Un ataque por la red

LABORATORIO #1

Escenario

Introducción

Se ha producido un ataque en un dispositivo de nuestra red y hemos logrado capturar los paquetes de red correspondientes para su posterior análisis.

Para resolver el presente laboratorio el alumno debe contar con el archivo de evidencia **network-evidence.zip** el cual puede ser bajado del aula virtual.

Dentro de este archivo encontraremos una captura de datos de la red de un sistema que ha sido atacado.

Preguntas a responder

Para resolver el laboratorio, el alumno deberá responder las siguientes preguntas justificando en cada caso las respuestas y especificando las herramientas utilizadas:

1. Validar el hash de la evidencia. Continuar con las siguientes preguntas sólo en caso que la evidencia se encuentre validada.

Archivo	md5	sha1
network-evidence.zip	fac76800cdf6e4961f41c06ee7905313	2e26b80af69e25fd37e9bc465712d37b0d3ed713
network-evidence.pcap	6ad68928fe8062632c12c432ce785ac5	d261a70feeeabcd49a6cfdd33087989b472fd80d

2. ¿Cuántos dispositivos se encuentran involucrados en la conversación?
3. ¿Cuántas sesiones TCP contiene la evidencia?
4. Identifique la dirección IP del atacante y la dirección IP de la víctima.
5. ¿Puede geolocalizar a la dirección IP del atacante? ¿Quién es el dueño de esa dirección IP?
6. ¿Qué sistema operativo tienen los dispositivos involucrados?
7. ¿Cuánto tiempo le llevó al atacante perpetrar el ataque?
8. ¿Cuál fue el servicio atacado?¿Cuál fue específicamente la vulnerabilidad que el atacante explotó?
9. Detallar y graficar las acciones que el atacante efectuó sobre la máquina víctima.

10. Determine la existencia de un malware. En caso afirmativo, especifique el nombre de dicho malware.

11. Determine si el ataque fue realizado de forma manual o automática y si tuvo éxito.

Herramientas sugeridas

A continuación se listan un conjunto de herramientas sugeridas para resolver el laboratorio.

- **Wireshark** o **Tshark** (la versión de línea de comandos) es el analizador de protocolos de red más importante y más utilizado del mundo. Le permite ver lo que está sucediendo en su red a un nivel microscópico y es el estándar de facto en muchas empresas comerciales y sin fines de lucro, agencias gubernamentales e instituciones educativas. Wireshark se desarrolla gracias a las contribuciones voluntarias de expertos en redes de todo el mundo y es la continuación de un proyecto iniciado por Gerald Combs en 1998. https://www.wireshark.org/

- **NetworkMiner** es una herramienta de análisis forense de redes (NFAT) para Windows. NetworkMiner se puede utilizar como un rastreador de red pasivo / herramienta de captura de paquetes para detectar sistemas operativos, sesiones, nombres de host, puertos abiertos, etc. sin poner tráfico en la red. NetworkMiner también puede analizar archivos PCAP para análisis fuera de línea y para regenerar / reensamblar archivos y certificados transmitidos a partir de archivos PCAP. https://www.netresec.com/

- **p0f** es una herramienta que utiliza una serie de sofisticados mecanismos de identificación de huellas de tráfico pasivo para identificar a los sistemas detrás de cualquier comunicación TCP / IP. La versión 3 es una reescritura completa del código base original, que incorpora una cantidad significativa de mejoras en la toma de huellas a nivel de red e introduce la capacidad de detección sobre tráfico a nivel de aplicación (por ejemplo, HTTP). https://lcamtuf.coredump.cx/p0f3/

- **VirusTotal** es un servicio en línea para analizar archivos y URLs sospechosas para detectar tipos de malware y compartirlos automáticamente con la comunidad de seguridad. https://www.virustotal.com/gui/

- **Snort** es el sistema de prevención de intrusiones (IPS) de código abierto más importante del mundo. Snort IPS usa una serie de reglas que ayudan a definir la actividad de red maliciosa y usa esas reglas para encontrar paquetes que coincidan con ellos y generar alertas para los usuarios.

Desafíos potencialmente peligrosos

Algunos desafíos forenses que vamos a realizar pueden contener piezas de código realmente maliciosas.

Tomar todas las precauciones del caso dado que

¡El profe no arreglará tu computadora!