Fiesta ETSIIT 2022

HellMan WRITEUP

Escuela Técnica Superior de Ingenierías Informática y de Telecomunicación

Granada, 11 de mayo de 2022

Introducción

En este reto nos enfrentamos ante un análisis de tramas por medio de *Wireshark*, un conocido analizador de protocolos muy usado para el análisis de redes de comunicación.

Para resolver el reto son recomendables conocimientos básicos de protocolos de comunicación, aunque investigando las tramas un poco es de fácil solución.

Resolución

Lo primero es analizar de manera breve la trama, comprobamos así qué tipo de conexiones se están dando para hacernos una idea de dónde buscar.

El reto puede ser muy tedioso si no se descartan las tramas inútiles como las *SSDP*, *IGMP*, *MDNS* o los *TCP RST* (las tramas TCP rojas y negras). Estos protocolos no son protocolos de intercambio de información y por ello se descartan, es fácil descubrir esto si los buscamos en internet o incluso en *Wireshark*, donde podemos ver los contenidos y descripciones de estos.

Las conexiones con información suelen ser TCP principalmente, así que comenzamos a analizar las conexiones TCP que encontramos. Utilizando la opción de *Wireshark* pulsando click derecho sobre la trama que queramos analizar:

Seguir - Flujo TCP

De esta manera es muy rápido el análisis ya que nos mostrará todo el flujo de la conexión en vez de ir de uno en uno.

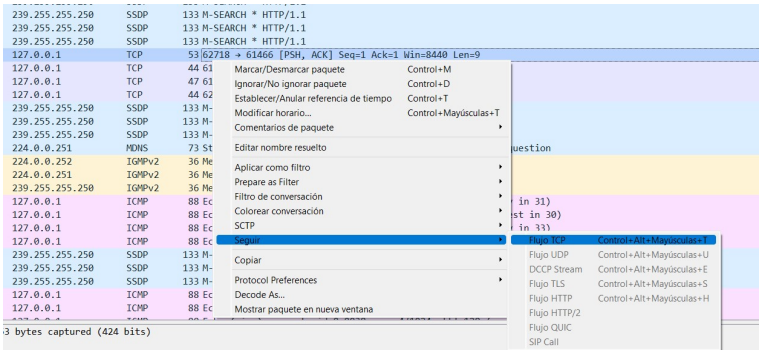

Figura 1: Análisis de la primera trama TCP

Si observamos lo que contiene la trama no nos dice mucho, se consideraría "basura".

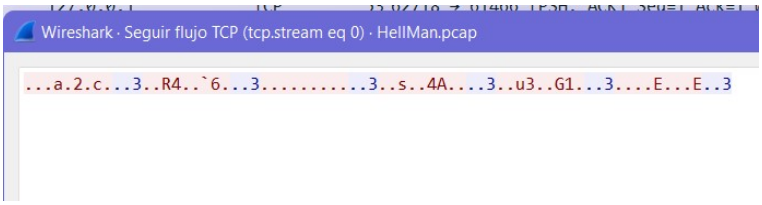

Figura 2: Contenido de la primera trama TCP

De la misma manera podemos ir descartando tramas que no contencan nada interesante, otro dato a tener en cuenta son los puertos de conexión. Si vemos conexiones a puertos carasterísticos podemos intuir que algo sucede en esa comunicación.

El primer puerto característico es el 8888, seguimos el flujo TCP de la conexión y comprobamos qué tiene.

Figura 3: Contenido de la trama TCP con conexión al puerto 8888

Se observan una serie de mensajes encriptados y al final se puede leer que se trata de un intercambio Diffie-Hellman, método de cifrado digital para el intercambio de claves simétricas, por lo que la información cifrada será ïmposible"de descifrar ya que hace uso de hashes.

Hacemos caso omiso a las claves y observamos la última sentencia que parece ser Base64, aunque si no nos damos cuenta podemos usar detectores como *CyberChef*, que también usaremos para decodificar.

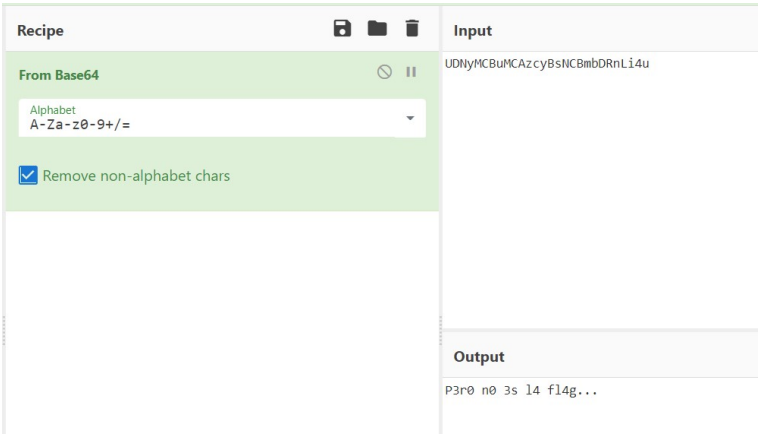

Figura 4: Ddecodificación en *CyberChef* de mensaje en Base64

Parece que estábamos en un "*Rabbit Hole*"... A lo largo del archivo pcap hay varias comunicaciones que no contienen nada y solo están puestas para distraer, como las comunicaciones por *UDP* en *TPLINK*.

Una vez superadas todas las distracciones, nos fijamos en la comunicación TCP por el puerto 1234, puerto más que sugerente. Si seguimos el flujo encontramos una comunicación en binario.

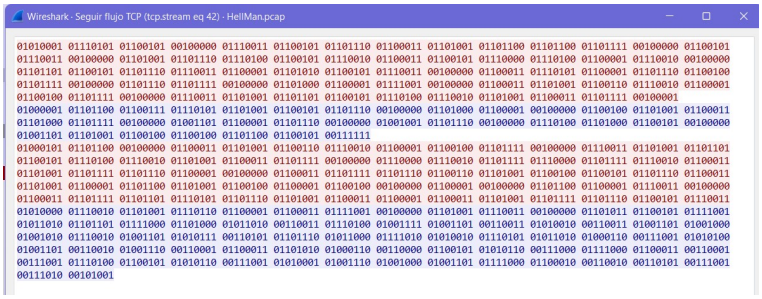

Figura 5: Flujo TCP por el puerto 1234

Si usamos *CyberChef* esta vez para pasar de binario a texto obtenemos lo siguiente.

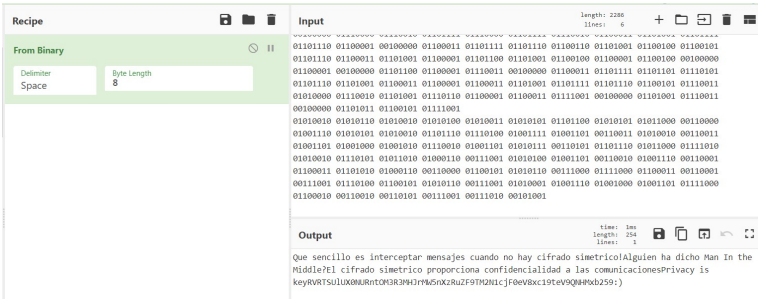

Figura 6: Descifrado de la comunicación TCP por el puerto 1234

Parece que esto pinta bien. De nuevo obtenemos un conjunto de caracteres que parecen *Base64*, así decodificamos.

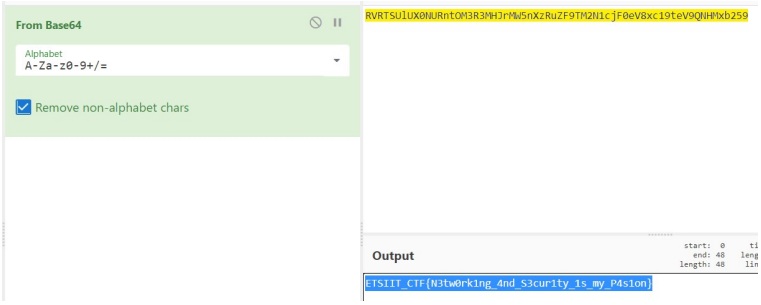

Figura 7: Descifrado de la flag

¡Y ya tenemos la flag!

Autora del reto:

Raquel Romero Pedraza - raquelrom@correo.ugr.es