Entrega № 5 Proyecto

Seguridad Informática

Auditoria de la Aplicación y
Decompilación

Camilo Zepeda Hoffmann

Profesor Maximiliano Vega

15 de Noviembre 2017

1. Resumen

Al igual que los incrementales anteriores se dan a conocer los pasos correspondientes a una nueva prueba de auditoría exponiendo las actividades y puntos encontrados a lo largo de la experiencia.

2. Pruebas y Herramientas

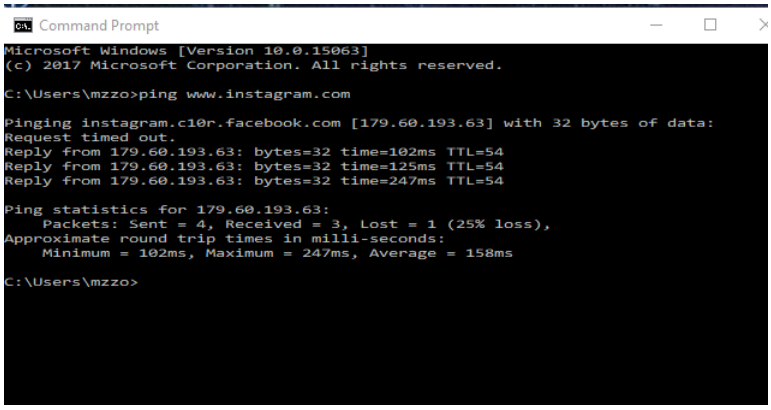
Se realizan pruebas del tipo interceptoras, con tal de captar información sensible utilizando falseos de certificados y Wireshark. Entonces para determinar lograr un mayor comprendimiento de los pasos realizados, se nombra:

- **Paso 1**: se hace uso de la Herramienta Metasploit utilizada para desarrollar y ejecutar exploits contra una máquina remota, generando scripts de utilidad, declarando ejercicios como DoS u otros, de tal manera de generar pruebas dentro de la IP obtenida.

- **Paso 2**: es necesario realizar un ping por CMD de la página atacar, de tal manera de obtener su Ip y datos pertinentes, utilizando el siguiente comando:

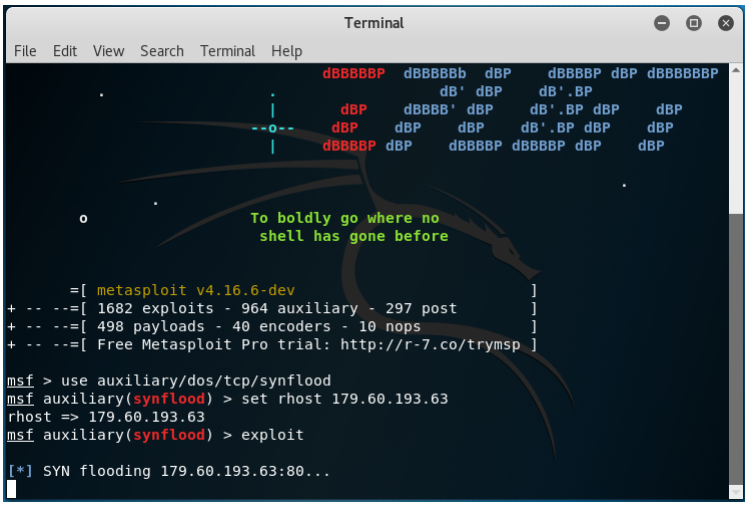
  ping www.instagram.com

  de lo cual se obtiene:



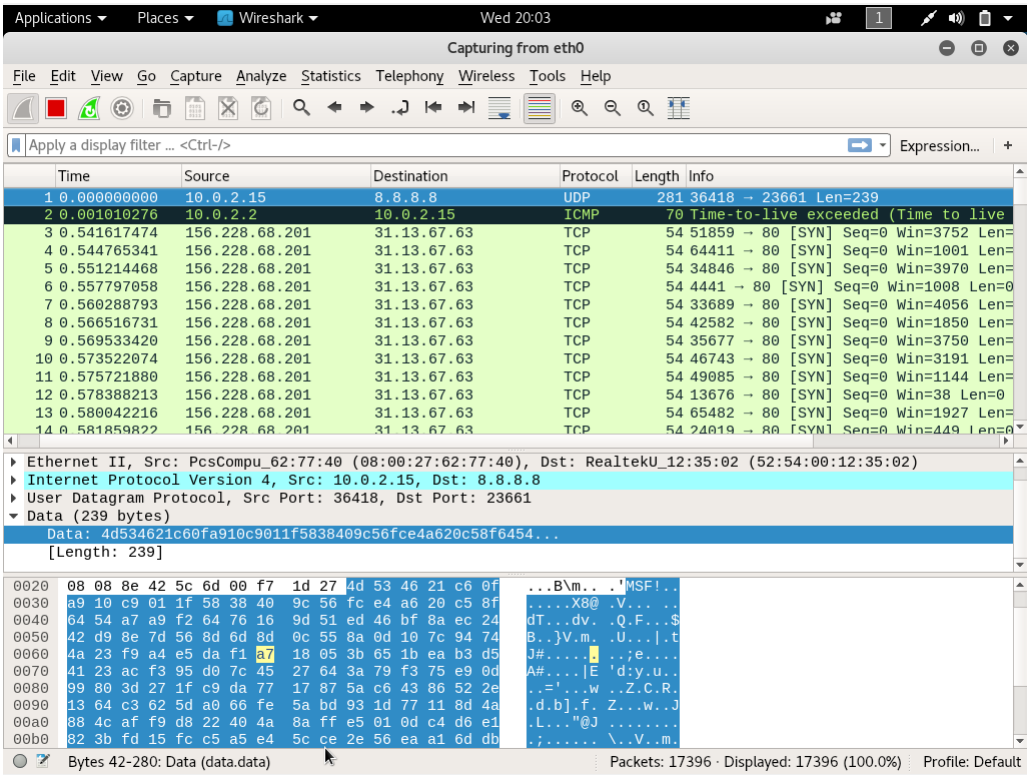
Si bien al realizar el ping se obtiene una ip consistente, tras realizar diversos ping al mismo sitio se generan distintas IP's lo que implica una distribución realizada por parte de los desarrolladores. Aún con la resolución del asunto es posible destacar respuestas por partes del sitio, dando paso a vistas del tipo ICMP. Entonces se logra destacar que existe uso del servidor **Gunicorn** para manejo de peticiones, el cual a diferencia de Apache es más fácil de implementar y menos intensivo con la CPU, de igual manera para la ejecución de comando se utiliza **Fabric** como despliegue de ejecución (consultas)

- **Paso 3**: Se dispone a utilizar el siguiente comando **use auxiliary/dos/tcp/synflood**, donde se provee **auxiliary**, el cual permite la obtención de información sobr el objetivo, con tal de determinar las posibles vulnerabilidades. Además de proveer el protocolo **tcp** y el tipo de ataque a realizar, el cual para este caso corresponde a **dos** y **synflood**



Entonces tras proveer los comandos necesarios para realizar el ataque es necesario describir el rhost al cual atacar, donde la IP obtenida corresponde al ping generado en el paso anterior, siendo entonces **179.60.193.63**

- **Paso 4**: ya inicializado el ataque se utiliza la herramienta wireshark con tal de ver el envio de paquetes en línea, siendo la respuesta:



En la figura anterior es posible apreciar los diferentes paquetes enviados, asociados a sus respectivas respuestas. Cabe destacar, que si bien el ataque se realiza exitosamente no es posible generar un ataque consistente debido a los escasos recursos y lo amplio de la red de la página asociada.

Referencias

[1] www.instagram.com

[2] http://gunicorn.org/

[3] https://www.si6networks.com/presentations/ANTEL07/fgont-antel07-icmp-attacks.pdf

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

[5] https://www.kali.org/

[6] https://www.metasploit.com/