Entrega № 4 Proyecto Seguridad Informática

Auditoria de la Aplicación y Decompilación

Camilo Zepeda Hoffmann

Profesor Maximiliano Vega

02 de Noviembre 2017

1. Resumen

Ya en conocimiento de los datos y archivos encontrados se realizan pruebas asociadas a la captación de paquetes, utilizando prácticas de man-in-the-middle y herramientas pertienentes que efecten la recopilación de los nombrados paquetes.

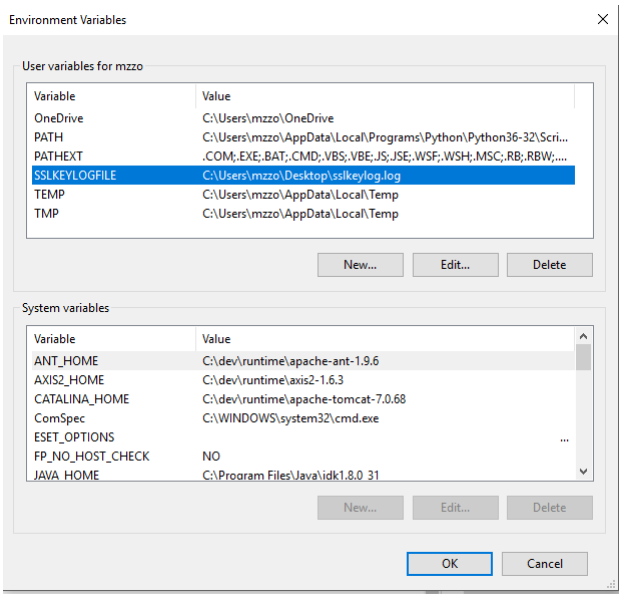
2. Pruebas y Herramientas

Se realizan pruebas del tipo interceptoras, con tal de captar información sensible utilizando falseos de certificados y Wireshark. Entonces para determinar lograr un mayor comprendimiento de los pasos realizados, se nombra:

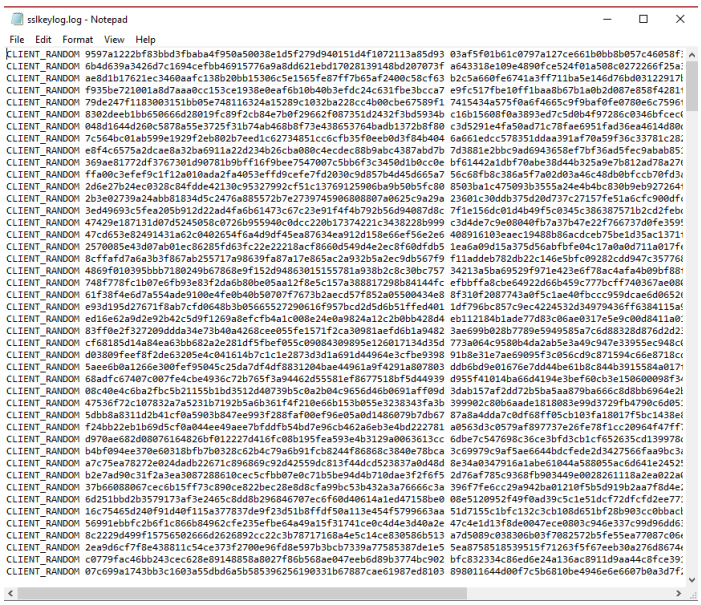
- **Paso 1**: es necesario generar una variable ambiente del tipo **PATH** que contenga de nombre SSL y la ruta del archivo a efectuar:

  ```
  C\\ruta\\ruta\\ sslkeylog.log
  ```

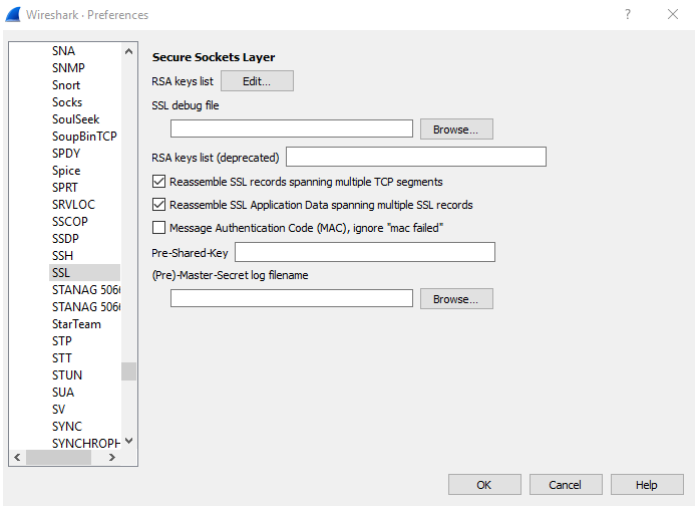
  donde **sslkeylog.log** corresponde al archivo contenedor de los certificados ssl falsificados. Lo anterior se describe en la siguiente imagen:



  Al generar la variable de ambiente dentro del entorno del sistema operativo, se genera de manera automáticamente el archivo nombrado, el cual contiene:

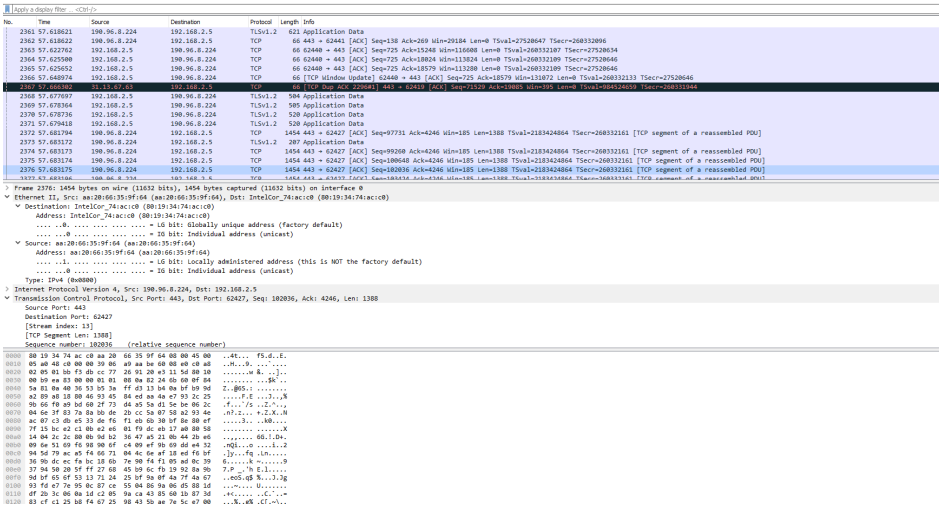


- **Paso 2**: ya extraído el archivo anteriormente mencionado, se procede a adjuntar los certificados a herramienta **WireShark**, con tal de generar una captación y evaluación real del desempeño de los certificados. A continuación se presenta lo descrito:

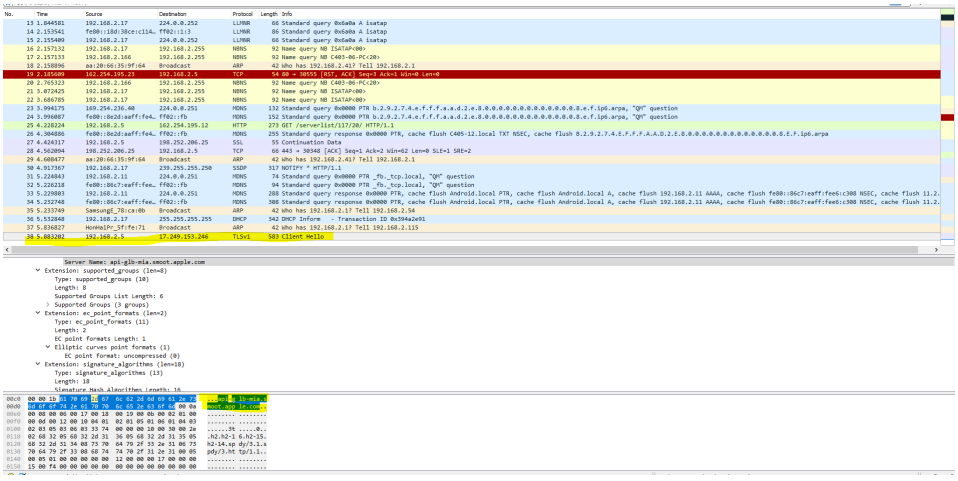


Es necesario proveer la ruta especifica en donde se encuentra el archivo generado por el PATH, de tal manera que trabajen como decifradores de las request generadas al hacer man-in-the-middle, trabajando entonces sobre los paquetes captados al probar la aplicación.

- **Paso 3**: Una vez realizado los pasos anteriores se procede generar la prueba de captación de paquetes, para lo cual fue necesario implementar el computador como emisor de conexión WIfi recepcionado por el dispositivo móvil contenedor de la aplicación. Entonces se obtiene:



La figura anterior describe la prueba asociada, dando a conocer los paquetes e intentando descifrar los archivos y request solicitadas, por medio de los certificados generados. Otro ejemplo concluyente de los resultados fue:



Es posible apreciar lectura de los paquetes, entregando paquetes del tipo TCP y CLIENT HELLO, de la cuál se adjunta una recepción del paquete mayormente ilegible, pero aún así, no se encuentra información consistente y tangible de las respuestas. Lo que implica que no es posible captar la información de los usuarios o bien sentencias explotables, dando a entender que los certificados generados no proveen de información y por tanto de utilidad.

2.1. Propuestas para Quintp Incremento

Con el fin de lograr una mayor comprensión de lo propuesto se define el siguiente listado.

- Analizar en profundidad las funciones Internas React, depurando la información.
- Generar certificados SSL para el desarrollo de Man-in-the-Middle
- Buscar posibles Scripts utilizados para robar información.

- Utilizar herramientas de OpenSSL con tal de generar nuevos certificados ssl, capaces de captar información de utilidad.

Referencias

[1] A. Plaza, Ün fallo de seguridad en Instagram muestra la vulnerabilidad de las cuentas | Hipertextual", Hipertextual, 2017. [Online]. Available: https://hipertextual.com/2013/05/fallo-de-seguridad-en-instagram. [Accessed: 11- Oct- 2017].

[2] "La posibilidad de usar varias cuentas en Instagram presenta un fallo de seguridad - TreceBits", TreceBits, 2017. [Online]. Available: http://www.trecebits.com/2016/02/16/la-posibilidad-de-usar-varias-cuentas-en-instagram-presenta-un-fallo-de-seguridad/. [Accessed: 11- Oct- 2017].

[3] .El hackeo a Instagram, más grave de lo esperado: 6 millones de cuentas", ADSLZone, 2017. [Online]. Available: https://www.adslzone.net/2017/09/02/el-hackeo-instagram-mas-grave-de-lo-esperado-6-millones-de-cuentas/. [Accessed: 11- Oct- 2017].

[4] https://www.buzztouch.com/forum/thread.php?tid=B60C6EE41CD7D289048B0F4

[5] https://github.com/arashpayan/appirater

[6] https://iphoneros.com/44273/asi-es-el-modo-reachability-para-poder-utilizar-el-iphone-6-plus-con-una-sola-mano-video

[7] https://curl.haxx.se/docs/history.html