ANÁLISIS DE DATOS

PRACTICA 5

C.E.S ACADEMIA LOPE DE VEGA

CFGS: 2º Administración de Sistemas Informáticos en Red

Curso: 2017/2018

Asignatura: Seguridad y Alta Disponibilidad

Prof. Miguel Angel González

Autor: Rafael Osuna Ventura

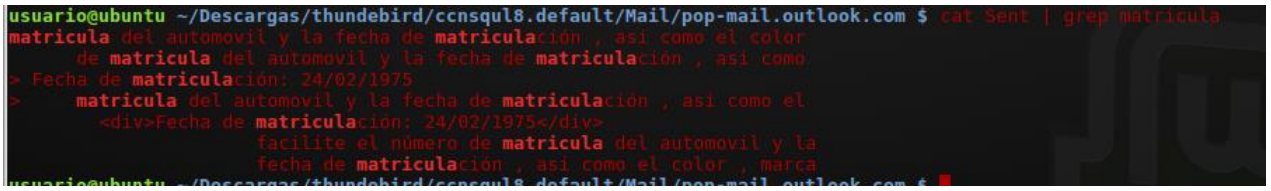
Rafael Osuna Ventura
2ºASIR

Ejercicio 1.

Parece que D. Furioso, profe de mates, ha tenido un percance y no quiere facilitar cierta la información relativa a la matrícula de su coche desaparecido, necesaria para tramitar el parte con el seguro. Hemos logrado acceder al equipo de D. Furioso y hemos realizado una extracción de su carpeta de correo electrónico. Tenemos que examinar sus comunicaciones para obtener la información.

Para encontrar la matricula empezamos descomprimiendo el archivo correo.zip, luego buscamos los correos electrónicos donde seguramente haya constancia de la matrícula. Haciendo uso del comando cat y grep buscaremos dentro los mensajes la matricula.

Primero probamos en los mensajes enviados. En estos se nos hace referencia a la matricula, pero esta no nos aparece.



Ahora vamos a probar en la bandeja de entrada, en esta encontraremos el número de matrícula**: C047057**

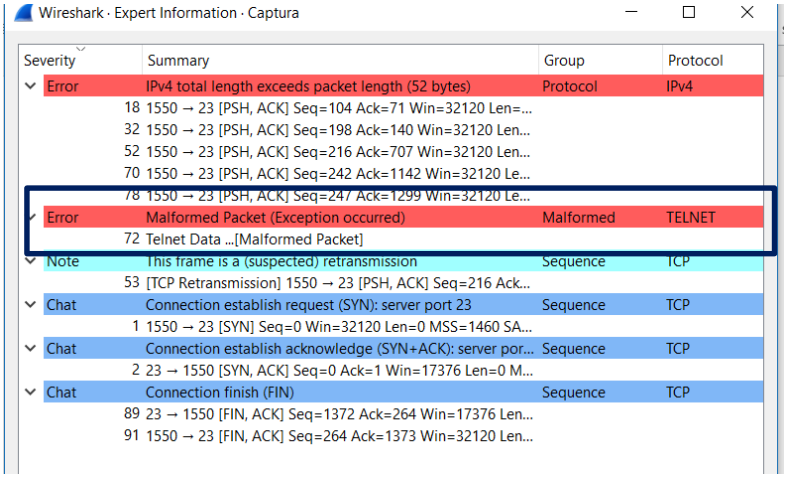
Rafael Osuna Ventura
2ºASIR

Ejercicio 2.

Alguien está usando servicios sin cifrar el tráfico, algo que no se puede permitir, transmitiendo las credenciales de acceso en texto plano. Se ha obtenido una captura de tráfico donde se ha producido una conexión remota entre dos equipos. Debemos encontrar las credenciales utilizadas en dicha conexión para conocer quién es el usuario e indicarle que debe hacerlo de manera correcta.

Nos fijamos que el enunciado nos dice que se realiza una conexión remota por lo que ya sabemos que protocolo se ha usado, TELNET. Ya podemos empezar a filtrar la información.

Si nos vamos a sumario se nos muestra la información relevante de esta captura, y observamos que a hay un error en una trama con protocolo TELNET.



Esa debe de ser la trama en el que venga la información que estamos buscando. Efectivamente al buscar en ella encontramos el usuario y contraseña.

fake:user

```
B.
.......................".....'.....#..
9600,9600....#.bam.zing.org:0.0....'..DI
color.............!.................".....
OpenBSD/i386 (oof) (ttyp2)

login: fake
......Password:user

......Last login: Sat Nov 27 20:11:43 on
Warning: no Kerberos tickets issued.
OpenBSD 2.6-beta (OOF) #4: Tue Oct 12 20
```

Rafael Osuna Ventura
2ºASIR

Ejercicio 3.

Se ha detenido un sospechoso de haberse infiltrado en una gran empresa en España, desde la que ha estado enviando un código a un asociado para informar sobre ciertas acciones previamente establecidas. Se necesita encontrar indicios de la supuesta clave que ha enviado.

Hemos obtenido una captura de tráfico de su ordenador. Analízala para ver si existe algún tipo de mensaje o palabra clave que haya intentado ocultar con especial cuidado.

Analizamos la captura con Wireshark pero solo obtemos información que nos dará una pista sobre que buscar a la hora de analizar la captura en NetworkMiner. La información que hemos obtenido es que es amante de la cultura romana.

Ahora desde NetworkMiner, no encontramos nada, pero en el apartado imágenes entre todas encontramos varias de monumentos romanos en España.

En alguna de estas imagines hay texto camuflado dentro:

La palabra clave como se observa es HISPANIA