, 4740, 5000, 5001, 5060, 5061, 5090, 5091, 5672, 5675, 6000, 6100, 6110, 6120, 6130, 6140, 6150, 6160, 6170, 6180, 6190, 6529, 6700, 6701, 6702, 6789, 6790, 7000, 7001, 7102, 7103, 7105, 7551, 7626, 7701, 7800, 8000, 8001, 8471, 8787, 9006, 9084, 9899, 9911, 9900, 9901, 9902, 10000, 10001, 11146, 11997, 11998, 11999, 12205, 12235, 13000, 13001, 14000, 14001, 20049, 29118, 29168, 30000, 32905, 32931, 32768

-a --autoportscan

端口扫描，自动与SCTP了解TCP/IP协议栈的任何主机

-i --linein

接收IP扫描输入

-f --fuzz

模糊测试所有的远程协议栈

-B --bothpackets

发送数据包的初始化块一个，和其他shutdown\_ack

-b --both\_checksum

发送校验和：新的和旧的驱动Adler32 CRC32

-C --crc32

随着新的CRC32计算校验和

-A --adler32

与旧Adler32计算校验和

-Z --zombie

不合作的SCTP协作平台。没有报告。

-d --dummyserver

从端口10000上的一个虚拟的SCTP服务器。然后，您可以尝试扫描它从另一台机器。

-E --exec <script\_name>

执行<< script\_name >每次开放的SCTP端口发现。执行参数：< script\_name > host\_ip sctp\_port

-t --tcpbridge <listen TCP port>

桥连接的TCP端口> <听远程指定SCTP端口。

-S --streams <number of streams>

尝试建立SCTP关联与指定<流数>远程指定SCTP的目的地。

扫描端口9999上的192.168.1.24

./sctpscan -l 192.168.1.2 -r 192.168.1.24 -p 9999

对于SCTP在172.17.8可用扫描。\*和端口扫描与SCTP栈任何主机

./sctpscan -s -l 172.22.1.96 -r 172.17.8

常用的端口扫描172.17.8 \*。

./sctpscan -s -F -l 172.22.1.96 -r 172.17.8

扫描端口的所有类网络频繁

./sctpscan -s -F -r 172.22 -l `ifconfig eth0 | grep 'inet addr:' | cut -d: -f2 | cut -d ' ' -f 1 `

简单验证端到端在本地机上：

./sctpscan -d &

./sctpscan -s -l 192.168.1.24 -r 192.168.1 -p 10000

这个工具不工作在大多数NAT。这意味着大多数的路由器/防火墙不知道如何NAT SCTP包。你\_need\_使用具有公网IP地址的计算机这个工具（即non-rfc1918）