



Actividad #: 4

Autor/es: Ariana González Pinto

Carrera: Tecnología Superior en Desarrollo de Software

Docente: Ing.: Edison Espinoza

-Fecha:10/11/2024

Explicación del comando

netsniff-ng: Es la herramienta principal que se usa para capturar, analizar y reproducir tráfico de red en tiempo real o en archivos de captura.

-h: Muestra el menú de ayuda o la lista de opciones disponibles para utilizar con netsniff-ng.

Al ejecutar netsniff-ng -h, saldrá un listado de las opciones y parámetros que se usa con netsniff-ng. Esta información incluye opciones para:

```
root@kali: /
File Actions Edit View Help
root@kali)~[/]
# netsniff-ng -h
netsniff-ng 0.6.8, the packet sniffing beast
http://www.netsniff-ng.org

Usage: netsniff-ng [options] [filter-expression]
Options:
-i|-d|--dev|-in <dev|pcap|> Input source as netdev, pcap or pcap stdin
-o|--out <dev|pcap|dir|cfg|> Output sink as netdev, pcap, directory, trafigen,
or stdout
-C|--fanout-group <id> Join packet fanout group
-K|--fanout-type <type> Apply fanout discipline: hash|lb|cpu|rnd|roll|qm
-L|--fanout-opts <opts> Additional fanout options: defrag|roll
-f|--filter <bpf-file|expr> Use BPF filter from bpf file/stdin or tcpdump-like
expression
-t|--type <type> Filter for: host|broadcast|multicast|others|outgoing
-F|--interval <size|time> Dump interval if -o is a dir: <num>KiB/MiB/GiB/s/
sec/min/hrs
-R|--rfraw Capture or inject raw 802.11 frames
-n|--num <0|uint> Number of packets until exit (def: 0)
-P|--prefix <name> Prefix for pcaps stored in directory
-O|--overwrite <N> Limit the number of pcaps to N (file names use numbers
0 to N-1)
-T|--magic <pcap-magic> Pcap magic number/pcap format to store, see -D
```

1. **Captura de tráfico:** Permite capturar paquetes en una interfaz de red específica.
2. **Reproducción de tráfico:** Puedes enviar tráfico previamente capturado a través de una interfaz de red.
3. **Filtrado de tráfico:** Filtra paquetes específicos según ciertos criterios (como puertos o protocolos).
4. **Opciones de salida:** Especifica el formato y ubicación de los archivos de captura.
5. **Modos avanzados:** Como el modo de captura de baja latencia, análisis detallado de tráfico, estadísticas de red, entre otros.

```
root@kali: /
File Actions Edit View Help
netsniff-ng --in eth0 --out dump.pcap -s -T 0xa1b2c3d4 --bind-cpu 0 tcp or udp
netsniff-ng --in wlan0 --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 wlan0 --out dump.pcap -c -u 'id -u bob' -g 'id -g bob'
netsniff-ng --in any --filter http.bpf --jumbo-support --ascii -V

Note:
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/netsniff-ng/netsniff-ng/issues
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
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

root@kali)~[/]
```

```
root@kali: /home

File Actions Edit View Help

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/netsniff-ng/netsniff-ng/issues
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
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.

(root@kali)-[/]
# cd /home

(root@kali)-[/home]
# pwd
/home

(root@kali)-[/home]
# ls
capturaAriana capturaelkin kali

(root@kali)-[/home]
#
```

Cuando se ejecuta `cd /home`, el terminal cambia tu ubicación al directorio `/home`. Después de este comando, mostrará como directorio actual `/home`, y desde allí se puede ver los directorios de los usuarios o navegar a otros subdirectorios.

Si después se ejecuta el comando `ls`, saldrá una lista de carpetas de usuarios, como:

```
root@kali: /home/capturaAriana

File Actions Edit View Help

capturaAriana capturaelkin kali

(root@kali)-[/home]
# cd capturaAriana

(root@kali)-[/home/capturaAriana]
# ls
wcaptura.pcap wcapturatx.pcap

(root@kali)-[/home/capturaAriana]
# mkdir wMercedes.pcap

(root@kali)-[/home/capturaAriana]
# ls
wcaptura.pcap wcapturatx.pcap wMercedes.pcap

(root@kali)-[/home/capturaAriana]
# ls -l
total 4
-rwxrwxr-x 1 root root 0 Nov 11 12:30 wcaptura.pcap
-rw-rw-r-- 1 root root 0 Nov 11 12:23 wcapturatx.pcap
drwxrwxr-x 2 root root 4096 Nov 11 18:59 wMercedes.pcap

(root@kali)-[/home/capturaAriana]
#
```

El comando `mkdir wMercedes.ccap` se usa para **crear un nuevo directorio (carpeta)** con el nombre `wMercedes.ccap` en el directorio actual.

- **mkdir:** Es el comando para "make directory" (crear un directorio).
- **wMercedes.ccap:** Es el nombre del nuevo directorio que se está creando. En este caso, `wMercedes.ccap` es solo un nombre y no tiene ningún significado especial. Aunque

termina en .ccap, el sistema de archivos lo interpretará simplemente como una carpeta, a menos que tenga otro contexto en el sistema.

```
root@kali: /home/capturaAriana
File Actions Edit View Help
# mkdir wMercedes.pcap
(root@kali)~/home/capturaAriana
# ls
wcaptura.pcap  wcapturatx.pcap  wMercedes.pcap
(root@kali)~/home/capturaAriana
# ls -l
total 4
-rwxrwxr-x 1 root root 0 Nov 11 12:30 wcaptura.pcap
-rw-rw-r-- 1 root root 0 Nov 11 12:23 wcapturatx.pcap
drwxrwxr-x 2 root root 4096 Nov 11 18:59 wMercedes.pcap
(root@kali)~/home/capturaAriana
# netsniff-ng -i eth0 -out /home/capturaelkin/wMercedes.pcap -s icmp
Running! Hang up with ^C!
0 packets incoming (0 unread on exit)
0 packets passed filter
0 packets failed filter (out of space)
39 sec, 10381 usec in total
(root@kali)~/home/capturaAriana
#
```

Se ejecuta el comando `ls -l` dentro de la ruta donde se creó el directorio `wMercedes.ccap`, se verá un listado detallado de los archivos y directorios que están en ese directorio.

ls: Lista el contenido del directorio actual.

-l: Muestra los detalles de cada archivo o carpeta en formato de lista larga.

```
root@kali: /home/capturaAriana
File Actions Edit View Help
more [options] <file> ...
Display the contents of a file in a terminal.
Options:
-d, --silent          display help instead of ringing bell
-f, --logical         count logical rather than screen lines
-l, --no-pause       suppress pause after form feed
-c, --print-over     do not scroll, display text and clean line ends
-p, --clean-print    do not scroll, clean screen and display text
-e, --exit-on-eof    exit on end-of-file
-s, --squeeze        squeeze multiple blank lines into one
-u, --plain          suppress underlining and bold
-n, --lines <number> the number of lines per screenful
<number>            same as --lines
+<number>          display file beginning from line number
+<pattern>         display file beginning from pattern match

-h, --help          display this help
-V, --version       display version

For more details see more(1).
(root@kali)~/home/capturaAriana
#
```

Este comando de **netsniff-ng** se usa para capturar tráfico de red en la interfaz `eth0`, filtrando solo paquetes ICMP (como el tráfico de ping), y guardar la captura en un archivo llamado `wMercedes.pcap` dentro del directorio `/home/capturaelkin`.



- **-i eth0**: Especifica la interfaz de red a capturar. En este caso, es eth0 (puede ser diferente en otros sistemas, por ejemplo, wlan0 en caso de Wi-Fi).
- **--out /home/capturaelkin/wMercedes.pcap**: Define la ubicación y el nombre del archivo donde se guardarán los datos capturados. Aquí se guardarán en /home/capturaelkin/wMercedes.pcap.
- **-s icmp**: Filtra la captura de paquetes para que incluya solo tráfico ICMP (Internet Control Message Protocol), que es el protocolo usado por herramientas como ping.



