PingMe

Enunciado

> Me identifico como una persona de género paquete sexual binario.

Files

- pingMe.pcapng

Solución

Si abrimos la captura con la herramienta Wireshark podemos observar que todo el tráfico es ICMP desde un mismo host a dos diferentes.

Siguiendo la información proporcionada en el enunciado podemos observar que nos dice que es ***paquete sexual binario*** y si nos fijamos bien, solo tenemos dos direcciones IP destino, que casualmente acaban en 0 y 1 respectivamente.

Vamos en orden esa secuencia binaria para analizarla. Para ello, utiizaremos una herramienta similar a Wireshark que es **TShark**, un analizador de tráfico de red de línea de comando que puede instalarse mediante apt.

Una vez instalada filtraremos la salida por:

```
$ tshark -r pingMe.pcapng -Y "ip.src == 10.0.1.33" -T fields -e ip.dst
```

Con esto logramos que la salida por consola solo aparezcan las direcciones destino en las cuales la dirección source es la 10.0.1.33. La salida es algo como esto:

```
10.0.2.30
10.0.2.31
10.0.2.30
10.0.2.31
10.0.2.30
 <snip>
10.0.2.31
```

```
10.0.2.31
10.0.2.31
10.0.2.30
10.0.2.31
```

Ahora con bash podemos limpiar la salida para quedarnos solo con el último dígito, de la siguiente forma:

```
$ tshark -r pingMe.pcapng -Y "ip.src == 10.0.1.33" -T fields -e ip.dst | awk -F'.' '{print substr($NF,length($NF),1)}' | tr -d '\n'
```

Con esto conseguimos que la salida sea un único string de 0 y 1 extraídos del último dígito de cada IP destino.

```
0101001101010101010001110101010101010011011110110100100101000011010011010101000001011111011010100011000001101011001100110101111100111111010111110100101001110101001101010011011101011111011100000011000101101110001101100101111101001101001100110010100000101111101
```

Con la ayuda de la herramienta online CyberChef podemos convertirlo a texto ASCII obteniendo así la flag.

> ***SUGUS{ICMPj0k3?_Ju57_p1n6_M3!}***