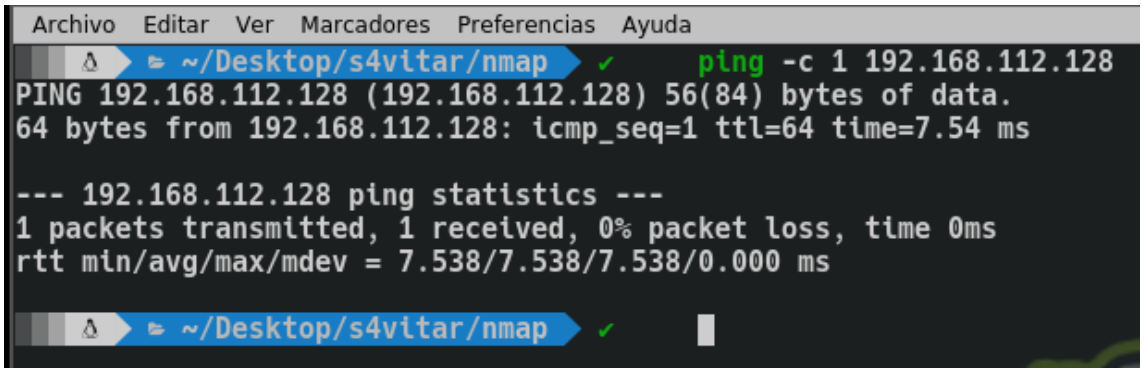
ANALISIS DE TRAFICO CON TSHARK

Maquina origen: *192.168.112.169*

Maquina destino: *192.168.112.128*

Enviamos una traza ICMP a la maquina destino y capturamos el tráfico con tcpdump:



Como se observa es una maquina Linux y responde al comando ping.

Al leer la captura en formato json:

Tshark -r captura.cap -T json 2>/dev/null

Obtenemos en este segmento la información que queremos filtrar:

Y lo filtramos:

Tshark -r captura.cap -T json 2>/dev/null | grep -E ‘ip.src”|ip.dst”’ | tr “,” “ ”

grep -E ‘ip.src”|ip.dst”’ = el parámetro -E deja filtrar por varios parámetros, en este caso nos interesa saber la IP origen y destino (ipp.src y ipp.dst). En el filtro le agrego unas comillas dobles al final para un filtrado mas específico y tener esa respuesta.

tr “,” “ ” = es algo estético nada más, el filtrado terminaba en ‘,’ (coma) y como somos muy **tikis mikis** no me gustaba y lo reemplazo por un espacio en blanco.

Se puede ver como hay 4 resultados:

Uno con la dirección IP de la que envío el ping (192.168.112.128) como IP de origen que es la consulta y otra con la dirección de la otra maquina (192.168.112.128) como origen que es la respuesta.

Saludos desde Bolivia s4vitar sigue adelante.