



**Universidad Tecnológica**  
*de San Luis Río Colorado*



## **UNIVERSIDAD TECNOLÓGICA DE SAN LUIS RIO COLORADO**

**NETSNIFF-NG**

**MTR. CESAR EDUARDO ROMERO HERNANDEZ**

**ALUMNO: VICTOR MANUEL GALVAN COVARRUBIAS**

**ING. EN DESARROLLO Y GESTIÓN DE SOFTWARE**

San Luis Río Colorado, Sonora

Feb, 2022





**Netsniff-ng** es una herramienta que, aunque tiene características interesantes y es potente, es poco conocida. Se trata de un sniffer (buscador) diseñado especialmente para sistemas Linux, muy similar a herramientas como TCPDump o TShark, pero con ventajas adicionales.

**El rendimiento**, el cual es mucho más óptimo que otros sniffers existentes, ya que los paquetes manejados por Netsniff-ng no son copiados entre el espacio del kernel y el espacio del usuario.

Para el correcto funcionamiento de **netsniff-ng** también se recomienda utilizar versiones recientes del kernel de Linux ya que implementan el concepto de “**rings**” del tipo RX y TX, los cuales permiten un control mucho más eficiente de los buffers utilizados para la recepción y transmisión de paquetes de datos.

El tamaño de cada uno de estos **rings** puede variar dependiendo de las limitaciones físicas de la interfaz de red y típicamente se calcula en base al ancho de banda soportado por la interfaz de red.

La herramienta permite la **captura de paquetes desde un dispositivo o un fichero** de capturas y dicha información también puede **ser inyectada/redireccionada a un dispositivo de red o un fichero** de capturas.

También soporta filtros especiales sobre el tipo de tráfico a capturar aplicando el interruptor “-t”. Los posibles valores que puede asumir “-t” son los siguientes:

- **broadcast**: Permite filtrar solamente el tráfico broadcast.
- **multicast**: Permite filtrar solamente el tráfico multicast.
- **host**: Permite filtrar solamente los paquetes cuyo destino es la máquina desde donde se ejecuta la herramienta.
- **others**: Permite filtrar los paquetes cuyo origen o destino es distinto de la máquina desde donde se ejecuta la herramienta.

- **outgoing:** Permite filtrar solamente los paquetes cuyo origen es la máquina desde donde se ejecuta la herramienta.

Por otro lado, tal como mencionaba anteriormente, también es posible la **reinyección de tráfico** utilizando esta herramienta, para ello se puede utilizar un fichero PCAP o una interfaz de red que contendrá/capturará los paquetes de datos que serán reinyectados en una interfaz de red determinada. Para ello, se debe utilizar también el interruptor “-mmap”.

```

$ netstiff-ng -h
netstiff-ng 0.0.0, the packet sniffing beast
http://www.netstiff-ng.org

Usage: netstiff-ng [options] [filter-expression]
Options:
  -i|-d|-dev|-in|-dev|-pcap|-> Input source as netdev, pcap or pcap stdin
  -o|-out|-dev|-pcap|-dir|-f|-> Output sink as netdev, pcap, directory, traf
  -g|-n|-s|-t|-t|-t Join packet famout group
  -x|-x|-x|-x|-x|-x Apply famout discipline: hashlib|cpu|rdn|rol
  -l|-l|-l|-l|-l|-l Additional famout options: defrag|roll
  -f|-f|-f|-f|-f|-f Use BPF filter from bpfc file/stdin or tcpd
  -e|-e|-e|-e|-e|-e Filter for: host|broadcast|multicast|others|
  -t|-t|-t|-t|-t|-t Filter for: host|broadcast|multicast|others|
  outgoing
  -i|-interval|-size|-time Dump interval if -o is a dir: count|KB|MB|G
  |B/s|sec/min|hrs
  -n|-n|-n|-n|-n|-n Capture or inject raw 802.11 frames
  -m|-m|-m|-m|-m|-m Number of packets until exit (def: 0)
  -p|-p|-p|-p|-p|-p Prefix for pcaps stored in directory
  -q|-q|-q|-q|-q|-q Limit the number of pcaps to N (file names u
  se numbers 0 to N-1)
  -T|-T|-T|-T|-T|-T Pcap magic number/pcap format to store, see
  -B|-B|-B|-B|-B|-B Use Linux "cooked" header instead of link he
  ader
  -D|-D|-D|-D|-D|-D Dump pcap types and magic numbers and quit
  -B|-B|-B|-B|-B|-B Dump generated BPF assembly
  -r|-r|-r|-r|-r|-r Randomize packet forwarding order (dev+dev)
  -M|-M|-M|-M|-M|-M No promiscuous mode for netdev
  -A|-A|-A|-A|-A|-A Don't tune core socket memory
  -N|-N|-N|-N|-N|-N Disable hardware time stamping
  -m|-m|-m|-m|-m|-m Mmap(2) pcap file I/O, e.g. for replaying pc
  aps
  -G|-G|-G|-G|-G|-G Scatter/gather pcap file I/O
  -C|-C|-C|-C|-C|-C Use slower read(2)/write(2) I/O
  -S|-S|-S|-S|-S|-S Specify ring size for: count|KB|MB|GB
  -K|-K|-K|-K|-K|-K Kernel pull from user interval in us (def: 1
  000)
  -J|-J|-J|-J|-J|-J Support replay/fwd 64KB Super Jumbo Frames (
  def: 2048)
  -b|-b|-b|-b|-b|-b Bind to specific CPU
  -u|-u|-u|-u|-u|-u Drop privileges and change to userid
  -g|-g|-g|-g|-g|-g Drop privileges and change to groupid
  -P|-P|-P|-P|-P|-P Make this high priority process
  -Q|-Q|-Q|-Q|-Q|-Q Do not touch IRQ CPU affinity of NIC
  -s|-s|-s|-s|-s|-s Do not print captured packets
  -q|-q|-q|-q|-q|-q Print less-verbose packet information
  -X|-X|-X|-X|-X|-X Print packet data in hex format
  -L|-L|-L|-L|-L|-L Print human-readable packet data
  -U|-U|-U|-U|-U|-U Update GeoIP databases
  -V|-V|-V|-V|-V|-V Be more verbose
  -v|-v|-v|-v|-v|-v Show version and exit
  -h|-h|-h|-h|-h|-h Guess what?!

Examples:
netstiff-ng -i eth0 -out dump.pcap -s -f 0-a1b2c3d4 -bind-cpu 0 tcp or
udp
netstiff-ng -i wlan0 -ffraw -out dump.pcap -silent -bind-cpu 0
netstiff-ng -i dump.pcap -mmap -out eth0 -k1000 -silent -bind-cpu 0
netstiff-ng -i dump.pcap -out dump.cfg -silent -bind-cpu 0
netstiff-ng -i dump.pcap -out dump2.pcap -silent tcp
netstiff-ng -i eth0 -out eth1 -silent -bind-cpu 0 -j -type host
netstiff-ng -i eth1 -out /opt/probe/ -s -m -interval 100000 -b 0
netstiff-ng -i wlan0 -out dump.pcap -c -u id -u bob -g id -g bob
netstiff-ng -i any -filter http.bpf -jumbo-support -ascii -f

Notes:
For introducing bit errors, delays with random variation and more
while replaying pcaps, make use of tc(8) with its disciplines (e.g. netem).

Please report bugs at https://github.com/netstiff-ng/netstiff-ng/issues
Copyright (C) 2009-2013 Daniel Borkmann <dborkmann@kernel.org>
Copyright (C) 2009-2013 Emmanuel Roulet <emmanuel.roulet@gmail.com>
Copyright (C) 2012 Markus Amend <markus@netstiff-ng.org>
Swiss Federal Institute of Technology (ETH Zurich)
License: GNU GPL version 2.0
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.
[hal@kali]~$

```