

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:

```
Archivo  Editar  Ver  Marcadores  Preferencias  Ayuda
~ / Desktop / s4vitar / nmap  ✓  ping -c 1 192.168.112.128
PING 192.168.112.128 (192.168.112.128) 56(84) bytes of data.
64 bytes from 192.168.112.128: icmp_seq=1 ttl=64 time=7.54 ms

--- 192.168.112.128 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 7.538/7.538/7.538/0.000 ms

~ / Desktop / s4vitar / nmap  ✓
```

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:

```
{
  "icmp": {
    "icmp.type": "0",
    "icmp.code": "0",
    "icmp.checksum": "0x0000cb33",
    "icmp.checksum.status": "1",
    "icmp.ident": "11872",
    "icmp.ident": "24622",
    "icmp.seq": "1",
    "icmp.seq_le": "256",
    "icmp.resp_to": "1",
    "icmp.resptime": "0.234",
    "icmp.data_time": "Jan 4, 2021 16:44:14.000000000 -04",
    "icmp.data_time_relative": "0.375594000",
    "data": {
      "data.data": "30:ba:05:00:00:00:00:00:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24:25:26:27:28:29:2a:2b:2c:2d:2e:2f:30:31:32:33:34:35:36:37",
      "data.len": "48"
    }
  }
}
```

Y lo filtramos:

```
~ / Desktop / s4vitar / nmap  ✓  tshark -r captura.cap -T json 2>/dev/null | grep -E 'ip.src|ip.dst' | tr ", " " "
{"ip.src": "192.168.112.169", "ip.dst": "192.168.112.128"}
{"ip.src": "192.168.112.128", "ip.dst": "192.168.112.169"}

~ / Desktop / s4vitar / nmap  ✓
```

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 envió 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.