netsniff-ng 0.6.1, the packet sniffing beast

http://www.netsniff-ng.org

格式： netsniff-ng [选项] [筛选器]

Options:

-i|-d|--dev|--in <dev|pcap|-> 输入源的意思，PCAP或pcap stdin

-o|--out <dev|pcap|dir|cfg|-> 输出下沉的意思，PCAP，目录，trafgen，或stdout

-C|--fanout-group <id> 加入包扇出组

-K|--fanout-type <type> 应用学科：哈希|扇出LB | CPU | RND |辊| QM

-L|--fanout-opts <opts> 附加选项：磁盘碎片整理|辊扇出

-f|--filter <bpf-file|-|expr> 使用Bipolar Electrocoagulation文件/ stdin或tcpdump的样子带通滤波器

-t|--type <type> 过滤器：主机|广播|组播|别人|外向

-F|--interval <size|time> 把区间如果O是一个导演：<数> KIB / MIB /钩/秒/秒/分钟/小时

-R|--rfraw 捕获或注入原始的802.11帧

-n|--num <0|uint> 数据包直到退出（定义：0）

-P|--prefix <name> 存储在目录PCAPs前缀

-T|--magic <pcap-magic> PCAP幻数/ PCAP格式存储，看到D

-w|--cooked 使用“cooked ”头，而不是链路头

-D|--dump-pcap-types 转储pcap类型和神奇的数字和退出

-B|--dump-bpf 把生成的滤波器组件

-r|--rand 随机分组的转发顺序（Dev ->开发）

-M|--no-promisc 对于意思不混杂模式

-A|--no-sock-mem 不调整核心插槽内存

-N|--no-hwtimestamp 禁用硬件时间戳

-m|--mmap Mmap（2）pcap文件I/O，例如重放PCAPs

-G|--sg 分散/聚集pcap文件I/O

-c|--clrw 使用慢读（2）/写（2）I / O

-S|--ring-size <size> 指定环大小：<数> KIB / MIB /钩

-k|--kernel-pull <uint> 在我们从用户间隔核拉（定义：10us）

-J|--jumbo-support 支持回放/ FWD 64kb超级巨型帧（定义：2048b）

-b|--bind-cpu <cpu> 绑定到特定的处理器

-u|--user <userid> 放弃特权和更改用户名

-g|--group <groupid> 放弃特权和改变GroupID

-H|--prio-high 使这个高优先级的过程

-Q|--notouch-irq 不要触摸CPU亲和力网卡IRQ

-s|--silent 不打印捕获的数据包

-q|--less 打印更详细的数据包信息

-X|--hex 在十六进制格式的打印数据包数据

-l|--ascii 打印可读的数据包数据

-U|--update 更多的数据库更新

-V|--verbose 更详细的

-v|--version 显示版本和退出

-h|--help Guess what?!

实例:

netsniff-ng --in eth0 --out dump.pcap -s -T 0xa1b2c3d4 --b 0 tcp or udp

netsniff-ng --in wlan0 --rfraw --out dump.pcap --silent --bind-cpu 0

netsniff-ng --in dump.pcap --mmap --out eth0 -k1000 --silent --bind-cpu 0

netsniff-ng --in dump.pcap --out dump.cfg --silent --bind-cpu 0

netsniff-ng --in dump.pcap --out dump2.pcap --silent tcp

netsniff-ng --in eth0 --out eth1 --silent --bind-cpu 0 -J --type host

netsniff-ng --in eth1 --out /opt/probe/ -s -m --interval 100MiB -b 0

netsniff-ng --in vlan0 --out dump.pcap -c -u `id -u bob` -g `id -g bob`

netsniff-ng --in any --filter http.bpf --jumbo-support --ascii -V

注意:

对于引入位错误，随机变化的延迟和更多而重放PCAPs，利用TC（8）与学科（如考研英语）。

Please report bugs to <netsniff-ng@googlegroups.com>

Copyright (C) 2009-2013 Daniel Borkmann <dborkma@tik.ee.ethz.ch>

Copyright (C) 2009-2012 Emmanuel Roullit <emmanuel.roullit@gmail.com>

Copyright (C) 2012 Markus Amend <markus@netsniff-ng.org>

Swiss federal institute of technology (ETH Zurich)

License: GNU GPL version 2.0

这是免费软件：你可以自由地改变和重新分配它。没有任何保证，在法律允许的范围内。