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 Rio Colorado, Sonora Feb, 2022

netsniff-ng
the packet sniffing beast

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”.