

Atk6-thcping6

Atk6-thcping源自于github.com/vanhauser-thc/thc-ipv6项目之一，主要用于自定义手工制作的ping6包。

——by van Hauser

一，帮助手册

atk6-thcping6 v3.6 (c) 2019 by van Hauser / THC vh@thc.org www.github.com/vanhauser-thc/thc-ipv6

van Hauser/THC vh@THC.org www.github.com/vanhauser-thc/thc-ipv6, 2019年3月6日 (c)
Syntax: atk6-thcping6 [-EafqxO] [-e ethertype] [-H t:l:v] [-D t:l:v] [-F dst] [-e ethertype] [-L length] [-N nextheader] [-V version] [-t ttl] [-c class] [-l label] [-d size] [-S port] [-U port] [-T type] [-C code] interface src6 dst6 [srcmac [dstmac [data]]]

语法：atk6-thcping6[-EafqxO][-e ethertype][-H t:l:v][-D t:l:v][-F dst][-e ethertype][-L length][-N下一个命令][-v版本][-t ttl][-c类][-l标签][-d大小][-S端口12444；-U端口[-t类型-c]src6 dst6接口[srcmac[dst[数据]]]

Options:

选项：

-T number ICMPv6 type to send (default: 128 = ping)

-要发送的T编号ICMPv6类型（默认值：128=ping）

-C number ICMPv6 code to send (default: 0)

-要发送的C号ICMPv6代码（默认值：0）

-S port use a TCP SYN packet on the defined port instead of ping

S端口在定义的端口上使用TCP SYN数据包，而不是ping

-U port use a UDP packet on the defined port instead of ping

-U端口在定义的端口上使用UDP数据包，而不是ping

-n count how often to send the packet (default: 1)

-n计算发送数据包的频率（默认值：1）

-h show more command line options (help!)

-h显示更多命令行选项（帮助！）

You can put an "x" into src6, srcmac and dstmac for an automatic value.
可以在src6、srcmac和dstmac中输入“x”作为自动值。

Craft a ICMPv6/TCP/UDP packet with special IPv6 or EH header options.
使用特殊的IPv6或EH报头选项创建ICMPv6/TCP/UDP包。

Returns -1 on error or no reply, 0 on normal reply or 1 on error reply.
错误或无应答时返回-1，正常应答时返回0，错误应答时返回1。

一，参数介绍

-x

泛洪模式（不检查回复）

-w 时间

数据包之间的等待时间，单位为“ms”，默认等待时间为1000

-a

添加带有路由器报警选项的逐跳报头

-q

添加带有快速启动选项的逐跳报头

-O

发送TCP数据，快速打开cookie请求选项（需要配合“-S”参数一起使用）

-E

作为以太网帧 IPV4发送

-e 帧

发送指定的以太网帧（16进制）

-H t:l:v

添加一个具有特殊内容的逐跳标头

-D t:k:v

添加一个特殊内容的目标头

-F iP(ipv6)

ipv6 最终目的的源路由

-f

添加一次性分段标题

-L 长度

设置假有效的载荷长度（0~65535）

-N 报头

设置一个假的标头（0~255）

-V 版本号

设置一个IP版本号（0~15）

-t 生存时间

设置一个数据包的生存时间

-c 类

在（0~4095）中指定一个类

-l 标签

在（0~1048575）中指定一个标签

-d 大小

自定义ping缓存数据区的大小

port**-S 端口**

在定义的端口撒谎那个使用一个TCP同步数据包，而不是Ping

-U 端口

在定义的端口上使用UDP包，而不是Ping

-n 频率

计算机发送数据包的频率（默认值为1）

t:l:v 语法:type:length:value，以十六进制表示，例如（1:2:0eab）

您也可以在src6,srcmac和dstmac中输入 "X"作为自动值

错误或无法回复时返回“-1”，正常回复返回时回“0”，错误回复时返回“0”

三，命令实例

```
atk6-thcping6 -E -e 7 -H t:l:v -F fe80::20c:29ff:feb4:7ffc/64 -e 7 -L 7 -N 7 -V 7 -t 7 -c 7 -l 7 -d 7 -S 7 -T 7 -C 7 vm
```

```
net8 fe80::485d:7e23:566:b84d fe80::20c:29ff:feb4:7ffc/64 1c:1b:b5:c0:fb:07 00:0c:29:b4:7f:fc x
```

设置为以太网帧IPV4进行发送，以太网帧为7，设置一个特殊逐跳头为t:l:v，目标为fe80::20c:29ff:feb4:7ffc/64，设置数据包帧为7,设置数据包长度为7，设置设报头为7，设置版本号为7，设置生存时间为7，设置累为7,设置标签为7，设置大小为7设置端口为7,设置网卡为vmnet8，设置源IPV6地址为“fe80::485d:7e23:566:b84d”，设置目标IP地址为“fe80::20c:29ff:feb4:7ffc/64”，设置源MAC地址为“1c:1b:b5:c0:fb:07”，设置目标MAC地址为“00:0c:29:b4:7f:fc”为自动值。对数据包进行自定义发送

```
Address: IntelCor_c0:fb:07 (1c:1b:b5:c0:fb:07) #atk6-thcping6 -E -e 7 -H t:l:v -F fe80::20c:29ff:feb4:7ffc/64 -e 7 -L 7 -N 7 -V 7 -t 7 -c 7 -l 7 -d 7 -S 7 -T 7 -C 7 vm
... ..0. .... = LG bit: Globally unique address:net8 fe80::485d:7e23:566:b84d fe80::20c:29ff:feb4:7ffc/64 1c:1b:b5:c0:fb:07 00:0c:29:b4:7f:fc x
... ..0. .... = IG bit: Individual address (unWarning: the data option is ignored if the -d option is supplied
Length: 7 0000.0000 tcp-syn packet sent to fe80::20c:29ff:feb4:7ffc
No packet received, terminating.
```